LA HISTÒRIA DE LA CRIPTOGRAFIA I EL CRIPTOANÀLISI. DES DE L'ANTIC EGIPTE FINS A L'ACTUALITAT.

Rivest Shamir Adelman

ABSTRACT

En aquest treball el lector serà introduït en el món de la criptografia i el seu antagonista, el criptoanàlisi. Estudiarem l'evolució que ha patit al llarg de la història de la humanitat, des de l'Antic Egipte fins a l'actualitat. Paral·lelament, tractarem els principis més bàsics, com la transposició i substitució, i, a mesura que anem avançant al llarg de la història, veurem quins avenços es produeixen en aquests camps. Una vegada arribem a l'actualitat explicarem els principals algoritmes que es fan servir avui en dia i xifrarem i desxifrarem un missatge, tot utilitzant l'RSA, explicat de manera detallada. A través del treball, aconseguirem adonar-nos quant d'important arriba a ser la criptografia en el nostre dia a dia i que diferent seria l'era de l'internet sense ella, i d'igual manera sense el criptoanàlisi.

En este trabajo el lector será introducido en el mundo de la criptografía y su antagonista, el criptoanálisis. Estudiaremos la evolución que ha sufrido a lo largo de la historia de la humanidad, desde el Antiguo Egipto hasta la actualidad. Paralelamente, trataremos los principios más básicos, como la transposición y sustitución, y, a medida que vayamos avanzando a lo largo de la historia, veremos qué adelantos se producen en estos campos. Una vez llegamos a la actualidad, explicaremos los principales algoritmos que se usan hoy en día y cifraremos y descifraremos un mensaje, utilizando el RSA, explicado de manera detallada. A través del trabajo, conseguiremos darnos cuenta cuánto de importante llega a ser la criptografía en nuestro día a día y que diferente sería la era del internet sin ella, y de igual manera sin el criptoanálisis.

In this work the reader will be introduced into the world of cryptography and its antagonist, cryptanalysis. We will study the developments that have taken place throughout human history, from Ancient Egypt to the present. At the same time, we will deal with the most basic principles, such as transposition and substitution, and, as we move forward in history, we will see what progress is made in these fields. Once we get to the current era, we will explain the main algorithms that are used nowadays and encrypt and decrypt a message, using RSA, explained in detail. Throughout the work, we will be able to realise how important cryptography is in our daily basis life and how different the era of the Internet would be without it, and also without cryptanalysis.

INTRODUCCIÓ

La principal intenció d'aquest treball de recerca és investigar i entendre què és la criptografia, els principis matemàtics que utilitza i la història de la criptografia mateixa, des de l'Antic Egipte fins a la actualitat. Aprofundiré en la lluita entre la criptografia i el criptoanàlisi, la guerra que sembla que no té final, l'evolució que ha anat patint al llarg de la història i una part pràctica explicant el funcionament i procediment d'un algoritme (RSA), xifrant pas per pas un missatge. Aspiro a poder explicar i intentar introduir al lector en aquest magnífic camp, comprendre com funcionen alguns dels sistemes d'encriptacions actuals i tot explicat de manera amena i senzilla. Per acabar, intentaré explicar la importància que té la criptografia en el nostre dia a dia.

1. Criptografia

Des dels inicis de les civilitzacions, la comunicació segura ha estat essencial per a la seguretat i bon funcionament d'una societat, fins a arribar al punt que sense la criptografia, probablement el món seria molt diferent de com el coneixem, com a mínim, segur que els fets històrics més remarcables haurien tingut un final diferent. Encara que no siguem conscients, la criptografia és una eina que es porta utilitzant des de l'Antic Egipte. La criptografia com a tal va sorgir per la necessitat dels governants de transmetre la informació d'una manera segura, desde ocultar el missatge (esteganografia) fins a codificar el missatge (criptografia).

La **criptografia** és l'art de la comunicació secreta, on l'objectiu principal és amagar el significat del missatge, però no amagar el missatge. És a dir, tothom podrà llegir el missatge, amb la intenció que ningú el pugui entendre, excepte a la persona que va dirigit el missatge, que s'han posat prèviament d'acord i han establert uns paràmetres per a poder codificar i descodificar el missatge. Però no ens avancem tant, pas per pas. Primer de tot, per a poder entendre què és la criptografia i com ha anat evolucionant (en les seves tècniques, principis, etc.) hem d'entendre els seus principis. La paraula codi fa referència a un mot particular de comunicació secreta, que al llarg dels anys ha perdut aquest significat. En un codi, una paraula o frase és reemplaçada per una paraula, un número o un símbol. Per exemple, quan un grup

d'amics vol fer un "botellón", volen fer servir el WhatsApp per parlar-ho però saben que la mare d'en Roger (nom completament inventat) revisa els missatges, llavors per a que ella no sospiti d'aquest "botellón" els participants d'aquesta activitat "il·legal" han acordat que faran servir el codi "xuxes" per a referir-se a l'alcohol. Aquesta colla de nois i noies acaben de posar en pràctica un dels principis de la criptografia i a més, han aconseguit que ningú sàpiga de la seva activitat "il·legal". Posant-se prèviament en contacte, acordant i canviant una paraula per una altre o una frase per una paraula, aconsegueixen que només aquells que coneixen el codi podran entendre el missatge i per a tots aquells que interceptin el missatge, com la mare d'en Roger, no entendran res. Una altre tècnica alternativa al codi és la xifra, encara més senzilla, reemplaça lletres en comptes de paraules. Per exemple, cada lletra d'una frase podria ser reemplaçada per la següent lletra de l'abecedari, de forma que A fos reemplaçada per B, B per C i així successivament. Si fem servir aquesta tècnica, el missatge **comprem millor vodka** passaria a ser **dpnqsfn njmmps wpeib**. Les xifres tenen un paper molt important, essencial, en la criptografia.

Seguint amb les definicions quan descrivim a una persona que intenta desxifrar una xifra, fem servir el terme desxifrador de codis, no és el terme més exacte ni correcte, el més precís és desxifrador de xifres. Generalment però, la criptografia és bastant fàcil d'entendre, en termes bàsics. Per exemple, el missatge abans de ser codificat, s'anomena text pla (en castellà sona millor, ¿texto llano?) i el missatge després d'haver estat codificat s'anomena text xifrat.

Una paraula que també hem de deixar molt clar des de l'inici, principalment perquè és l'antagonista de la criptografia, el **criptoanàlisi**. El criptoanàlisi és la ciència oposada a la criptografia, per tant és l'art de desxifrar criptogrames (etimològicament parlant). Els criptoanalistes s'encarreguen de donar sentit a un conjunt de paraules i símbols que aparentment no tenen sentit. Els criptoanalistes van des de lingüistes fins a matemàtics i el seu objectiu és destruir o desxifrar qualsevol tipus de codi o xifra. En el següent punt en parlarem amb més profunditat sobre la guerra entre la criptografia i el criptoanàlisi.

Et podries arribar a preguntar quina utilitat té la criptografia en la actualitat, doncs bé, la criptografia és present en el dia a dia de tots. Des de comprar per internet,

passant per enviar un missatge a un amic o fins i tot a una transacció econòmica. La criptografia és una part essencial de l'internet. Ens permet tenir connexions segures, protegir les nostres dades i assegurar que quan comprem alguna cosa no hi hagi tercers en els tràmits de pagament, per posar algun exemple. En tot el que et puguis imaginar sobre l'internet, la criptografia és present. Per tant, en aquest treball no només intentaré introduir els principis de la criptografia, sinó que en major o menor mesura intentaré explicar com funcionen les comunicacions avui en dia i fins quin punt s'està arribant. Entendrem perquè la criptografia ha estat i és essencial en la nostra societat i com la guerra entre criptografia i criptoanàlisi determina el curs de la història.

1.2 Criptografia i Criptoanàlisi

En aquest punt vull centrar-me en parlar-vos sobre l'eterna guerra que han dut a terme aquestes dues ciències.

Per la mateixa raó que la criptografia va sorgir per la necessitat de protegir les comunicacions i que la informació no caigués en mans enemigues, el criptoanàlisi va aparèixer just pel contrari, per a desxifrar aquests missatges i desvelar secrets. Aquesta batalla intel·lectual ha comportat un impacte tant en la història com en avenços científics.

Els creadors de codis han utilitzat l'enginy per a crear codis cada vegada més difícils de desxifrar i els desxifradors han inventat mètodes per a poder desxifrar aquests missatges. Hem de tenir en compte que es pot considerar que el desenvolupament dels codis és una evolució, degut a que els codis mateixos estan constantment sent atacats pels desxifradors. A la que els desxifradors estableixen un mètode per a debilitar un codi, aquest deixa de ser útil. És igual que la lluita per la supervivència, o t'adaptes i millores el teu codi, o aquest codi no evoluciona i queda en desús.

Podem fer la comparativa amb el regne animal: per exemple amb les papallones abedules (Biston betularia[1]). Aquestes papallones eren blanques, per a camuflar-se

[1] Communment coneguda com papallona del bedoll, les *Biston betularia*s son un dels exemples més emblemàtics de la teoria de l'evolució.

FIGURA 1: Imatge d'una Biston betularia.

amb els arbres i protegir-se dels depredadors. Quan va arribar la industrialització, a la industrialització li direm avenç científic (un nou mètode per a desxifrar codis), el medi va canviar, l'escorça dels arbres va canviar a negre, degut al fum de les fàbriques. Per tant, les papallones ja no estaven segures dels seus depredadors, direm que els depredadors són els criptoanalistes. Arriba la industrialització (avenç científic per a desxifrar), debilita la protecció de les papallones (fa vulnerable al codi) i els depredadors se les mengen (els criptoanalistes aprofiten aquesta debilitat i poden desxifrar els missatges). Les papallones (codis) tenen dues opcions, o els seus successors evolucionen (per selecció natural) i neixen sent de color negre, és a dir, evolucionen (el codi evoluciona i venç a la debilitat) o les papallones acabaran morint totes (el codi quedarà en desús). Ja sé que la selecció natural no funciona ven bé així, però ajuda a explicar el concepte.

Una vegada aclarit aquesta guerra contínua entre criptògrafs i criptoanalistes, podem entendre que aquesta batalla ha generat molts avenços científics, tan tecnològics com matemàtics. No deixa de ser com una guerra d'un producte en un mercat, lluites amb la competència per a millorar el teu producte, ajustes preus de producció, abaixes els preus de venda, investigues per a millorar-lo, etc. Doncs en el món de la criptografia passa el mateix, lluiten entre ells, en el cas de la criptografia lluita per aconseguir un sistema o mètode d'encriptació indesxifrable i el criptoanàlisi per aconseguir el mètode que pugui desxifrar qualsevol encriptació. És per això que comunament s'anomena la batalla sense fi.

Durant el curs dels segles la criptografia ha tingut segles d'esplendor, on havien descobert una xifra o codi que semblava indesxifrable, per tant la criptografia tenia l'avantatge sobre el criptoanàlisi, i també hi ha hagut èpoques on els mètodes

criptoanalítics eren molt superiors als xifrats, per tant anaven un pas per davant i tenien avantatge, era una època on els secrets entre estats pràcticament no existien.

2. La història de la criptografia

Des de l'Antiga Grècia fins l'actualitat, veurem com va començar i sobretot com ha anat evolucionant al llarg del temps i pels diferents territoris. Com ha afectat a les diverses civilitzacions, quin impacte ha tingut i l'enginy que han tingut els criptògrafs i criptoanalistes arreu del món. El fet que hagi decidit explicar la història de la criptografia no és més que una excusa literària, utilitzo la història i els diferents fets històrics per a explicar l'evolució de la criptografia.

A més, al llarg dels segles veurem quina de les dos ciències portava l'avantatge en vers l'altra i quins efectes va provocar aquest avantatge.

2.1 L'evolució de l'escriptura secreta

Les primeres tècniques criptogràfiques es remunten a l'any 400 a.C. La primera tècnica que va sorgir en mig d'una guerra, la segona guerra mèdica. Xerxes, el rei de reis de l'imperi Persa, tenia planejat venjar la derrota del seu pare, volia castigar a Atenes per la revolta a Jònia i la victòria de Marató. Tal és així que va preparar una gran expedició per envair i destruir als atenesos. El problema per a les polis gregues és que Xerxes havia estat preparant aquesta campanya militar durant quatre anys i ningú excepte Demaratus ho sabia. Demaratus era un grec que havia sigut expulsat de Grècia, concretament havia estat rei d'Esparta, però per culpa d'una història molt llarga que no té importància havia estat expulsat de la seva pàtria i va buscar refugi a Pèrsia. Resumint molt, Demaratus va ajudar als grecs a guanyar la guerra.

La tècnica que va utilitzar Demaratus per a la comunicació secreta, no és més que la ocultació del missatge. Aquest tipus de comunicació secreta, aquella que s'aconsegueix mitjançant l'ocultació de l'existència d'un missatge, es coneix com a **esteganografia**. Etimològicament ve del derivat grec *steganos*, significa ocult, i *graphos*, que significa escriptura.

Des de la invenció de la esteganografia, inimaginables mètodes s'han fet servir. Per exemple, en la segona guerra mundial, hi havia una clara necessitat d'enviar missatges sense que l'enemic pogués interceptar-los. Per això la esteganografia va passar a un primer pla. La tècnica més utilitzada va ser la **tinta invisible**, ja descoberta en el segle I per Plinio el Vell, que explicava com la planta Tithymalus podia fer-se servir com a tinta invisible. A l'assecar-se es torna transparent, però si calentes la tinta suaument es crema i es torna de color marró. Això és degut a que molts fluids orgànics contenen molt de carboni i es cremen fàcilment. Un altre exemple és el **micropunt alemany**, una tècnica fotogràfica per a reduir una fulla sencera al tamany d'una microfitxa d'un mil·límetre de diàmetre. Per l'ull nu això era impossible de detectar i així és com aconseguien els espies alemanys passar la informació.

FIGURA 2: Exemple de micropunt alemany.

El llarg ús de l'esteganografia demostra que ofereix un cert nivell de seguretat, però té una debilitat molt gran. Si registren al missatger i troben el missatge, la informació és revelada en aquell mateix instant. La intercepció del missatge compromet immediatament tota la seguretat. És a dir que si algú és dediqués a registrar al missatger de totes les formes i tècniques que es coneixen d'ocultació del missatge, inevitablement el missatge quedaria revelat.

És per aquesta raó que paral·lelament, es va produir l'evolució de la criptografia, on l'objectiu principal no és amagar el missatge, sinó ocultar el seu significat. D'aquesta manera l'emissor i el receptor es posen d'acord seguint un procés de codificació, aconseguint així que el receptor podrà invertir el procés de codificació i fer que el seu missatge sigui inintel·ligible. El principal avantatge envers la esteganografia és que si el missatge cau en mans enemigues, aquest missatge segueix sent incomprensible per a algú que no coneix el protocol que han seguit emissor i

receptor. A l'enemic li resultarà pràcticament impossible recrear el missatge original a partir d'aquest text xifrat.

Encara però, ens falta tocar una alternativa per a la comunicació secreta, que més que alternativa és una unió. Sabem que la esteganografia i la criptografia són independents, però també és possible ocultar i codificar un missatge al mateix temps, augmentant la seguretat exponencialment. Si tornem al micropunt d'abans, la tècnica alemana esteganogràfica per a ocultar el missatge, podríem afegir un sistema de seguretat encara major. Si el missatge inicial el codifiquem, i després utilitzem la tècnica fotogràfica, resultarà un missatge codificat d'un mil·límetre de diàmetre. No només haurem ocultat el missatge sinó que també haurem amagat el significat del missatge. En aquests casos que combinem la criptografia amb la esteganografia, els aliats podien interceptar i bloquejar les comunicacions entre els espies alemanys, però no aconseguiren mai esbrinar la informació en aquells missatges. Això si, la criptografia és més poderosa i segura perquè evita que si la informació cau en mans enemigues, encara que interceptin el missatge, aquest seguirà sent incomprensible.

2.1.1 Les branques de la criptografia

La criptografia pot ser dividida en dos branques, la substitució i la transposició

La transposició

En la transposició les lletres del missatge es col·loquen d'una altra manera, generant un anagrama. Com quan a l'escola canviàvem d'ordre les lletres d'una paraula i ens pensàvem que ningú podia saber quina era la paraula original. Al contrari del que ens pensàvem, una paraula amb poques lletres té un número molt limitat de possibilitats, la qual cosa provoca que la seguretat sigui pràcticament nul·la. Si tenim una paraula amb tres lletres, només hi ha sis possibles permutacions però només que afegim una lletra més el nombre de possibles permutacions augmenta factorialment. Amb la paraula **curt**, tenim 24 possibles permutacions. És evident que amb poques lletres la seguretat del mètode de transposició no és gaire segura, però només que augmentem una mica el tamany del missatge, les permutacions augmenten molt. **Per exemple, avui he menjat paella dolenta**. La frase anterior

conté només 35 lletres, algunes lletres es repeteixen, per tant existeixen 1.853.866.257.150.935.048.845.824.000.000 permutacions possibles.

$$RP_n^{a,b,c\ldots} = \frac{n!}{a!\cdot b!\cdot c!}$$

$$RP_{35}^{a,d,e,n,i,j,l,m,n,o,p,r,t,u,v,x} = \frac{35!}{8!\cdot 5!\cdot 4!\cdot 3!\cdot 2!\cdot 2!\cdot 2!} = 185386625715093504884582400000$$

Llavors ens adonem que la quantitat de possibilitats en un petit missatge és immens. Tenim un problema però, la transposició crea un anagrama molt complicat de resoldre, si les lletres estan de manera aleatòria serà tant difícil per al receptor com per l'enemic resoldre l'anagrama. Per a que la transposició sigui viable necessitem que emissor i receptor es posin d'acord en la utilització d'un sistema senzill de codificació i descodificació, però que a la vegada sigui segur si cau en mans enemigues.

Una transposició molt utilitzada, inclús els més menuts la fan servir, és la transposició de **riel**. Consisteix en escriure el missatge en dos línies diferents. Una vegada el missatge hagi estat escrit en aquestes dos línies la segona línia s'adjunta al final de la primera, creant el missatge codificat final. Per exemple

MAMA AVUI NO HE RECOLLIT LA HABITACIÓ, NO EM CASTIGUIS PLIS

MMAUNHRCLILHBTCOOMATGIPI

AAVIOEEOLTAAIAINECSIUSLS

MMAUNHRCLILHBTCOOMATGIPI AAVIOEEOLTAAIAINECSIUSLS

El receptor del missatge pot recuperar el missatge original, l'únic que ha de fer és invertir el procés realitzat per a codificar el missatge. Si volguéssim complicar la transposició, podríem fer servir la xifra de riel de tres línies, s'escriu el missatge inicial en tres línies en comptes de dues, o també podries canviar de línia cada dos o tres lletres.

Un altre tipus de transposició és el primer aparell criptogràfic militar de la història, la Escítala. Ens hem de remuntar fins el 400 aC per arribar al origen d'aquesta tècnica tan antiga. Principalment era utilitzada pels militars espartans per a enviar-se missatges secrets. Els sistema era molt senzill, tan emissor com receptor havien de tenir dues vares de fusta del mateix diàmetre, i sobre aquesta vara es posava un cinturó de cuir. Llavors, una vegada la tira de cuir estava enrotllada, el missatge s'escrivia longitudinalment, és a dir d'esquerra a dreta (perquè escrivien d'esquerra a dreta). Una vegada escrit el missatge, la tira de cuir es desenrotllava i quedava un missatge sense cap tipus de sentit. Quan aquesta tira de cuir arribava al receptor, simplement havia d'enrotllar el cinturó en la vara de fusta, i el missatge es revelava. Per a que el missatge sigui descodificat, la tira de cuir s'ha d'enrotllar en una vara de fusta del mateix diàmetre que la utilitzada per l'emissor, per molt que un enemic sabés quina tècnica havia utilitzat, hauria d'encertar amb el diàmetre, perquè sinó fos així el missatge que apareixeria seria o bé un sense sentit o un diferent a l'original.

FIGURA 3: Imatge d'una escítala.

La substitució

En la substitució cada lletra és substituïda per una lletra diferent. En la transposició cada lletra manté la seva identitat però canvia de posició, en canvi en la substitució, cada lletra canvia la seva identitat però no de lloc, manté el lloc original. La transposició i la substitució són complementàries.

L'exemple més antic de substitució el trobem al Kamasutra, escrit en el segle IV per Brahmín Vatsyayana, però que està basat en manuscrits molt més antics, del segle IV aC. El Kamasutra recomana que les dones han d'estudiar diverses arts, concretament 64. L'art més curiós és el número 45, l'art de l'escriptura secreta, per a poder parlar amb els seus amants sense que ningú s'assabentés. La tècnica que recomana el llibre és emparellar a l'atzar les lletres del abecedari.

El primer ús de substitució per a usos militars que trobem documentat és *La guerra de les Galies*, de Juli Cèsar. Aquest és el primer document on s'explica que Cèsar va canviar les lletres romanes per gregues, xifra de substitució. Però el llibre on s'explica molt extensament una xifra de substitució que va utilitzar molt freqüentment, és *en les Vides dels Cèsars LVI*, de Suetoni. La tècnica que utilitzava era ben senzilla, Cèsar simplement substituïa cada lletra del missatge per la lletra que estava tres llocs al davant en l'abecedari. Per a agilitzar aquest procés, feia servir dos alfabets, el primer alfabet pla, el que s'utilitza per a escriure el missatge original, i l'alfabet xifrat, les lletres que substitueixen l'alfabet pla. Aquesta tècnica de substitució en l'alfabet xifrat en la qual es mou cada lletra tres llocs, s'anomena **la xifra del Cèsar**. Fem un petit parèntesi per a recordar que una xifra és aquella substitució criptogràfica on cada lletra és substituïda per una altre lletra o bé, un símbol.

Per a fer-nos a la idea de la quantitat de possibilitats que hi ha, si canviem ordenadament l'alfabet i diem que un alfabet pot ser qualsevol combinació de l'alfabet pla (l'original) el número de xifres que creem és encara més gran que la xifra de Cèsar, unes

400.000.000.000.000.000.000.000.000 possibles combinacions, xifres diferents.

Si volem parlar d'una codificació general, normalment parlem de l'ús d'un **algoritme**, que no és més que un conjunt de processos o regles per a resoldre una codificació en particular. En el cas de la xifra del Cèsar l'algoritme substitueix cada lletra de l'alfabet pla per una de l'alfabet xifrat. Un altre terme important és **la clau**, que és aquella que defineix, en aquest cas, quin alfabet xifrat hem de fer servir. Per molt que sabéssim quin algoritme fem servir, si no tenim la clau, en aquest cas l'alfabet xifrat que hem fet servir, no es podrà desxifrar el missatge. Aquest principi és molt important perquè la seguretat no depèn de les regles que seguim, sinó de la clau. A més de la clau, també ha de tenir l'algoritme una amplia gama de possibles claus potencials. És a dir, si una persona utilitza la xifra del Cèsar, només hi ha 25 claus potencials. Si l'enemic intercepta el missatge i creu que utilitzes la xifra de Cèsar, només haurà de comprovar les 25 possibilitats, un procés relativament ràpid. Però si en comptes de limitar-nos ha fer la xifra de Cèsar i utilitzem un algoritme que permet que l'alfabet xifrat sigui qualsevol combinació de l'alfabet pla, les possibles claus

potencials són les mateixes que el número[2] del principi de la pàgina, moltes. Si hi ha moltes claus potencials, per molt que sàpiguen l'algoritme que utilitzem serà pràcticament impossible que desxifrin el missatge.

Aquesta és una de les avantatges d'aquesta xifra, és molt fàcil de posar en pràctica i el nivell de seguretat que ofereix és molt elevat. A més, per a l'emissor és fàcil definir la clau, ha de determinar l'ordre de les 26 lletres de l'alfabet xifrat i per a l'enemic li serà impossible. La simplicitat de la clau també és molt important, perquè l'emissor i el receptor han de compartir la clau, i contra més fàcil sigui, més difícil serà que hi hagi malentesos.

Encara que determinar les 26 lletres de l'alfabet xifrat sigui relativament fàcil, hi ha una manera molt més senzilla de crear una clau i a canvi sacrifiques una petita reducció dels números de claus potencials. En el sistema, en comptes de combinar a l'atzar les lletres del alfabet pla, l'emissor utilitza una frase o paraula clau. Per exemple, per a utilitzar la frase **RON COLA** hem de treure els espais i les lletres repetides (**RONCLA**), i després utilitzar-ho com el principi de l'alfabet xifrat. La resta de l'alfabet xifrat l'omplirem seguint l'ordre de l'alfabet començant per on acaba la frase clau.

Alfabet pla	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabet xifrat	R	O	N	C	L	A	B	D	E	F	G	H	I	J	K	M	P	Q	S	T	U	V	W	X	Y	Z

La gran avantatge de fer servir la frase clau radica en la fàcil memorització de la paraula o frase i de l'alfabet xifrat. Gràcies a això la xifra de substitució va dominar l'art de l'escriptura secreta durant més de deu segles (I-X aprox.). Com que cap desxifrador havia aconseguit trobar alguna debilitat, la xifra no li havia fet falta evolucionar, una de les raons perquè durés tan de temps. Inclús alguns desxifradors consideraven que era indesxifrable. Però tot té un final i gràcies als avenços matemàtics a Orient, es va aconseguir un mètode per a desxifrar aquests missatges en qüestió de minuts.

[2] 400.000.000.000.000.000.000.000.000 possibles combinacions.

2.1.2 Els criptoanalistes àrabs

Ens hem de remuntar al segle IX, a l'imperi Islàmic. Des de feia uns quants segles la ciència i l'art estaven en augment, creant així una base científica molt forta per als futurs científics, garantint l'èxit d'alguns. Una de les causes principals per a la riquesa de la cultura islàmica es degut a l'organització que hi havia en aquella època. Els califes van centrar els seus esforços en crear una societat organitzada i que pogués garantir la supervivència durant molts segles, a més de ser ja una societat rica. En comptes de fer com els seus successors, van abaixar els impostos per a que hi hagués un creixement en la industria, petits negocis i el comerç en general. Tot això se sustentava gràcies a una comunicació segura, fent servir la criptografia. Els governants utilitzaven molt sovint l'alfabet xifrat per a les seves comunicacions diàries. En general, feien servir la xifra de substitució **monoalfabètica**, aquella xifra de substitució on l'alfabet xifrat consisteix de lletres o símbols, o els dos alhora.

Una altre concepte molt important que es va inventar aquí és el criptoanàlisi. A l'igual que xifraven missatges també els desxifraven i aquests mateixos criptoanalistes àrabs van ser els que van trobar un mètode en la xifra de substitució monoalfabètica.

El primer gran avanç criptoanalític esdevé d'unes conclusions que van arribar els teòlegs de l'islam. Es van dedicar a estudiar la etimologia, la semàntica i la consistència de patrons lingüístics. Amb aquest últim estudi es van adonar que hi ha algunes lletres que són més utilitzades que unes altres. Per exemple, en àrab les lletres **a** i **1** són les més freqüents, mentre que la **q** és una lletra molt poc utilitzada.

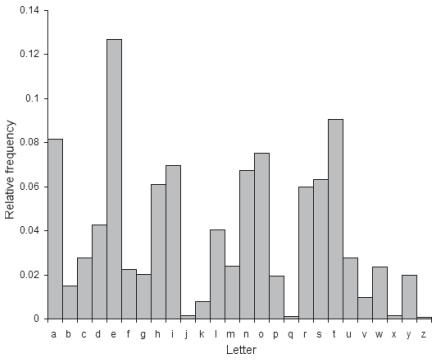


FIGURA 4 [3]

[3] Gràfica que ens mostra l'abundància de l'utilització de les lletres en la llengua anglesa.

Encara que els estudiosos religiosos no ho sabien, van donar amb el primer gran avanç cap al criptoanàlisi. No se sap qui va ser el primer adonar-se de que la variació en la freqüència en les lletres podria ser la clau per a desxifrar les xifres. Tot i això, el primer escrit que es coneix d'aquesta tècnica és del científic del segle IX Abú Yusuf Yaqub ibn Ishaq ibn Sabbah ibn Omran ibn Ismail al Kindi, també conegut com **el filòsof dels àrabs**. El tractat més important que va escriure es titula *El desxiframent de missatges criptogràfics* i no va ser descobert fins el 1987, a Istanbul.

En el llibre apareix una breu explicació que resumeix com era la tècnica del revolucionari sistema criptoanalític:

Per a resoldre un missatge xifrat, si sabem en quina llengua està escrita, hem de trobar un text pla diferent, escrit en la mateixa llengua i que tingui una extensió aproximada d'una fulla, com a mínim, i després contar quantes vegades apareix cada lletra. Aquella lletra que estigui més vegades l'anomenem *primera*, a la segona en freqüència *segona* i així successivament fins haver acabat amb totes les lletres del text pla. Hem de repetir el procés amb el text que volem resoldre, el text xifrat. Els símbols que apareguin amb més freqüència els substituïm amb la forma de la lletra *primera* del text pla, el següent símbol amb més freqüència els substituïm per la forma de la lletra *segona*, i així amb tots els símbols restants.

Per exemple, en castellà, la lletra més comuna és la **e**, seguida de la **a**, després la **o**, la **s** i així successivament. Després, analitzem el text xifrat i determinem la freqüència de cada lletra i/o símbol. Per exemple, si la lletra més freqüent és la F, és probable que fos substituïda per la e. La segona lletra més comuna és la X, per tant és probable pensar que la X sigui en realitat la a, i així successivament. Aquesta tècnica es coneix com **anàlisi de freqüència**, on ens demostra que no és necessari revisar els bilions de claus possibles sinó que podem revelar el significat del missatge codificat analitzant simplement la freqüència dels caràcters en el text xifrat.

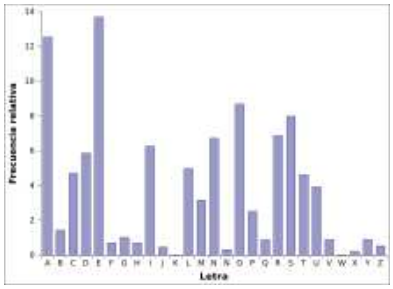


FIGURA 5: Aquesta gràfica ens mostra la freqüència de les lletres en la llengua castellana.

Pot passar a vegades que aquesta tècnica no funciona, bé pot ser perquè el text és massa petit, o perquè el text simplement no correspon amb l'estàndard de freqüència. Per exemple, Georges Perec va escriure *La Disparition*, una novel·la de 200 pàgines on no apareix cap paraula amb la lletra e. En el cas que aquest llibre fos codificat amb una xifra de substitució monoalfabètica, quan s'intentés desxifrar seguint la tècnica de l'anàlisi de freqüència, aquest mateix anàlisi es veuria entorpit per la manca d'aparició de la lletra e, que en el cas de l'espanyol és la lletra més freqüent, igual que en l'anglès.

2.1.3 El renaixement a Occident

Mentre que els àrabs ja havien establert les primeres tècniques de criptoanàlisi, els europeus encara estaven barallant-se amb les bases de la criptografia. Entre els anys 800 i 1200, els àrabs eren els reis de l'escriptura secreta i Europa seguia estancada en L'Edat Mitjana.

Només els monestirs es preocupaven de l'estudi de l'escriptura secreta, ja que els monjos buscaven significats ocults en la bíblia. Aquesta intriga dels monjos era deguda a que a l'Antic Testament tenia parts que havien estat criptografiades. A vegades, es feia servir la xifra de substitució hebrea, coneguda com **Atbash**. Consisteix bàsicament en agafar cada lletra i anotar el número de llocs que està respecte al principi del alfabet i substituir-la per la lletra que es troba a un mateix nombre de llocs respecte el final de l'alfabet. En català per exemple, la **a** passaria a ser la **z**. Es creu que la principal intenció de fer servir aquesta xifra era per afegir misteri, no per a ocultar el significat.

Gràcies als monestirs i a aquesta intriga, es va despertar l'interès per la criptografia d'una forma seriosa. El primer llibre europeu on es descriu l'ús de la criptografia és en *La Epístola sobre les obres d'arts secretes i la nul·litat de la màgia*, escrit per Roger Bacon, un monjo del segle XIII.

Ja en el segle XIV l'ús de la criptografia s'havia estès notablement. Els científics i els alquimistes la utilitzaven per a mantenir en secret els seus descobriments.

En el segle XV, la criptografia europea era ja una indústria. El renaixement de les arts i les ciències va ajudar al desenvolupament de la criptografia. Per l'altre banda, la política es va veure en la posició perfecte per aprofitar-la en una millor

comunicació secreta. A Itàlia, va ser el primer lloc on es van crear les oficines de xifres, per a garantir la seguretat en els seus missatges, ja que a Itàlia, la majoria de ciutats eren ciutats-estats independents i cada una d'elles tenia com a objectiu superar estratègicament a la resta de ciutats-estats. Alhora que la criptografia s'estava convertint en una eina diplomàtica, el criptoanàlisi també començava a sorgir a Occident. Els diplomàtics acabaven de familiaritzar-se amb les habilitats requerides per a la comunicació segura i ja hi havia persones que tractaven de destruir aquesta seguretat.

Es creu que es probable que el criptoanàlisi fos descobert independentment a Europa, però també existeix la possibilitat que fos importat directament del món àrab.

El primer gran criptoanalista conegut a Europa és Giovanni Vincenzo Soro, secretari de Xifres de Venècia, a partir del 1506. Ràpidament la seva reputació va augmentar per la seva habilitat de desxifrar missatges. Fins i tot, el Vaticà va demanar-li en diverses ocasions que desxifrés missatges. El papa Clement VII va enviar-li dos missatges xifrats i els dos van ser retornats havent estat desxifrats amb èxit.

Un altre nom conegut és el del criptoanalista Philibert Babou, criptoanalista del rei Francesc I de França. Cap al final del segle XVI, els francesos van consolidar la seva habilitat desxifradora, i per tant estaven al capdavant del criptoanàlisi europeu, amb la arribada de François Viéte, que obtenia un plaer especial desxifrant les xifres espanyoles. Els criptògrafs espanyols es van tornar bojos quan van descobrir que per als francesos els seus missatges eren transparents. En poc temps, més de mitja Europa llegia els missatges espanyols sense dificultat alguna, els criptògrafs espanyols es van convertir en la vergonya i la riota d'Europa.

La vergonya d'Espanya també venia donada per la guerra entre els criptògrafs i criptoanalistes. Era una època on els criptògrafs encara pensaven que era segura la xifra de substitució monoalfabètica i els criptoanalistes començaven a utilitzar l'anàlisi de freqüència. Els països que sí eren conscients de les debilitats de la xifra de substitució monoalfabètica, tenien moltes ganes de trobar una xifra millor, per poder protegir els seus secrets.

Una de les millores més significatives a aquesta xifra va ser la invenció de **nuls**, símbols o lletres que no codifiquen per res, és a dir, no eren substituts de lletres del

missatge original sinó que eren simples buits per a despistar als criptoanalistes. Per exemple, puc substituir cada lletra per un número entre 1 i 99, deixant 73 números que no representen res, l'emissor simplement no ha de fer cas a aquests números perquè ja sap que no codifiquen a res. A vegades també **daletrexavbanh malametn pherr hah desaqkilivrar lhaz frheqwensyaz dehl texztw**. Fent servir els nuls i escriure malament les paraules pensaven que serien capaços de despistar als criptoanalistes.

Una altra tècnica que feien servir era l'ús del codi. Si bé sabem que una xifra de substitució és aquella que substituïm una lletra per una altre, en un codi substituïm una paraula per una lletra o símbol. Si per exemple vull quedar amb els meus amics per a fer un "botellón" sense que ningú ho sàpiga, suposant que ens llegeixen els missatges, sobretot per la mare d'en Roger, Podem utilitzar els codis per a parlar entre nosaltres.

Ens hem posat d'acord i tenim aquest petit abecedari per a parlar amb clau:

Quedem= T	Darrere escoles = "	A les 22 = @	Arribo tard = S
Botellón= V	A l'església = %	A les 23 = !	Al parc = (

Amb aquesta petita mostra podríem mantenir ja una conversació i només nosaltres que sabem els significats d'aquests codis entendrem el missatge. Si per exemple vull posar pel grup que quedem per fer "botellón" a les deu al darrere de les escoles, escriuré: **T-V-"-@**.

És veritat que els codis ofereixen un nivell molt gran de seguretat però tenen dos defectes molt importants. La flexibilitat dels codis per a poder escriure qualsevol missatge radica en el número de codis que tinguis. Si jo vull escriure qualsevol tipus de missatges hauré de crear un llibre amb totes les paraules i codis que corresponen a cada una d'elles, hauré de fer un diccionari i això requereix molt de temps i esforç, no compensa. L'altre gran inconvenient és que si aquest llibre de codis cau en mans enemigues les conseqüències són catastròfiques. En canvi, si faig servir una xifra de substitució una vegada l'emissor i receptor s'hagin posat d'acord amb les 26 lletres de l'alfabet xifrat, podran codificar qualsevol missatge.

Tots els esforços dels criptògrafs per a despistar als criptoanalistes no van servir de gaire. La majoria van ser capaços de desxifrar els missatges codificats. Gràcies a la

seva habilitat es va crear un corrent constant de secrets i informació revelada, afectant en gran mesura a la història d'Europa durant aquesta època.

2.2 Le chiffre indéchiffrable

Durant segles, la xifra de substitució havia sigut la més utilitzada tant per la facilitat de fer-la servir com perquè era suficientment segura per a guardar els secrets. Però amb la invenció de l'anàlisi de freqüència, aquesta seguretat havia estat completament destruïda. Pel que fa la guerra entre el criptoanàlisi i la criptografia, estaven guanyant "per bastant" els criptoanalistes. Encara que hi havia una necessitat imminent de recuperar la seguretat en les comunicacions, no va ser fins al final del segle XVI que sorgí aquesta xifra, coneguda com la xifra indesxifrable (spoiler: no és indesxifrable). Els orígens d'aquesta xifra comencen amb l'erudit León Battista Alberti, nascut al 1404 a Florència. Encara que fos conegut com a un molt bon arquitecte i escriptor d'un dels primers llibres sobre arquitectura, es sap que en algun moment de la dècada dels 60, el seu amic Leonardo Dato l'introduí en el magnífic món de l'escriptura secreta. Com ja sabem, la xifra de substitució monalfabètica només necessita un alfabet xifrat per a codificar el missatge, doncs bé, Alberti proposava utilitzar dos o més alfabets xifrats, aconseguint despistar als criptoanalistes i augmentar la seguretat en els missatges.

Resumint molt, la seva tècnica consisteix en tenir dos alfabets xifrats i xifrar el missatge alternant els alfabets. Encara que havia donat amb la solució del mil·lenni, no va ser capaç de desenvolupar el seu mètode i convertir-lo en una descodificació plenament formada.

Els encarregats d'acabar de formar el mètode van ser Johannes Trithemius, Giovanni Porta i finalment **Blaise de Vigenère**, un diplomàtic francès nascut el 1523. En una missió diplomàtica de dos anys de durada a Roma va conèixer el treball Alberti, Johannes i Giovanni. Encara que en la seva feina la criptografia era poc habitual, no va ser fins que va anar a Roma que es va aficionar profundament pel món criptogràfic. Als 39 anys va decidir

jubilar-se i dedicar la resta de la seva vida a l'estudi de l'escriptura secreta. Combinant les idees dels seus antecessors, va aconseguir una nova xifra, una xifra molt poderosa![4]

Encara que els tres autors anomenats anteriorment van fer una contribució essencial, va ser Vigenère qui la va unificar i la va desenvolupar de forma definitiva. Es coneix com **la xifra Vigenère**, la innovació d'aquesta nova xifra recau en la utilització de 26 alfabets xifrats diferents per a xifrar un missatge. Quan es vol fer servir aquesta xifra, el primer pas és fer un quadre de Vigenère (el quadre el pots trobar en la següent pàgina). Es tracta, com podem observar en la taula, d'un alfabet pla seguit de 26 alfabets xifrats, cada un començant amb la lletra següent a l'anterior. La línia 1 representa un alfabet xifrat de canvi de Cèsar d'una posició, la línia 2 representa un alfabet xifrat de canvi de Cèsar de dos posicions, i així successivament. Les lletres de dalt en minúscula representen les lletres de l'alfabet pla, per tant podria codificar cada lletra del text pla per 26 alfabets xifrats diferents. Per exemple, si volem codificar la lletra **g**, si fem servir l'alfabet 4 codificarà per **K** però si fem servir l'alfabet xifrat 15 codificarà per **U**. Si l'emissor només fa servir un alfabet xifrat llavors realment estarà utilitzant el canvi de Cèsar, li proporcionarà una seguretat molt pobre. Per a exprimir la xifra Vigenère hem de fer servir una línia diferent del quadre Vigenère per a xifrar les diferents lletres del missatge. Per exemple, l'emissor podria xifrar la primera lletra per l'alfabet 5, la segona pel 2, la tercera lletra pel 22 i així successivament.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

FIGURA 7 [5]

[4] FIGURA 6: La imatge ens mostra la figura de Blaise de Vigenère

[5] Taula amb tots els alfabets per a la utilització de la xifra Vigenère.

Per a que el receptor pugui desxifrar el missatge, ha de saber quin alfabet s'ha fet servir per a codificar cada lletra, per tant han d'establir un patró que s'aconsegueix utilitzant una paraula clau. Per a poder entendre com funciona el procés de la paraula clau desxifrarem **necessitem més gels per aquesta nit**, utilitzant la clau **FESTA**. El primer pas és lletrejar la clau a sobre del missatge que volem xifrar, repetint la clau les vegades que faci falta. Comencem a xifrar el missatge, la primera lletra, **n**, primer hem de identificar quina lletra de la paraula clau li correspon, la F, que alhora hi ha una línia particular en el quadre Vigenère que comença per la lletra F, la línia 5, llavors aquesta línia servirà per a codificar la lletra **n** del text pla. Si mirem a la taula, podem observar que en la línia 5 la lletra que codifica per **n** és S, la **n** del text pla és representada per la S en el text xifrat. Per a codificar la segona lletra del missatge, en aquest cas la **e**, hem de fer exactament el mateix. Mirem quina lletra clau li correspon, en aquest cas la E que correspon a la línia 4. Observem que la lletra que codifica a **e** en la línia 4 és I, Per tant, la lletra **e** és representada per I en el text xifrat. Si ens fixem en la desena lletra, la **m** de la paraula més, i en la lletra clau que li correspon, la E, haurem de codificar la lletra per l'alfabet xifrat de la línia 4, que en aquest cas la **m** és representada per Q en el text xifrat. Haurem de repetir el procés fins arribar a la última lletra del missatge.

Clau	F	E	S	T	A	F	E	S	T	A	F	E	S	T	A	F	E	S	T	A	F	E	S	T	A	F	E	S	T	A
Text pla	n	e	c	e	s	s	i	t	e	m	m	e	s	g	e	l	s	p	e	r	a	q	u	e	s	t	a	n	i	t
Text xifrat	S	I	U	X	S	W	M	L	X	M	R	I	K	Z	E	Q	W	H	X	R	F	U	M	X	S	Y	E	F	B	T

La gran avantatge de la xifra Vigenère és que resulta indesxifrable utilitzant l'anàlisi de freqüència explicat anteriorment. En el text xifrat pot aparèixer la mateixa lletra del text pla representada per diferents lletres, o tenir diferents lletres en el text pla que codifiquen per la mateixa lletra en el text xifrat. En el nostre exemple la primera lletra del text xifrat és la S, que representa la **n** del text original, la cinquena lletra també és la S però en aquest cas representa la s del text original. Una altre cas és amb les dos **m** del text original, la primera és representada en el text xifrat per la M però la segona és codificada per la R. Aquestes propietats que té la xifra Vigenère li proporcionen un clar problema al criptoanalista. El fet de que una lletra apareix diverses vegades en el text xifrat i pugui representar en cada cas una lletra diferent del text original, això li genera una ambigüitat tremenda al criptoanalista.

Podríem pensar que gràcies a la seguretat que ens proporciona, fos natural que s'utilitzés arreu del món i fos ràpidament implementada en les comunicacions, però la veritat és molt diferent. Aquest sistema aparentment perfecte, es mantindrà ignorat durant els dos segles següents.

2.2.1 Substitució monoalfabètica i polialfabètica

Les formes tradicionals de xifra de substitució són la monoalfabètica, aquelles que només utilitzaven un alfabet xifrat per a xifrar cada missatge. La xifra Vigenère en canvi, pertany a la **substitució polialfabètica**, perquè utilitza diversos alfabets xifrats en cada missatge. Aquesta propietat de la substitució polialfabètica és on radica la seva força i seguretat, però també fa que sigui molt complicada d'utilitzar. Només pel fet de l'esforç addicional requerit per a fer-la servir, va provocar que la majoria no la utilitzés. Això també és degut a que les necessitats del segle XVII per a enviar missatges xifrats era més que suficient la xifra de substitució monalfabètica. Era fàcil d'utilitzar i segura envers gent que no tenia coneixements de criptoanàlisi. Podríem pensar que per a les comunicacions militars llavors si van fer servir la xifra de substitució polialfabètica, però la veritat és que es van negar a fer-la servir perquè una de les prioritats en les comunicacions militars és la velocitat i simplicitat en els missatges, i aquesta xifra clarament no complia cap dels dos requisits.

Els criptògrafs van pensar que en alguna xifra diferent per a fer servir en les comunicacions militars, una de les opcions era la xifra homofònica. En la xifra homofònica cada lletra és reemplaçada per una varietat de substituts, on el número de substituts és proporcional a la freqüència de la lletra. Per exemple, en l'anglès la lletra **a** és aproximadament el 8 per cent de totes les lletres escrites, per tant hauríem de fer servir 8 tipus diferents de lletres o símbols diferents. La raó perquè es fa això és perquè al final de cada codificació cada símbol constituirà el 1 per cent del text codificat. L'objectiu principal de la xifra homofònica és preservar l'equilibri dels símbols del text xifrat.

Es pensava que aquesta xifra podria arribar a ser segura, però aquest tipus de text encara té moltes pistes útils per al criptoanalista. Per exemple, cada lletra d'un idioma té personalitat, determinada per la seva relació amb les altres lletres, i per molt que canviem la freqüència i l'equilibrem els trets encara es poden veure. Si fem

servir l'anglès, una de les lletres amb personalitat més forta és la **q**, que només apareix seguida de la lletra **u**. Si busquem la **q** en el nostre text xifrat, el primer que hauríem de saber és que com que la **q** representa el 1 per cent aproximadament, és probable que només estigui substituïda per una lletra o símbol. I si sabem que la **u** representa el 3 per cent, voldrà dir que estarà substituïda per 3 lletres o símbols diferents. L'únic que haurem de fer és buscar un símbol que només estigui seguit per tres símbols en concret, llavors seria raonable pensar que aquest símbol representa la lletra **q** i els altres tres representen la **u**.

Una xifra homofònica pot semblar similar a una xifra polialfabètica, però existeix una diferència molt gran, la xifra homofònica és en realitat un tipus de substitució monoalfabètica. Una lletra del text original pot ser representada per diversos símbols, però cada símbol només pot representar a una lletra. En canvi, en una xifra polialfabètica, una lletra del text original també pot ser representada per diferents símbols, però aquests símbols també representen altres lletres diferents al llarg del text xifrat.

Gràcies a la alteració de la xifra monoalfabètica, com la xifra homofònica, van permetre poder xifrar de manera segura.

2.2.2 Les cambres negres

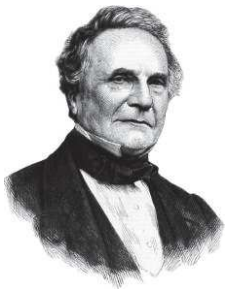
A partir del segle VIII el criptoanàlisi va començar a industrialitzar-se, amb equips governamentals que treballaven per a desxifrar la majoria de missatges xifrats que arribaven als seus territoris, aquests centres d'intel·ligència s'anomenaven cambres negres. Cada estat europeu tenia la seva Cambra negra.

Treballaven de manera molt rigorosa, perquè era essencial que les activitats no interrompessin el funcionament del servei postal. Per exemple a Viena, les cartes que devien ser entregades a les diferents ambaixades de Viena primer eren enviades a la cambra negra, on arribaven a les set del matí. Els secretaris fonien els segells de lacre i un equip de estenògrafs treballava paral·lelament per a fer còpies idèntiques de les cartes. En menys de tres hores totes les cartes havien sigut segellades en els seus sobres i retornades a la oficina de correus per a poder ser entregades als seus destinataris. Tant les cartes que arribaven o sortien de Viena eren prèviament copiades. Aquestes còpies es passaven als criptoanalistes, que

asseguts en petites cabines, eren els encarregats de desxifrar el significat dels missatges. A part d'aconseguir intel·ligència importantíssima per als emperadors d'Àustria, la cambra negra també venia informació als diferents estats. Les cambres negres estaven tornant a fer insegures totes les formes de xifra monoalfabètica. Degut a aquesta inseguretat de la xifra monoalfabètica, els criptògrafs es van veure obligats a adoptar la xifra Vigenère, més complexa i segura. Amb el temps, tots els secretaris de xifres es van passar a les xifres polialfabètiques.

2.2.3 Criptoanàlisi a la xifra Vigenère

La xifra Vigenère va tornar la seguretat a les comunicacions durant gairebé més d'un segle. Durant aquest temps, els secrets d'estat van ser molt difícils d'obtenir mitjançant el desxiframent. A més, la xifra Vigenère era molt utilitzada per a les comunicacions de negocis importants. Le chiffre indéchiffrable inclús va ser considerada com la xifra indesxifrable, fins a l'arribada de la personalitat més important del món del criptoanàlisi del segle XIX, Charles Babbage. Nascut l'any 1791, a Londres, fill d'un banquer. Quan es va casar sense el permís del seu pare es va quedar sense accés a la seva fortuna però no li va impedir viure feliçment i gaudir d'una vida plena. Bàsicament, Babbage era un inventor, trobava solució a qualsevol problema que se li pogués ocórrer. Charles va fer la major contribució al criptoanàlisi des de que els àrabs van desxifrar la xifra monalfabètica en el segle IX, feia ja més de un mil·lenni. Charles va decidir embarcar-se en l'aventura de desxifrar la xifra Vigenère quan Thwaites, un dentista de Bristol, va afirmar haver inventat una nova xifra, que en realitat, era igual a la Vigenère. Babbage va explicar que aquesta xifra ja havia sigut inventada des de feia segles, però Thwaites el va desafiar a que la desxifrés, i Babbage va acceptar.[6]



Quan un criptoanalista intenta desxifrar una xifra difícil és com si intentés nedar a contracorrent. El criptoanalista intenta de qualsevol manera trobar algun salvavides per a mantenir-se viu i poder seguir nadant. Si el criptoanalista està nedant en un mar de xifra monoalfabètica, llavors els seus salvavides seran l'anàlisi de freqüència,

[6] FIGURA 8: Imatge de Charles Babbage.

buscarà aquelles lletres més freqüents i fins i tot les més especials, amb més personalitat. En canvi, en una xifra de substitució polialfabètica les freqüències estan molt més equilibrades, degut a la utilització de més d'un alfabet xifrat. És per això, que a primera vista, sembla ser que en aquest mar no hi ha cap salvavides.

Hem de recordar, que la força de la xifra Vigenère radica en que la mateixa lletra serà codificada per diferents lletres o símbols. Per exemple, si la paraula clau és **CREP**, llavors cada lletra del text original pot ser potencialment substituïda de quatre maneres diferents, perquè la clau té quatre lletres. Cada lletra de la paraula clau defineix un alfabet xifrat diferent en el quadre de Vigenère. Suposem que volem codificar la lletra **m** i veureu com depenen de la lletra de la paraula clau, codificarà per a una o un altre lletra.

Si fem servir la lletra C de CREP per a codificar la lletra m, la lletra del text xifrat que serà utilitzada és la O.

Si fem servir la lletra R de CREP per a codificar la lletra m, la lletra del text xifrat que serà utilitzada és la D.

Si fem servir la lletra E de CREP per a codificar la lletra m, la lletra del text xifrat que serà utilitzada és la Q.

Si fem servir la lletra P de CREP per a codificar la lletra m, la lletra del text xifrat que serà utilitzada és la B.

De la mateixa manera que una lletra en el text xifrat pot ser una lletra o altre, depenent de la lletra de la paraula clau que li correspongui, amb les paraules passa el mateix. Depenent de la posició de la paraula en relació amb la clau, serà codificada d'una manera o altre. Per exemple, la paraula **més** pot ser codificada com **OVW**, **DIH**, **QTU** o **BGJ**. Encara que això dificulta molt el criptoanàlisi, no fa que sigui impossible. Ens hem de quedar amb que ens hem d'adonar que si només hi ha quatre maneres diferents de codificar la paraula **més**, i el missatge original té varies vegades la paraula **més**, llavors és molt probable que alguna de les quatre codificacions possibles es doni i es repeteixi en el text xifrat. Ho demostrarem amb el següent exemple, on la frase **més aigua, més carn i més sucres** ha sigut codificada utilitzant la xifra Vigenère i la paraula clau **CREP**.

Clau	C	R	E	P	C	R	E	P	C	R	E	P	C	R	E	P	C	R	E	P	C	R	E	P	C
Text pla	m	e	s	a	i	g	u	a	m	e	s	c	a	r	n	i	m	e	s	s	u	c	r	e	s
Text xifrat	O	V	W	P	K	X	Y	P	O	V	W	R	C	I	R	X	O	V	W	H	W	T	V	T	U

Casualment la paraula **més** en tots els casos és codificada per **OVW** en les tres ocasions que apareix. La causa per la que les tres vegades es repeteix la forma, és degut a que estan exactament a vuit lletres de distància tant la primera com la segona vegada, i sabem que vuit és un múltiple del número de lletres de la paraula clau, que com sabem, té quatre lletres. Dit d'una altre manera, els tres **més** han sigut codificats segons la mateixa relació amb la paraula clau, **més** cau assota de **CRE** en les tres ocasions perquè la clau ha passat exactament dos vegades entre els diferents **més**, de manera que es repeteix la relació i per tant, la codificació.

Babbage es va adonar d'aquest tipus de repetició, que li va subministrar el salvavides que necessitava per a poder nadar a contra corrent i arribar a conquistar la xifra Vigenère. Va aconseguir establir un mètode relativament senzill que qualsevol criptoanalista podria seguir per a desxifrar la xifra.

FIGURA 9 [7]

Imaginem que hem interceptat aquest missatge, sabem que ha sigut codificat utilitzant la xifra Vigenère, però no sabem res del missatge original ni tampoc de la paraula clau. El primer pas és com l'explicació d'abans, hem de trobar seqüències

[7] Missatge encriptat.

de lletres que es repeteixen al llarg del text. Aquestes repeticions podrien ser produïdes per dos fenòmens diferents. El primer, dos seqüències de lletres diferents del text original han sigut codificades utilitzant diferents parts de la clau però que casualment han donat a una seqüència idèntica en el text xifrat, això és molt poc probable que passi (seria l'indicatiu que ens diria hem arribat a un carrer sense sortida, no tindríem cap salvavides i el desxiframent es tornaria molt més complicat) i el segon fenomen, el qual podem aprofitar i passa la gran majoria de les vegades (la gran majoria de vegades el segon fenomen és el que es dona), en el qual la mateixa seqüència de lletres del text original ha sigut codificada utilitzant la mateixa part de la clau.

Si ens limitem a seqüències llargues, llavors podem descartar pel complert el primer cas. Per exemple, la seqüència **E-F-I-Q** apareix em la primera línia i després en la cinquena, separada per 95 lletres. L'objectiu és trobar la clau, perquè si trobem la clau podrem desxifrar el missatge com si fóssim els receptors. Una vegada tenim les seqüències que es repeteixen, i el número de lletres que hi ha entre repetició i repetició, farem una taula on identificarem els factors dels espais, és a dir pels números que es poden dividir els espais entre repeticions(bàsicament els divisors d'aquell número en concret). Per exemple, la seqüència **E-F-I-Q** es repeteix al cap de 95 lletres, i els divisors de 95 són 1,5,19 i 95 aquests a la vegada són factors de 95 perquè poden dividir exactament a 95 sense deixar decimals. Per tant, aquests factors suggereixen que la clau pot tenir quatre possibilitats:

1. La clau té 1 lletra i es repeteix 95 vegades entre les codificacions.
2. La clau té 5 lletres i es repeteix 19 vegades entre les codificacions.
3. La clau té 19 lletres i es repeteix 5 vegades entre les codificacions.
4. La clau té 95 lletres i es repeteix 1 vegada entre les codificacions.

D'aquestes possibilitats, a simple vista podem descartar unes quantes. Podem descartar la primera possibilitat perquè si la clau només tingués una lletra seria llavors una xifra monoalfabètica, i per a aquesta xifra ja sabem tenim un mètode per a desxifrar-la, l'anàlisi de freqüència. Per a identificar si la clau té 5, 19 o 95 lletres hem d'observar els factors de totes les seqüències que es donen en el text, creant una taula com aquesta.

Secuencia repetida	Espacio entre repeticiones	Posible longitud de la clave (o factores)																	
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
E-F-I-Q	95				✓														✓	
P-S-D-L-P	5				✓															
W-C-X-Y-M	20	✓		✓	✓					✓										✓
E-T-R-L	120	✓	✓	✓	✓	✓		✓		✓		✓			✓					✓

FIGURA 10: Les seqüències repetides en el text que estem estudiant.

Si ens fixem en la taula veurem que hi ha una possible longitud de la clau on totes les seqüències coincideixen, el 5. Tot concorda i sembla tenir sentit amb una clau de 5 lletres.

Llavors suposem que la clau té 5 lletres, el següent pas és deduir quines són les lletres de la clau. Per a començar, anomenarem a les 5 lletres de la següent manera: $L_1 - L_2 - L_3 - L_4 - L_5$, de forma que L_1 representa la primera lletra i així successivament. El procés de codificació comença amb la primera lletra del text original amb la primera lletra clau, L_1 que aquesta mateixa defineix alhora una línia del quadre Vigenère, que proporciona un alfabet xifrat de substitució monoalfabètica. El que passa és que quan hem de codificar la segona lletra, ho fem servint la L_2 per a definir una línia diferent del quadre Vigenère, una nova línia del quadre de Vigenère que alhora ens dona una alfabet xifrat de substitució monoalfabètica. La tercera lletra del text es codificarà segons L_3, la quarta lletra segons L_4 i la cinquena segons L_5. A partir de la sisena lletra tot canvia, perquè com que la clau té cinc lletres una vegada s'acaba es torna a repetir, generant cicles infinits de la mateixa clau fins a l'última lletra del text. Per tant, la sisena lletra serà codificada segons la L_1, la sèptima lletra serà codificada segons L_2 i així successivament, repetint el cicle fins a l'última lletra. Ara ja sabem que la xifra polialfabètica consta de 5 xifres monoalfabètiques, que representen un cinquè del text. La màgia de tot això és que ja sabem com criptoanalitzar les xifres monoalfabètiques.

A partir d'ara l'objectiu serà trobar les lletres de la paraula clau, anirem lletra per lletra. Sabem que un de les 26 línies del quadre Vigenère, definida per L_1, ens proporciona l'alfabet xifrat per a codificar les lletres 1º, 6º, 11º, 16º...(o el que és el mateix, totes les lletres que estan a sota de L_1). Si observem aquestes podrem utilitzar l'anàlisi de freqüència tradicional per a poder descobrir l'alfabet xifrat en qüestió. Una de les claus que hem de recordar és que els alfabets xifrats del quadre

de Vigenère són simplement l'alfabet normal però desplaçats entre 1 i 26 posicions, com la xifra de canvi de Cèsar. És per això que les gràfiques de distribució de freqüències haurien de ser similars a la distribució de freqüències normal, excepte perquè estan desplaçades. Agafem la distribució de freqüències normals i el comparem amb la distribució de freqüències de L_1 .

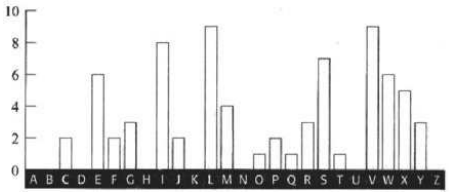


FIGURA 11:Distribució de freqüències per a les lletres del text xifrat que codifiquen utilitzant L_1 .

FIGURA 12: Distribució de freqüències en condicions normals en anglès.

Per a poder saber quants espais està desplaçat ens hem de fixar en les pujades i baixades, les depressions...En general busquem la combinació dels trets més significatius. Un d'aquests trets que sobresurten a la resta és els tres pilars de R-S-T seguits d'una gran depressió de les sis lletres següents, des de la U fins a la Z. Aquest és un tret molt característic i relativament senzill de veure. En L_1 el més similar que trobem són els tres pilars V-W-X, seguits de la depressió que va des de Y fins a la D. El que ens estaria dient això és que les lletres que estan codificades segons L_1 s'han desplaçat quatre posicions(l'alfabet xifrat comença en E). Per tant podem suposar que L_1 és E. Si fem la comparació de les dues taules però la taula L_1 desplaçada quatre espais a l'esquerra ens adonarem que els trets més significatius coincideixen pràcticament perfectament.

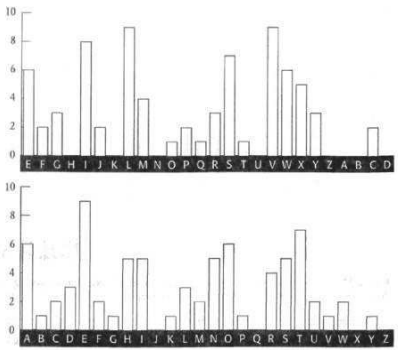


FIGURA 13: Comparació de la distribució de L_1 desplaçada quatre llocs (gràfica superior) amb la distribució de freqüències normal de l'anglès (inferior).

Resum del que hem de fer: busquem repeticions al text xifrat per a poder identificar la longitud de la clau, que ha resultat ser de cinc lletres. Llavors hem dividit el text en cinc parts, cada part codificada amb una xifra de substitució monoalfabètica definida per una lletra de la paraula clau. Analitzant les lletres de la part que li correspon a L_1 hem pogut demostrar que L_1 és E. Llavors l'únic que ens quedarà fer és repetir el mateix procés per a identificar la segona lletra de la clau, la tercera, la quarta i la cinquena. Crec que no és necessari repetir el procés quatre vegades més i per tant arribem directament a la clau ja desxifrada. Analitzant cada part del text, podem deduir que la segona lletra de la clau és la M, la tercera és la I, i la quarta és la Y. La clau és **EMILY**. L'únic que ens quedarà fer una vegada ja tenim la clau és invertir el procés de la xifra Vigenère i ja tindrem complert el criptoanàlisi. La primera lletra del text xifrat és la **W**, que ha estat codificada per E, si anem al quadre i mirem quina lletra està substituint **W**, descobrirem que la primera lletra del text original és la S. Repetint aquest procés amb totes les lletres del text xifrat i ja tindrem el missatge original, evidentment faltarà posar els espais entre paraules, punts, comes, etc. Una vegada tot acabat, el text resultant (AKA el text original) és el següent:

Sit thee down, and have no shame,
Cheek by jowl, and knee by knee:
What care I for any name?
What for order or degree?

Let me screw thee up a peg:
Let me loose thy tongue with wine:
Callest thou that thing a leg?

Thou shalt not be saved by works:
Thou hast been a sinner too:
Ruined trunks on withered forks,
Empty scarecrows, I and you!

Fill the cup, and fill the can:
Have a rouse before the morn:

Which is thinnest? thine or mine? *Every moment dies a man,*
Every moment one is born

Encara que el primer criptoanàlisi satisfactori va ser realitzat per Babbage, cap al 1854, aquest descobriment no va ser reconegut en absolut perquè mai ho va publicar. No va ser descobert fins que uns estudiosos van examinar les seves notes. Independentment, també va ser descoberta la mateixa tècnica per Friedrich Wilhelm Kasisiki, un oficial retirat del exèrcit prussià. Kasiski si que va publicar la seva tècnica i és per això que la tècnica de criptoanalitzar la xifra Vigenère és coneguda com la Proba Kasiski, i la contribució de Babbage ha sigut ignorada pràcticament en gran mesura.

2.3 El desenvolupament de les màquines de xifres. Dels discos de xifres a l' Enigma

La primera màquina de xifres, els discos de xifres, no va arribar fins al segle XV per l'arquitecte italià León Alberti, un dels pares de la xifra polialfabètica (ja mencionat anteriorment). Aquesta màquina no és més que dos discs, un més gran que l'altre, on a la vora de tots dos està inscrit l'alfabet. Llavors, col·loca el més petit a sobre del gran i els fixa amb una agulla que servia com a eix. A la següent imatge podeu veure el primer model de bidiscs de xifres.

FIGURA 15 [8]

Els dos discs poden girar independentment l'un de l'altre(?), de forma que els dos alfabets poden tenir diferents posicions relatives, és a dir un simple canvi de Cèsar.

[8] Primer model de discs de xifres.

Per tant, amb aquest senzill aparell, que inclús sembla una joguina, pots codificar un missatge. Per a codificar un missatge amb el canvi de Cèsar, simplement posem la **A** externa amb la lletra interna que vulguem, posant al davant de la **A** externa la lletra que desitgem que sigui la primera lletra del text xifrat. El disc extern serà el alfabet original i l'intern, l'alfabet xifrat. Per a xifrar un missatge hem de buscar cada lletra del missatge original amb la seva relativa del disc interior, aquella lletra que sigui la relativa a la original del text s'escriu com a part del text xifrat. Encara que el disc de xifres sigui una màquina molt simple, no deixa de ser una eina molt útil que facilita la codificació i ha perdurat durant gairebé cinc segles.

Una altre manera d'explicar el funcionament del disc de xifres és considerant-lo com un modificador, agafa la lletra del text pla i la transforma en una altre cosa. Fins ara aquesta manera d'operar és molt fàcil, i la xifra resulta molt senzilla de desxifrar, però el disc de xifres també es pot fer servir d'una manera més complexa (spoiler, xifra polialfabètica). El seu inventor va proposar una altre manera de fer servir el disc de xifres, va suggerir que durant el missatge, la posició del disc canviés, generant així una xifra polialfabètica (per això Alberti és considerat el pare de la xifra polialfabètica). Imaginem-nos que Alberti vol utilitzar el disc de xifres per a xifrar la paraula **selectivitat**, utilitzant la clau **MORT**.

Començaria situant la A externa juntament amb la **M** interna. Llavors codificaria la primera lletra del missatge, **s**, buscant-la en el disc intern i veurem quina és la seva lletra relativa del disc intern, en aquest cas és la **E**.

Per a codificar la segona lletra hauria de ressituar el disc segons la segona lletra de la clau, per tant hauria de posar la A externa amb la **O** interna. Després codificaria la segona lletra, la **e**, que en l'alfabet xifrat de la **O** correspon a la lletra **S**. La codificació continua col·locant el disc de xifres segons la lletra de la clau, en aquest cas la **R**, després la **T**, i una altre vegada tornem amb la **M**, i així successivament.

El disc de xifres permet accelerar la codificació i a més redueix els errors si ho comparem amb codificar un missatge amb el quadre Vigenère. Encara que aquest nivell extra de codificació complica el desxiframent del missatge, no ho fa indesxifrable, perquè simplement estem davant d'una versió mecanitzada de la xifra Vigenère, que ja sabem com criptoanalitzar-la. No va ser fins pràcticament més de

cinc segles, que sorgiria una màquina més difícil de desxifrar mai vist anteriorment (spoiler, Enigma).

Arthur Scherbius va néixer a Frankfurt, Alemanya, l'any 1878. Va estudiar electricitat en les universitats de Munich i posteriorment en Hannover, acabant la seva formació l'any 1903. L'any següent va rebre el doctorat en enginyeria. Juntament amb el seu amic Ritter va fundar l'empresa Scherbius & Ritter l'any 1918, una innovadora empresa de enginyeria que es dedicava a una mica de tot, des dels motors asíncrons fins a coixins elèctrics.

La seva fama a Alemanya va arribar ben d'hora degut als seus invents, especialment aquells que estaven relacionats amb els motors asíncrons. Scherbius estava al càrrec de la investigació i desenvolupament, també conegut com I+D (inclús avui en dia ho pots trobar com I+D+R, investigació, desenvolupament i recerca), buscant constantment nous projectes. Un dels seus projectes preferits era els sistemes criptogràfics, volia substituir-los per unes noves màquines adequades a la tecnologia del segle XX. L'any 1918 va patentar una màquina de xifra que estava basada en unes rodes giratòries interconnectades elèctricament per elements conductors que feien contacte amb elles al girar, o en altres paraules, va desenvolupar una versió elèctrica del disc de xifres, però amb una mica més d'enginy. El va patentar sota el nom d'Enigma, encara no ho sabia però aquesta màquina es convertiria en el sistema més segur i temible de codificació de la història.

La màquina Enigma és, sens dubte, una de les majors invencions, com a mínim en l'àmbit de la criptografia, del segle XX. No només per la seva funció sinó també per l'enginy que suposa crear-la, Scherbius va combinar i ordenar enginyosos components per a crear una complexa màquina de xifres. Per a entendre com funciona, descompondrem la màquina per parts i explicarem el funcionament i la utilitat que té cada part.

D'aquesta manera també intentarem aconseguir que ens quedi clar els principis fonamentals en què es va inspirar l'inventor per a crear-la.

La forma més bàsica de l'invent de Scherbius consisteix en tres elements connectats entre ells per cables: un **teclat** per a escriure cada lletra del text original o pla, una **unitat modificadora** que codifica cada lletra del text original en una lletra del text xifrat i un **taulell** que conté diverses llumetes que indiquen la lletra del text xifrat. Per

a simplificar l'explicació farem servir una màquina que té un alfabet de sis lletres. L'operador de la màquina prem en el teclat la lletra del text original per a que sigui codificada, generant una pulsació elèctrica que a través de la unitat modificadora central arriba al altre costat, és a dir al taulell amb les llumetes, on il·luminarà la lletra que es farà servir pel text xifrat.

La unitat modificadora central que acabem d'anomenar és la part més important de la màquina. També es coneix com a modificador, que no és més que un disc gruixut ple de cables. Des del teclat, els cables entren en el modificador, que en aquest cas al ser un alfabet de sis lletres hi haurà sis llocs d'entrada on els cables realitzaran una sèrie de girs dins del modificador fins a la sortida per l'altre costat (on també hi ha sis sortides). Tot el cablejat intern del modificador determinarà la codificació de les lletres del text original. Per exemples en el següent exemple el cablejat dicta que:

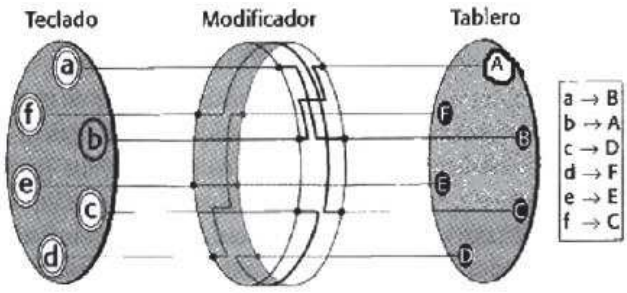


FIGURA 16 [9]

- Si teclegem la lletra **a** s'il·luminarà la lletra **B**, el que significa que **a** és codificada com **B**.
- Si teclegem la lletra **b** s'il·luminarà la lletra **A**, el que significa que **b** és codificada com **A**.
- Si teclegem la lletra **c** s'il·luminarà la lletra **D**, el que significa que **c** és codificada com **D**.
- Si teclegem la lletra **d** s'il·luminarà la lletra **F**, el que significa que **d** és codificada com **F**.
- Si teclegem la lletra **e** s'il·luminarà la lletra **E**, el que significa que **e** és codificada com **E**.
- Si teclegem la lletra **f** s'il·luminarà la lletra **C**, el que significa que **f** és codificada com **C**.

[9] Imatge de la relació entre teclat, modificador i taulell.

La paraula **ceba** codificaria com a **DEAB**. Amb aquesta col·locació de l'aparell, el modificador defineix un alfabet xifrat en concret i la màquina serveix per a poder xifrar una xifra de substitució monoalfabètica simple.

La idea de Scherbius però no era tan simple, la idea era que el modificador girés automàticament un sisè de revolució cada vegada que es codifiqués una lletra (en el cas que fos un alfabet complet de 26 lletres diríem un vint-i-sisè de revolució). Amb aquest gir del modificador estem generant un nou alfabet xifrat cada vegada que es prem una lletra. Per tant, si tornem a xifrar el missatge **ceba**, la **c** seguiria codificant com a **D** però immediatament després de teclejar el modificador gira, creant un nou alfabet xifrat i ara **c** no seria codificada per **D**, sinó per **B**. D'aquesta manera si teclegéssim sis vegades seguides **b** obtindríem el següent text xifrat: **ACEBDC**. El alfabet xifrat canvia a cada codificació i la codificació de la lletra **b** canvia contínuament. En aquest cas el modificador amb la rotació ens estaria generant sis alfabets xifrats que es repeteixen infinitament, creant així una xifra de substitució polialfabètica.

La rotació del modificador és essencialment la característica més important de la màquina. Per contra, aquest model té una debilitat molt clara. Teclejar sis vegades qualsevol lletra, o teclejar sis vegades diferents lletres, provocarà que el modificador torni a la posició inicial, repetint el mateix patró de codificació.

Com a criptògraf, un dels objectius principals a la hora de crear una xifra és evitar patrons o repeticions, perquè donen regularitat a la estructura del text i faciliten el criptoanàlisi, les repeticions són signe de una xifra dèbil. Aquest problema pot desaparèixer introduint un segon disc modificador. Al afegir un segon disc, el patró de codificació no es repeteix fins que s'han codificat 36 lletres. Cada vegada que es codifica una lletra, el primer modificador gira un espai o revolució, en canvi el segon modificador roman quiet la major part del temps. El segon modificador només es mourà quan el primer modificador hagi realitzat una revolució completa (en aquest cas quan hagi girat sis vegades). El primer modificador té una dent que només quan fa la volta completa provoca que el segon modificador es mogui, i viceversa. El patró de codificació no es tornarà a repetir fins que el segon modificador torni a estar com al principi, o la codificació de 6x6, és a dir 36 lletres en total. Hi ha 36 disposicions dels modificadors diferents, o dit d'una altre manera hi ha 36 alfabets xifrat diferents.

Si en comptes de fer servir un alfabet de sis lletres fem servir l'alfabet complert, la màquina de xifres tindria 26x26 alfabets xifrats diferents, o el que és el mateix, 676 alfabets xifrats diferents.

De manera que és possible crear una màquina que estigui constantment canviant de alfabets xifrats, només necessitem combinar modificadors. Quan premem una tecla, depenent de la disposició dels diferents modificadors, aquesta lletra estarà sent codificada per un dels centenars alfabets possibles. Després de cada lletra polsada, la disposició torna a canviar i es codifica per un alfabet xifrat diferent.

Una altra avantatge és que al ser un moviment automàtic comporta una gran eficiència i exactitud.

Encara ens falten tres elements per a explicar. El primer, la màquina Enigma tenia un tercer modificador per a obtenir encara més complexitat: per a un alfabet complert, els tres modificadors li proporcionaven 26x26x26, és a dir, 17.576 disposicions diferents dels modificadors, que es tradueix a 17.576 alfabets xifrats diferents. Segon, Scherbius va afegir un reflector, és semblant en quant a forma a un modificador però a la vegada és diferent, perquè no gira i els cables entren i surten pel mateix lloc. Quan l'operador tecleja una lletra envia una senyal elèctrica a través dels tres modificadors. Quan aquesta senyal arribar al reflector, aquest la retorna pels mateixos tres modificadors, però per una ruta diferent.

Encara que a primera vista sembla que el reflector no fa res, perquè no augmenta el nombre de possibles alfabets xifrats, quan ens fixem com la màquina codifica i descodifica veurem la verdadera utilitat del reflector.

Si un operador desitja enviar un missatge secret primer ha de seguir una sèrie de paràmetres i passos, on s'haurà de posar d'acord amb els altres operadors, per a poder realitzar la codificació amb èxit i de forma segura. El primer pas és girar els modificadors per a posar-los en una posició en concret. Hi ha 17.576 posicions possibles, per tant 17.576 posicions de partida possibles. La posició inicial dels modificadors és clau perquè determinarà com es codifica el missatge. Si suposéssim que Enigma és com un sistema de xifres general, les posicions inicials serien la clau del missatge, sense ella serà impossible (com a mínim fins al desxiframent de l'Enigma) descodificar el missatge. Normalment les posicions inicials venen dictades per uns llibres de codis, que enumeren la clau, és a dir, les posicions dels

modificadors per a cada dia i tots els operadors han de tenir aquest llibre per a posar-se d'acord, tota la xarxa de comunicacions ha de tenir aquest llibre de codis, cosa que provoca temps i esforç per a distribuir tots els llibres, però molt més senzill i ràpid que si un exèrcit volgués utilitzar la xifra de quadern únic, que per a cada missatge necessitaríem una nova clau, i la distribució d'aquesta seria molt més complicada i inclús absurda.

Una vegada els modificadors estan col·locats segons la clau d'aquell dia, l'operador pot començar a codificar. Tecleja les lletres del missatge, cada vegada que prem la lletra del missatge original s'il·lumina en el taulell una lletra, que correspon a la lletra del text xifrat. Una cop ha acabat de generar el text xifrat complert, passa el missatge a un operador de ràdio perquè el transmeti al receptor desitjat. Per a poder desxifrar el missatge, el receptor necessita una màquina Enigma i el llibre de claus per a poder saber la posició correcta per a aquell missatge dels modificadors. Suposant que el receptor té la màquina i el llibre, una vegada hagi col·locat els modificadors en la posició dictada pel llibre, tecleja el text xifrat lletra a lletra i apunta les lletres que s'il·luminen en el taulell.

L'emissor tecleja el text original per a generar el text xifrat i l'emissor tecleja el text xifrat per a generar el text original, la codificació i la descodificació són processos que es poden invertir, són processos miralls, es reflecteixen. Aquesta propietat bé donada pel reflector. La màquina codifica la lletra del text pla en una lletra del text xifrat i mentre la màquina estigui en la mateixa posició, descodificarà la mateixa lletra del text xifrat en la mateixa lletra original del text pla. Mentre la màquina Enigma estigui en la mateixa posició, podrà codificar i descodificar el missatge, si jo teclejo el missatge codificat, Enigma em donarà el missatge descodificat (l'original) i si jo teclejo el missatge original, doncs el codificarà.

És probable que l'enemic es faci amb una màquina Enigma, però sense saber les claus, les posicions inicials, no serà gens fàcil desxifrar el missatge. Per a que el criptoanalista pugui desxifrar el missatge haurà de provar totes les combinacions, és a dir 17.576 possibles posicions inicials. Si el criptoanalista pogués comprovar una disposició dels modificadors per minut i treballés dia i nit, tardaria dos setmanes per a comprovar totes les claus. Això és un nivell de seguretat moderat, però si l'enemic posa a treballar a una dotzena de persones a comprovar les claus, llavors podrien

comprovar totes les claus en un dia. La seguretat per tant no és tan elevada i era necessari augmentar el número de claus possibles. Scherbius era conscient i és per això que va decidir millorar la seguretat del seu invent. Per a fer-ho podria simplement afegir més modificadors, però per contra el tamany de la màquina augmentaria.

En comptes de posar més modificadors va fer dues coses. Primer, va fer que els modificadors fossin intercanviables, així podries canviar els modificadors de lloc, augmentant el número de claus. Hi ha sis maneres diferents de posar els modificadors, augmentant el número de claus inicials possibles en un factor de 6.

La segona cosa nova que va implementar va ser un claviller entre el teclat i el primer modificador. El claviller permet inserir cables que tenen l'efecte d'intercanviar algunes lletres abans de que entrin al primer modificador. Per exemple, podríem utilitzar el claviller per a intercanviar les connexions de la lletra **c** i **d**, de manera que quan l'operador teclegi la lletra **c**, la senyal elèctrica en realitat seguirà la trajectòria de la **d**, i viceversa. L'operador de la Enigma tenia sis cables, el que significa que es podien intercanviar sis lletres, deixant catorze sense connectar ni modificar. Com que les lletres intercanviades pel claviller formen part de la disposició de la Enigma, era necessari que s'especifiquessin en el llibre de codis quines lletres s'intercanviaven i quines no. En la següent imatge podràs veure com funciona el claviller, en aquest cas com es fa servir una màquina d'un alfabet de sis lletres, només s'intercanviaran un parell de lletres, només farem servir dos cables per a canviar la trajectòria del senyal elèctric, en aquest cas la **a** i la **b**.

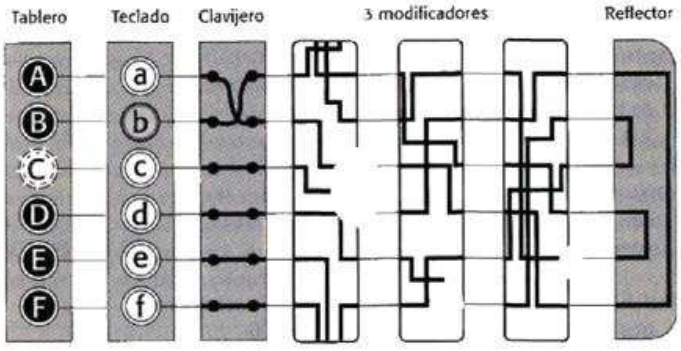


FIGURA 17 [10]

[10] Representació esquemàtica simplificada del funcionament d'una màquina Enigma.

Encara ens queda una altre element, l'anell, però que encara que té un afecte en la codificació, nosaltres no ho tindrem en compte perquè és la part menys significativa de la màquina Enigma.

Una vegada que coneixem totes les parts de la màquina (bé, només els elements principals i més importants), podem calcular el número de possibles disposicions inicials, és a dir el número de possibles claus. Per a calcular les possibles claus tindrem en compte, l'ordre de disposició dels modificadors, l'orientació dels modificadors i el claviller (les maneres d'intercanviar sis parells de lletres entre les 26 lletres de l'abecedari):

-Disposició dels modificadors: en aquest cas tenim 3 modificadors i els podem posar en qualsevol ordre, per tant tindrem sis possibles permutacions entre ells.

1-2-3/1-3-2/2-1-3/2-3-1/3-1-2/3-2-1=6

-Orientació dels modificadors: cada rotor es pot situar en 26 orientacions diferents i com que tenim tres rotors, tenim 17.576 possibles disposicions.

26x26x26=17.576

-Claviller: cada una de les 12 extremitats dels sis cables que tenim poden estar connectades en 26 posicions que no estiguin ocupades, i les extremitats dels cables connectades al seu relatiu (és a el seu parell de lletres) i tenint en compte els sis cables mateixos, tindrem 100.391.791.500 possibilitats.

$$N = \frac{26!}{6!(26-2\cdot 6)!\cdot 2^6} = 100.391.791.500$$

-Total: el número total és el múltiple dels tres resultats previs:

$$6\cdot 17.576\cdot 100.391.791.500 = 10.586.916.764.424.000$$

Aquest és el número de possibles claus d'aquest model de la màquina, però el model que més es va fer servir, i durant la segona guerra mundial també, és el següent:

-Disposició dels modificadors: hi havia 5 rotors, dels quals només es feien servir tres, per tant les variacions possibles són 60.

$$\frac{5!}{(5-3)!} = 60$$

-Orientació dels modificadors: al tenir tres com el model anterior, cada rotor es pot situar en 26 orientacions diferents i com que tenim tres rotors, tenim 17.576 possibles disposicions.

$$26x26x26=17.576$$

-Claviller: en aquest model hi havia 10 cables per claviller, per tant, si tenim en compte que cada una de les 20 extremitats dels deu cables pot ser connectada en qualsevol de les 26 lletres que no hagin estat prèviament ocupades per un altre cable, i que cada extremitat va a una de les lletres del parell de lletres intercanviades, i tenint en compte que hi ha 10 cables, tindrem 150.738.274.937.250 possibilitats.

$$N = \frac{26!^{10}}{10!(26-2\cdot 10)!\cdot 2} = 150.738.274.937.250$$

- Total: el número total és el múltiple dels tres resultats previs:

$$60\cdot 17.576\cdot 150.738.274.937.250 = 158.962.555.217.826.360.000$$

Tenim cent cinquanta-vuit trilions nou-cents seixanta-dos mil cinc-cents cinquanta-cinc bilions dos-cents disset mil vuit-cents vint-i-sis milions tres-cents seixanta mil possibles disposicions inicials, o claus.

2.4 Desxifrant l'Enigma

A partir de l'any 1926, any on es comencen a interceptar missatges alemanys codificats per l'Enigma, les comunicacions alemanyes van passar a ser inexpugnables. Tal era la seguretat de les comunicacions que cap estat va poder desxifrar la xifra. Encara que la xifra semblava indesxifrable, com que els aliats acabaven de guanyar la guerra, no tenien por d'Alemanya perquè aquesta havia estat paralitzada per la recent derrota. Com que els aliats es trobaven en un posició dominant, no van donar-li importància al fet que les comunicacions alemanyes eren completament segures. Tot i que la majoria d'estats no van donar-li importància a aquest fet, hi havia un país que no es podia permetre relaxar-se, Polònia. Al acabar la guerra va tornar a ser un estat independent, però es sent amenaçada. Per l'est estava la Unió Soviètica, que volia expandir-se per a estendre la seva ideologia, el

comunisme, i per l'altre banda estava Alemanya, el qual havia perdut el territori de Polònia al acabar la guerra. Els polonesos no es podien permetre baixar la guàrdia, perquè sabien que tard o d'hora, per una banda o altre, intentarien robar el que era seu, conquerir els seus territoris. És per això que al poc d'haver-se independitzat d'Alemanya, havien ampliat enormement el personal en l'oficina de xifres.

Encara que en el passat els polonesos havien sigut unes màquines per a desxifrar les xifres alemanyes, amb l'aparició de l'Enigma, el número de missatges alemanys desxifrats havia caigut en picat. Només començar, es van adonar que necessitaven entendre com funcionava i les parts que tenia Enigma. Tot i tenir una versió comercial, sabien que era una versió completament diferent. El primer pas cap al desxiframent d'Enigma era aconseguir una màquina Enigma, per a entendre com funcionava i com estava col·locat el cablejat, i, sense aquesta informació, el desxiframent no arribaria mai.

Qui si va donar el primer pas va ser Hans-Thilo Schmidt, nascut a Berlín l'any 1888. Fill petit d'un important professor i d'una aristòcrata. Schmidt va participar en la primera guerra mundial com a militar, però degut a la reducció del personal militar alemany, no va ser considerat per a continuar en l'exèrcit. Va intentar donar a conèixer com a home de negocis però en varies ocasions va fracassar. Bàsicament era la ovella negra de la família, perquè el seu germà gran, Rudolph, va romandre en l'exèrcit després de les retallades. Inclús va ser anomenat com a cap del personal del Cos de Senyals. S'encarregava de garantir la seguretat en les comunicacions. Parlant breu i malament, com que Schmidt era un fracassat, es va veure en l'obligació de demanar ajuda al seu germà per a aconseguir feina. El seu germà va aconseguir que treballés a la oficina de xifres com a responsables d'administrar les comunicacions xifrades d'Alemanya.

A causa de la gelosia de Schmidt envers el seu germà, a més del ressentiment que sentia per la seva nació (que recordem que l'havia rebutjat) va acabar venent informació a altres estats.

Gràcies a Schmidt (i a gràcies a la supèrbia francesa), els polonesos van aconseguir els documents necessaris per a poder fer l'Enigma i la informació necessària per a poder deduir els cablejats interns dels modificadors.

En els documents que Schmidt va entregar també s'explicava el disseny dels llibres de codis utilitzats pels alemanys. Cada mes tots els operadors de l'Enigma rebien aquests llibres on s'indicava la clau que s'havia de fer servir aquell dia, és a dir, les posicions dels modificadors i les lletres que s'havien d'intercanviar. Per exemple:

1. Posicions dels modificadors: 3-1-2
2. Orientació dels modificadors: T-L-W
3. Posicions del claviller(si suposem que tenien sis cables): A-G, D-Y, E-U, W-I, L-M, N-P.

Els alemanys tenien un neguit, i aquest era que si codificaven tots els missatges d'Alemanya amb la mateixa clau durant tot un dia, és possible que els enemics tinguessin massa mostra d'aquesta clau i amb això poguessin trobar alguna debilitat a Enigma(podem estar parlant que en les comunicacions alemanyes hi ha un flux de dos milions de lletres diàries). Com a precaució van decidir fer servir una **clau de missatge** per a cada missatge**.** Les **claus de missatge** tenien les mateixes disposicions dels modificadors i les mateixes posicions del claviller, però tenien una orientació dels modificadors diferents. Aquesta nova orientació havia de ser transmesa per l'emissor. Suposem que l'emissor (nosaltres) volem enviar un missatge a un altre operador. El primer que hem de fer és seguir les instruccions del llibre de codis d'aquell dia. Posem les orientacions i les disposicions dels modificadors i claviller que ens demana. En el dia d'avui l'orientació dels modificadors és **SCQ**. A continuació, escollim una paraula de tres lletres al atzar, tingui o no sentit. Aquesta paraula és la que farem servir per a canviar la orientació dels modificadors, **WAB**. Seguidament, codifiquem **WAB** segons la clau d'avui. La clau de missatge es tecleja en l'Enigma dos vegades, per a proporcionar un control doble al receptor. Llavors, l'emissor canvia la seva orientació dels modificadors a **WAB** i codifica el missatge desitjat. El receptor d'aquest missatge haurà de posar la clau del dia (disposició, orientació...) i escriure les sis primeres lletres, que revelaran la clau missatge. Llavors, el receptor posarà els modificadors segons la clau missatge i descodificarà el missatge en qüestió.

Encara que aquest sistema sembla fer a la xifra Enigma encara més difícil de desxifrar, és de fet, la seva perdició.

Tornem a Polònia l'any 1931. Els polonesos ja havien aconseguit els plànols d'Enigma i estaven preparats per a treballar nit i dia per a trobar les debilitats d'aquesta xifra.

Els encarregats de trobar aquestes debilitats van ser una nova generació de criptoanalistes. Durant la major part de la història de la criptografia i el criptoanàlisi, es pensava que els millors en el camp eren lingüistes, però l'arribada d'Enigma, i amb ella la mecanització del camp, es van veure obligats a canviar la seva política de reclutament. Al ser l'Enigma una xifra matemàtica, van deduir que els més adequats a desxifrar-la serien científics, més concretament matemàtics. Després de fer una sèrie de proves als millors matemàtics, van veure que tres dels vint previs, complien les seves expectatives. Un d'aquest tres era Marian Rejewski. [11]

Marian Rejewski va néixer l'any 1905, a Bromberg, aquell moment formava part del imperi Alemany. Després de l'institut va anar a estudiar matemàtiques a la universitat de Ponzan, PUT (Poznan University of Technology). L'any 1929, poc abans de graduar-se, va entrar en un curs de criptoanàlisi secret, dut a terme per l'oficina de xifres de Polònia. La raó per la qual van reclutar als matemàtics d'aquesta universitat és perquè a l'estar situada a l'oest del país, territori que havia format part d'Alemanya fins el 1918, aquests matemàtics parlaven Alemany. Tot i no ser la universitat més prestigiosa de l'estat, al parlar l'idioma de l'enemic, compensava.

En aquest curs va destacar i poc després va entrar a treballar a l'oficina de xifres. L'objectiu d'aquests matemàtics estava clar; havien de desxifrar l'Enigma.

Per fer-ho, tres peces d'informació eren necessàries: (1) entendre el funcionament general de l'Enigma, (2) el cablejat dels rotors, (3) tenir les claus diàries(la disposició dels rotors i del claviller i la orientació dels rotors). Rejewski només tenia la primera, informació aconseguida gràcies a l'exèrcit francès. Encara faltaven les altres dues fonts d'informació, però ja era un bon començament.

L'estratègia de Rejewski per atacar l'Enigma estava centrada en el fet que la repetició és l'enemic de la seguretat: les repeticions porten a patrons, l'arma preferida dels criptoanalistes. La repetició en l'Enigma era ben clara, la **clau**

[11] FIGURA 18: Imatge de Marian Rejewski.

missatge codificada dos vegades al principi de cada missatge. Com ja hem mencionat anteriorment, la repetició d'aquest missatge, el qual indica l'orientació dels rotors per a cada missatge, era present per a intentar evitar els errors causats per les interferències de ràdio i/o els errors dels operadors. Ràpidament es va adonar que si la clau estava repetida, això volia dir que la primera i quarta lletra, eren en realitat la mateixa, i, el mateix passa amb la segona i cinquena i la tercera i sisena. El fet que la primera i quarta lletra fos la mateixa, va permetre a Rejewski deduir una lleugera limitació en la disposició general de la màquina. Aquesta limitació demostra que la primera i quarta lletra estan íntimament relacionades.

Rejewski va estudiar aquesta relació entre les lletres. Per exemple, suposem que li arriba aquests quatre missatges i les sis primeres lletres de cada missatge són les següents: `BJGTDN`, `LIFBAB`, `ETULZR`, `TFREII`. Si ens fixem en la primera i quarta lletra de cada missatge podem establir unes relacions. B està relacionada amb T, L està relacionada amb B, E està relacionada amb L, T està relacionada amb E: (B,T), (L,B), (E,L),(T,E). Si pogués aconseguir suficient data (informació), podria establir seqüències de relacions. En el nostre cas B està relacionada amb T, T està relacionada amb E, E està relacionada amb L i L està relacionada amb B. Un cicle de 4: B→T→E→L→B. És un cicle de quatre perquè ha necessitat quatre salts per arribar a la mateixa lletra.

Va començar a estudiar aquest tipus de patrons, va fer una llista de totes les cadenes amb el número de connexions que tenia cada una. Fins ara, només hem tingut en compte la relació entre la primera i quarta lletra, però ell va estudiar les relacions de la segona i cinquena i de la tercera i sisena també. Amb això es va adonar que les cadenes canviaven cada dia. Hi havia dies on havia molts tipus de cadenes i altres dies on només hi havien poques cadenes, però molt llargues. La característica important d'aquestes cadenes és que són el resultat de la posició de la clau del dia: depenen de les posicions del claviller i de l'orientació i disposició dels modificadors. Necessitava reduir el nombre de claus possibles perquè sinó li seria impossible desxifrar l'Enigma.

El seu objectiu era reduir el número de claus possibles treien de l'equació el claviller. Va trobar una característica de les cadenes que depenia només dels modificadors: el número de connexions de les cadenes només depèn de la posició dels modificadors.

Suposem que la clau del dia ens diu que les lletres F i B s'han d'intercanviar. Si canviem aquest element de la clau, en comptes d'intercanviar B i F intercanviem T i K, la cadena que hem utilitzat anteriorment canviaria de la següent manera:

$$B \rightarrow T \rightarrow E \rightarrow L \rightarrow B \Rightarrow 4 \text{ connexions}$$

$$B \rightarrow K \rightarrow E \rightarrow L \rightarrow B \Rightarrow 4 \text{ connexions}$$

Per molt que canviem les lletres, el número de connexions seguirà sent el mateix, es manté constant. Rejewski acabava d'identificar una faceta de les cadenes que és exclusivament un reflex de la posició dels modificadors.

Ara, les possibles claus s'havia reduït a només el número de disposicions possibles dels modificadors (6), multiplicat pel número d'orientacions possibles de cada modificadors(26x26x26=17.576), és a dir 105.456 possibles claus.

$$617.576 = 105.456$$

El problema de trobar la clau de l'Enigma acabava de ser reduït aproximadament cent mil milions de vegades. Tot i que encara havia d'ocupar-se de les 105.456 possibilitats restants, el problema s'ha tornat molt més senzill.

Com que tenien accés a rèpliques de la màquina Enigma, el seu equip va treballar en provar cada una de les 105.456 posicions dels modificadors, catalogant la longitud de les cadenes generada per cada clau. Van trigar gairebé un any, però a partir de l'any 1935, podien obtenir la clau en un interval de temps molt petit, 12-20 minuts.

Encara que havia identificat la part de la clau del dia respecte als modificadors, encara havia d'establir les posicions del claviller, una tasca relativament senzilla. Començava orientant els modificadors segons la clau del dia i retirava tots els cables del claviller. Llavors agafava un text xifrat interceptat i després d'haver orientat els modificadors novament segons el missatge clau, teclejava aleatòriament en l'Enigma. Normalment apareixien galimaties però, a vegades, apareixien frases reconeixibles. Per exemple **vtllmenjalmacattons**, que probablement hauria de ser «vull menjar macarrons». Bé, potser el missatge no era exactament com aquest però tenia molta gana i és el primer exemple que m'ha vingut al cap.

Si suposem que el missatge és aquest llavors substituïm les lletres que estan en una posició errònia per les que si haurien de ser. Aquestes lletres són les que estan intercanviades en el claviller. Una vegada trobades totes les lletres intercanviades, els missatges alemanys d'aquell dia es tornen transparents.

Havia aconseguit que les comunicacions més segures del moment ja no ho fossin, i a més, eren transparents a ulls dels polonesos.

Inclús quan els alemanys van modificar lleugerament l'Enigma, Rejewski va contraatacar. El seu catàleg de cadenes ja no tenia cap utilitat, però va aconseguir inventar una versió mecanitzada del seu sistema de catalogació. Com que hi havia sis possibles disposicions dels modificadors, era necessari tenir sis màquines de Rejewski treballant en paral·lel. Juntes formaven una màquina que mesurava un metre d'altura i que era capaç de trobar la clau del dia en menys de dues hores, s'anomenaven **bombes**.

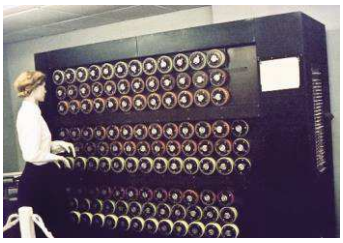


FIGURA 19: Imatge d'una màquina bomba.

No obstant, l'habilitat de Rejewski de poder desxifrar els missatges alemanys va arribar al seu final. El desembre de l'any 1938, els criptògrafs alemanys van augmentar la seguretat de l'Enigma. Van augmentar el número de modificadors per a escollir, és a dir, els operadors cada dia havien d'agafar tres dels cinc modificadors i posar-los en les posicions indicades. Per tant, si abans les possibles disposicions dels modificadors eren només 6, ara havia augmentat aquest número fins a 60($5!5-3!=60$). El primer que havia de fer era deduir els cablejats dels dos nous modificadors. A més, hauria de construir deu bombes més degut al augment dels modificadors. Un més després, el gener del 39, van augmentar el número de cables del claviller a 10. Si abans s'intercanviaven dotze lletres, ara eren vint lletres les que s'intercanviaven. El número de claus possibles havia augmentat a 150.738.274.937.250 (càlcul realitzat anteriorment). Rejewski havia demostrat que l'Enigma no era una xifra indesxifrable, però sense els mitjans necessaris no seria capaç de continuar amb el desxiframent.

El 27 d'abril de 1939 Alemanya acabava de trencar el tractat de no agressió amb Polònia. Això significava dues coses, la primera, que Polònia estava sent envaïda (bastant obvia la veritat), i la segona, si Polònia era envaïda, els seus avenços criptoanalítics, fins llavors secrets i desconeguts pels països aliats, es perdrien amb la seva caiguda. Confiaven que si distribuïen aquesta informació als francesos i als anglesos, que tenien més mitjans, potser ho aprofitarien per a treure-li partit al concepte de les bombes, i amb sort, guanyar la guerra.

El 30 de juliol, el cap del Biuro Szyfrów , Langer, va telegrafiar als seus homòlegs francesos i britànics invitant-los a Varsòvia per a tractar assumptes urgents referents a l'Enigma. En aquesta reunió, Langer els va oferir dues rèpliques de l'Enigma i dos plànols per a construir les bombes. Dos setmanes després de la reunió, Hitler va envair Polònia i la guerra va començar.

Amb l'arribada dels avenços polonesos, els britànics i francesos havien recuperat l'esperança de desxifrar l'Enigma, que fins ara havien assumit que era indesxifrable. Els polonesos havien demostrat que la màquina té debilitats, cosa que va motivar als criptoanalistes a seguir lluitant per aconseguir-ho. Gràcies als polonesos, també s'havia demostrat el valor els matemàtics en el camp. Anglaterra, durant tota l'existència de la **Sala 40**, la cambra negra britànica, havia estat dominada per lingüistes, doncs bé, la cosa estava apunt de canviar. Des de la sala 40 es va ordenar el reclutament de personal matemàtic i científic. La manera de reclutar-los no va ser gaire complicada, els van reclutar a través de la xarxa d'antics companys de la universitat: els que treballaven en la sala 40 es van posar en contacte amb els seus antics companys d'Oxford o Cambridge. També hi havia una xarxa de antigues universitàries que reclutaven a antigues companyes de les universitats de Newnham College, Girton College i de Cambridge.

Als nous membres se'ls va poratr a **Bletchley Park**, en Buckinghamshire, la seu del *Government Code and Cypher School* (Escola governamental de codis i xifres), organització recent fundada. Bletchley Park podia albergar a molt més personal que la sala 40, ja que s'esperava un flux de dos milions de paraules en plena guerra. En el centre de Bletchley Park hi havia una gran mansió victoriana, construïda per sir Herbert León.

La mansió, amb la seva biblioteca, menjador… va proporcionar la administració central per a tota la operació Bletchley. A la planta baixa es van crear multitud de rafals. Aquestes construccions improvisades de fusta es feien servir com a cambres de descodificació. Per exemple, el rafal 6 estava especialitzat en atacar les comunicacions fetes per l'Enigma de l'exèrcit alemany, passant els desxiframents al rafal 3, on els operaris d'intel·ligència traduïen els missatges i intentaven treure partit a la informació. El rafal 8 estava especialitzat en l'Enigma naval i passava els desxiframents al rafal 4 on intentaven treure-li partit a la informació. Al principi, Bletchley Park tenia un personal de no més de 200 persones, però en plena guerra, arribaria a un total de 700 homes i dones.

FIGURA 20: Bletchley Park.

Bletchley Park va tardar molt poc en familiaritzar-se amb l'Enigma i les tècniques poloneses, i en molt poc temps, ja les dominaven. Els desxifradors britànics exercien la mateixa rutina cada 24 hores. A mitjanit, els alemanys canviaven a una nova clau. Els desxifradors tenien la tasca de desxifrar la clau de cada dia. A vegades trigaven unes quantes hores, però en quant descobrien la clau, tot el personal de Bletchley Park començava a treballar per a desxifrar tots els missatges alemanys. Gràcies a Bletchley Park es s'havia abans d'hora el què anava a passar i poder advertir i saber tot el que passaria, és com jugar als escacs sabent els moviments que farà l'altre. Per a dir-ho d'alguna manera, llegien les ments dels alts càrrecs alemanys. Tota la informació aconseguida a Bletchley era passada directament a la seu central del MI6 (intel·ligència britànica) i al Almirallat(Office of the Admiralty and Marine Affairs, oficina del Almirallat i afers marins, la marina britànica bàsicament), que la remetia a la Oficina de Guerra o al Ministeri de l'Aire.

Una vegada dominades les tècniques poloneses, els criptoanalistes de Bletchley van desenvolupar els seus propis mètodes per a desxifrar els missatges alemanys. Es

van adonar que els operadors alemanys a vegades escollien claus molt obvies. Encara que se suposava que els operadors havien d'escollir tres lletres al atzar, en mig de la guerra a vegades no es posaven a pensar gaire en la clau i simplement teclejaven tres lletres consecutives en el teclat de l'Enigma, com per exemple QWE o BNM. Aquestes claus previsibles es van donar a conèixer com a **cilis**. Un altre cili era l'ús repetit de la mateixa clau, les inicials de la xicota de l'operador, o potser les seves inicials. Els criptoanalistes en comptes de començar directament a desxifrar l'Enigma de la manera difícil, primer perdien una mica de temps en provar les cilis, i, a vegades, valia la pena.

Hem d'aclarir que les cilis no són debilitats de la màquina sinó més aviat errors humans i/o debilitat de la manera de fer servir la màquina. Aquests errors humans van simplificar moltes vegades la tasca dels criptoanalistes. Per exemple, els responsables de redactar els llibres de codis van voler assegurar que les disposicions dels modificadors fossin imprevisibles, no permeten que cap modificador romangués en la mateixa posició durant dos dies seguits. A primera vista pot semblar una bona idea, però en realitat no ho és. Si descartem certes disposicions per a que un modificador romangui en la mateixa posició que el dia anterior significa que els redactors dels llibres de codis van reduir a la meitat el número de possibles disposicions dels modificadors. Els criptoanalistes de Bletchley es van adonar i van treure-li partit. En quant identificaven la disposició dels modificadors per un dia, immediatament podien descartar la meitat de les disposicions dels modificadors pel dia següent, reduint la seva feina a la meitat.

De manera similar, hi havia una regla que impedia que les posicions del claviller inclogués l'intercanvi entre qualsevol lletra i la seva veïna. En la teoria es pensava que aquests intercanvis obvis havien de ser evitats però, com abans, el compliment d'una regla redueix dràsticament el número de claus possibles.

Part de l'èxit de Bletchley Park és degut a la raríssima combinació de matemàtics, científics, lingüistes, addictes als mots encreuats, etc. Encara que hi van haver moltes figures importants a Bletchley, considero que he de destacar, nombrar i explicar la més important, la figura d'**Alan Turing**.

FIGURA 21: Alang Turing.

Alan Turing va néixer el 23 de juny de 1912 en Maida Vale, Londres. Fill d'un membre de l'administració pública Índia, cosa que va provocar que la major part del temps els seus pares estiguessin fora de casa i es passés la major part de la seva infantesa amb uns veïns. La seva intel·ligència ja es va fer notar des de ben petit. Als 9 anys, un dels seus professors li va dir a la seva mare: "he tingut nens intel·ligents i altres treballadors, però Alan és un geni". Turing es va canviar d'escola i va anar a la Hazelhurst Preparatory School l'any 1922. Els seus professors moltes vegades s'enfadaven amb ell per les bones notes que treia malgrat no prestar gaire atenció. Allà va conèixer el seu primer amor, Christopher Morcom. No obstant, la seva relació va ser truncada per la mort de Christopher l'any 1930 de tuberculosis.

Turing va entrar a estudiar matemàtiques a Cambridge l'any 1931. L'any 1934 es va graduar com el millor de la classe, i, a l'edat de 22 anys, va ser nomenat professor a Cambridge (Fellow of King's College). Turing va ser molt feliç durant la seva època a la universitat. No només perquè portava la vida idònia com a professor del King's College, casa de l'elit intel·lectual de tot el món, sinó perquè la homosexualitat era en gran mesura acceptada en la universitat. L'any 1939, la carrera acadèmica d'Alan es va veure compromesa. L'escola governamental de codis i xifres el va convidar a convertir-se en criptoanalista i el 4 de setembre de 1939, Turing es traslladà a Bletchley Park.

Hem de fer un petit parèntesis per a explicar que durant el seu doctorat i post doctorat, havia assistit a diverses reunions sobre la criptografia i el criptoanàlisi, sempre li havia interessat i li agradava molt, per això i per la seva excel·lència com a matemàtic va acceptar la invitació per a treballar a GC&CS (Government Codes and Cypher School).

Turing recorria cada dia 5 km des de Shentley Brook End fins a Bletchley Park. Es passava una gran part del temps en els rafals, ajudant al treball rutinari dels criptoanalistes, però també aprofitava part del seu temps per anar al centre de reflexió del grup d'experts, que abans de l'arribada del GC&CS havia sigut la botiga de fruites de Sir Herbert León. El centre de reflexió era on els criptoanalistes discutien i debatien sobre els nous problemes que podrien sorgir i com abordar-los. Turing es va centrar en què podia passar si els militars alemanys canviaven el protocol d'enviar els missatges. Fins ara, tot els avenços en el desxiframent de l'Enigma estaven basats en el treball de Rejewski, que aprofitava els patrons de repetició en la clau missatge. Turing i els seus companys van suposar que els alemanys no tardarien en adonar-se d'aquesta debilitat i que en qüestió de mesos canviarien el protocol, és per això, que el treball de Turing era trobar una manera alternativa d'atacar l'Enigma.

Estudiant els vells missatges desxifrats, creia que a vegades podia preveure part del contingut d'un missatge sense haver estat desxifrat prèviament, deia que ho podia saber basant-se en l'hora que s'havia enviat i en l'origen del missatge. Per exemple, l'experiència els deia que cada dia poc després de les sis del matí, un informe meteorològic era enviat. Per tant, un missatge interceptat a les sis i tres del matí podríem estar gairebé segurs que conté la paraula **wetter**, "temps" en alemany. Donat que totes les organitzacions militars segueixen un protocol molt rigorós, podem suposar que els missatges es redactaven amb un estil estrictament ordenat, de manera que es podia tenir molta confiança respecte la ubicació de **wetter** dins del missatge xifrat. L'experiència podia dir-li que les sis primeres lletres d'un text xifrat corresponien a les lletres del text original **wetter**. Quan tenim un fragment del text original que es pot associar amb un fragment del text xifrat, anomenem a aquesta combinació **puntal**.

Turing sabia que podia aprofitar els puntals per a desxifrar l'Enigma. Imaginem-nos que en un text xifrat sabem que una secció en específic, **ETJWPX**, representa **wetter**, llavors el desafiu serà identificar les posicions de la màquina per a que transformin **wetter** en **ETJWPX**. La manera directe, però gens viable, seria provar una a una cada possible clau, cosa inviable perquè has de comprovar aproximadament

159.000.000.000.000.000.000 de possibles claus.

L'objectiu era reduir el problema a xifres més accessibles, llavors Turing va seguir l'estratègia de Rejewski de separar els efectes de les posicions dels diferents components de la màquina. Volia separar el problema de descobrir quins modificadors estan en cada lloc i l'orientació que tenen amb el problema de descobrir els cablejats del claviller. Si aconseguís trobar un puntal que no tingués res a veure amb els cables del claviller, llavors la tasca es simplificaria enormement, ja "només" hi haurien 1.054.560 possibles orientacions dels modificadors (60 disposicions x 17.576 orientacions).

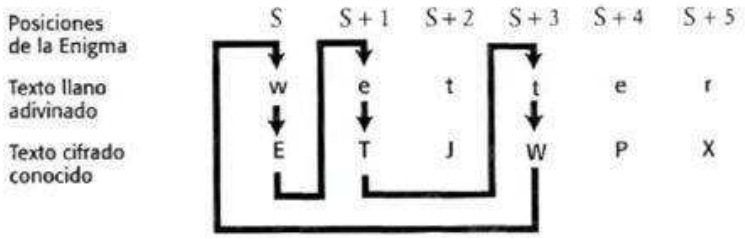


FIGURA 22: Funcionament esquemàtic dels rínxols.

Finalment, es va decidir per un tipus de puntal que té rínxols interns, similars a les cadenes utilitzades per Rejewski. A diferència de les cadenes de Rejewski, els rínxols de Turing no tenien res a veure amb la clau del missatge, els rínxols connectaven lletres del text original i lletres del text xifrat en un puntal. Si fem servir l'exemple anterior de la imatge i suposem que el puntal (en aquest cas **ETJWPX**) és correcte, llavors podem associar les lletres **w→E, e→T, t→W**. Encara que no coneixem ninguna de les posicions de la màquina Enigma, anomenarem **S** a la primera posició. Sabem que en **S** la **w** és codificada com a **E**. Després d'aquesta codificació, el primer modificador gira un lloc fins a la posició **S+1** i la lletra **e** és codificada com a **T**. El modificador torna a girar i arribem a la posició **S+3** on sabem que la lletra **t** és codificada com a **W**. Fins ara sabem que:

En la posició S, l'Enigma codifica w com E.

En la posició S+1, l'Enigma codifica e com T.

En la posició S+3, l'Enigma codifica t com W.

Turing va aprofitar aquest rínxols per a atacar l'Enigma. En comptes de treballar amb diverses Enigmes per a que anessin provant posició per posició, es va imaginar tres màquines separades, treballant cada una amb la codificació d'un element del rínxol. La primera màquina s'ocuparia de codificar **w** com **E**, la segona **e** com **T** i la tercera **t** com a **W**. Les tres màquines tindrien posicions idèntiques, excepte perquè la segona estaria una posició per davant respecte la primera i la tercera estaria tres posicions per davant respecte la primera. Llavors va pensar que podria connectar les tres màquines fent passar cables elèctrics entre els dispositius d'entrada i sortida de cada màquina. Va imaginar que les màquines canviarien les seves posicions del claviller i dels modificadors, per a trobar la clau, però el circuit elèctric de cables que connectaven les tres màquines només es tancaria quan totes les posicions fossin correctes per les tres màquines, permeten que l'electricitat circulés per les tres màquines. I si a sobre possés una bombeta al final del circuit, quan s'encengués estaria senyalant que el circuit està complert i que les màquines han trobat la clau.

Podries pensar que les màquines encara han de comprovar 159.000.000.000.000.000.000 possibles claus, doncs bé, per si ho estaves pensant, tens raó. Tot el que havia fet fins ara Turing no era més que la preparació pel salt lògic final, que simplificaria el problema en cent milions de milions de vegades.

Turing, havia construït el circuit elèctric de manera que s'anul·lés l'efecte del claviller.

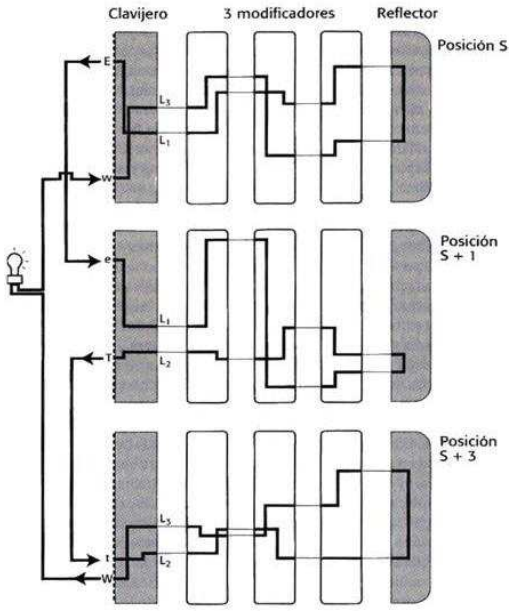


FIGURA 23: Esquema d'un prototip de la màquina que Turing estava creant.

Si ens fixem en la imatge, veiem com el corrent elèctric entra en els modificadors i surt per alguna lletra desconeguda, la qual anomenarem L_1. La corrent passa pel claviller, que transforma L_1 en E (recordeu que seguim amb el mateix exemple d'abans). Aquesta lletra E es connecta mitjançant un cable amb la lletra e de la segona Enigma i quan la corrent passa pel segon claviller es torna a transformar en L_1. O en altres paraules, els dos clavillers es contraresten. De la mateixa manera que abans, la corrent surt dels modificadors de la segona Enigma i entren en el claviller en L_2 abans de ser transformat en T. Llavors T es connecta mitjançant un cable amb la lletra t de la tercera Enigma, quan la corrent passa pel tercer claviller es torna a transformar en L_2. Els clavillers es contraresten durant tot el circuit, Turing ha aconseguit ignorar-los per complert.

Ja només necessitava connectar el dispositiu de sortida del primer joc de modificadors, L_1 directament al dispositiu de sortida del segon joc de modificadors, que també era L_1 de manera que va haver de connectar els 26 dispositius de sortida del primer joc de modificadors amb els 26 dispositius d'entrada corresponents del segon joc de modificadors, i successivament. És a dir, en comptes de tenir només un rínxols, ara tenia 26 rínxols, perquè com que no sabia quina lletra era, havia de tenir totes les lletres connectades perquè podia ser qualsevol. Per tant, en cada circuit havien d'haver 26 bombetes. Ara els modificadors només havien de provar les 17.576 orientacions, on el segon joc de modificadors sempre estigués un lloc per davant respecte el primer i el tercer dos llocs per davant respecte el segon, en aquest exemple. Quan els modificadors haguessin trobat les posicions correctes un dels circuits es completaria i s'il·luminaria una bombeta. Tot i això, encara hi havia dos problemes.

En primer lloc, podria ser que els modificadors estiguessin en un ordre incorrecte, perquè com ja sabem la màquina Enigma té cinc modificadors del qual cada dia es fan servir tres i ordenats en un ordre aleatori, donant 60 possibles disposicions. La solució a aquest problema seria tenir 60 jocs de tres màquines Enigmes funcionant en paral·lel.

En segon lloc, encara falta per descobrir els cablejats del claviller. Això és relativament senzill: utilitzant una màquina Enigma amb les disposicions i orientacions correctes dels modificadors, el criptoanalista tecleja el text xifrat

(**ETJWPX**) i observa el text pla resultant (**tewwer**). És evident que en el claviller s'hi han d'inserir els cables per a intercanviar la **w** i la **t**. Si teclegem altres parts del text podríem revelar la resta de cablejats del claviller. Aquestes màquines es van anomenar bombes en honor a Rejewski i també perquè tenien una certa semblança amb les bombes de Rejewski.

Cada una de les bombes de Turing tenia dotze jocs de modificadors Enigma connectats elèctricament, podent afrontar rínxols de lletres molt més llargs. Les bombes de Turing mesuraven 2x2x1 metres. La primera bomba va arribar el 14 de març de 1940 amb el nom de *Victory*. La màquina va resultar molt més lenta del que s'esperava i al principi tardava fins una setmana en trobar una clau. En poques setmanes però amb l'ajuda dels seus companys van presentar un disseny modificat, el qual funcionaria tal i com es pensava. El 10 de maig de 1940 els alemanys van canviar el seu protocol d'intercanvi de claus, cosa que el nombre de desxiframents satisfactoris de l'Enigma van caure en picat. L'apagada d'informació es va acabar el dia 8 d'agost, dia d'arribada de la segona bomba.

En menys d'un any i mig hi havia 15 bombes més funcionant, aprofitant els puntals i revelant claus. Si no hi havia cap contratemps, una bomba podia trobar una clau de l'Enigma en menys d'una hora. Una vegada s'havien establert els cablejats del claviller i les posicions i orientacions dels modificadors (la clau missatge) per a un missatge en particular, deduir la clau del dia es convertia en bufar i fer ampolles. Llavors, tota la resta de missatges enviats d'aquell dia també es podien desxifrar.

Per a que una bomba pogués començar a buscar una clau primer s'havia de trobar un puntal i no hi havia cap garantia de que el puntal fos correcte. Inclús, podria ser que el puntal fos correcte però no estigués en la posició correcta, donant pas a un fals negatiu. Per sort, hi havia un enginyós per a saber si un puntal estava en la posició correcte.

En el següent puntal, el criptoanalista creu que el puntal és correcte però no està segur si està associat amb les lletres apropiades del text xifrat.

FIGURA 24: puntal.

Una de les característiques de la màquina Enigma és que no pot codificar una lletra com a ella mateixa, a causa del reflector. La lletra N mai podrà ser codificada com a N, per tant, sabem que el puntal anterior està malament alineat, perquè la e codifica com a e i com acabem d'explicar, l'Enigma és incapaç de codificar una lletra com a ella mateixa. Llavors, l'únic que hem de fer és moure el text original fins que no tinguem cap codificació no possible. En el nostre cas només hem de moure el puntal un lloc cap a la dreta.

Els experts diuen que gràcies a Turing, es va escurçar la durada de la guerra en dos anys i va salvar aproximadament 14 milions de vides.

Hem de tenir en compte que durant tota la guerra i anys posteriors, només unes poques persones s'havien del descobriment d'Alan i que gràcies al seu enginy s'havia guanyat la guerra. Les úniques persones que ho sabien eren aquelles que havien treballat a Bletchley Park i els alts càrrecs polítics i militars. A Bletchley, Alan era considerat un geni i una eminència, però una vegada la guerra havia acabat, tothom va tornar a fer vida normal, com si no hagués passat mai res. Ningú sabia que un grup de persones, científics, lingüistes, matemàtics... havia treballat nit i dia per al seu país i que en gran part, la guerra havia acabat gràcies a ells. Eren herois que havien caigut en l'anonimat i ningú en sabia de la seva existència. Fins i tot se'ls tractava com a desertors perquè es pensava que no havien fet res pel seu país quan més ho necessitava, quan en realitat, ho havien donat tot.

Aquest anonimat va durar tres dècades, fins que el capità F.W. Winterbotham, responsable de distribuir la intel·ligència Ultra (Ultra era el nom de l'operació d'intel·ligència britànica en la qual participava Turing i tot Bletchley Park), va atacar al govern britànic al·legant que la xifra Enigma ja no es feia servir i que volia fer un llibre explicant tot el que havia passat a Bletchley Park. El llibre va ser publicat l'estiu del 1974, titulat *The Ultra Secret*, permeten als membre del personal de Bletchley la seva llibertat de poder parlar i explicar el que havien viscut durant la guerra. Finalment, havien rebut el reconeixement que mereixien. Tota Anglaterra es va assabentar i ja no van caure mai més en l'oblit.

Per desgràcia, no tots els treballadors de Bletchley van viure el suficient per a rebre un reconeixement públic. Aquest és el cas d'Alan Turing.

L'any 1952, mentre denunciava un robatori a la policia, sense voler va revelar que mantenia una relació homosexual. La policia el va detenir i va ser acusat d'incomplir la Secció 11 del Acte d'Esmena de la Llei Penal de 1885. Els diaris van fer públic el seu judici i Turing va ser humiliat públicament. Per si no fos suficient, se'l va prohibir treballar en projectes d'investigació, concretament aquells relacionats amb el desenvolupament de l'ordinador. A més, el van obligar a consultar a un psiquiatra i a sotmetre's a un tractament d'hormones, i, si no ho acceptava aniria a presó. Tot això li va causar una greu depressió i el 7 de juny de 1954, es va suïcidar amb cianur i una poma. Amb només 52 anys, una de les ments més brillants del segle XX, acabava de suïcidar-se.

3. Criptografia moderna i els seus orígens

3.1 El naixement de la criptografia de clau pública (RSA)

Després de la segona guerra mundial, els criptoanalistes van seguir amb el desenvolupament dels recents inventats ordinadors per a poder atacar les noves xifres. Ara podien aprofitar la velocitat i flexibilitat que els ordinadors programables els hi proporcionaven. Evidentment, al igual que al llarg de tota la història, els criptògrafs van contraatacar aprofitant el poder de les noves màquines programables inventades. Podem afirmar que l'ordinador causarà un impacte enorme en el transcurs de la guerra entre els codificadors i descodificadors.

En general, utilitzar un ordinador, per a codificar o desxifrar, és molt similar a la manera tradicional, però amb tres petites diferències. La primera, una màquina de xifres mecànica té limitacions pràctiques i tècniques, en canvi un ordinador pot imitar el funcionament d'una màquina mecànica hipotètica, on la seva xifra podria ser immensament més complexa. La limitació recau en el fet que jo puc crear una màquina virtual, exactament igual a una hipotètica màquina real i que no té cap limitació física. A mi no em costaria diners crear una màquina Enigma virtual, però en canvi la utilització de recursos i diners necessaris per a construir una Enigma són enormes. Amb un ordinador, puc generar aquesta mateixa màquina mecànica però sense costos. La segona diferència és el factor velocitat, simplement l'electrònica

funciona molt més ràpidament que un modificador mecànic, per exemple. Dit d'una altre manera, en el món virtual no existeixen les limitacions físiques.

La tercera diferència i alhora la més important, un ordinador modifica números en comptes de lletres d'un alfabet. Els ordinadors operen amb números binaris: seqüències d'uns i zeros, també coneguts com **dígits binaris**, o si ho abreviem, **bits**. Si suposem que volem codificar un text en l'idioma dels ordinadors, primera hauré de trobar un mecanisme que converteixi el meu missatge en el llenguatge dels ordinadors. Per tant, necessitem un sistema que faci d'intermediari entre el món dels bits i les llengües tradicionals, un conjunt de regles que relacionin el nostre alfabet amb els bits. Aquesta conversió s'anomena American Standard Code for Information Interchange (Codi estàndard americà per a l'intercanvi d'informació), comunament conegut pel acrònim **ASCII**.

Aquest conjunt de regles i protocols a seguir, assigna un número de set dígits a cada lletra de l'alfabet (quedem-nos amb la idea, de moment, que un **número binari** és simplement un patró d'uns i zeros que identifica únicament a cada lletra).

En total, hi ha 128 maneres (2^7) d'ordenar una combinació de set dígits binaris, de manera que ASCII pot identificar fins a 128 caràcters. A part de les 26 lletres de l'alfabet, ens deixa espai, a l'haver-hi 128 caràcters possibles, per a definir també les lletres minúscules, la puntuació i altres símbols. Una vegada que haguem convertit el missatge en números binaris, ja podrem començar amb la codificació.

Números binaris ASCII per a les lletres majúscules:					
A	1000001	J	1001010	S	1010011
B	1000010	K	1001011	T	1010100
C	1000011	L	1001100	U	1010101
D	1000100	M	1001101	V	1010110
E	1000101	N	1001110	W	1010111

F	1000110	O	1001111	X	1011000
G	1000111	P	1010000	Y	1011001
H	1001000	Q	1010001	Z	1011010
I	1001001	R	1010010		

Tot i està tractant amb ordinadors, la codificació se segueix regint pels principis de sempre, la substitució i la transposició. Tota codificació, no importa quan complexa sigui, es pot descompondre en combinacions de substitucions i transposicions.

Imaginem que volem codificar el missatge **HELLO** utilitzant una simple versió informatitzada d'una simple xifra de transposició. Una de les transposicions més simples és intercanviar els dígits primer i segon, tercer i quart i successivament.

Text original = HELLO= 1001000100010110011001001100100

Text xifrat = 0110001000101001100110001100011101

Una característica interessant de la transposició a nivell de dígits binaris és que la mateixa transposició pot succeir en la mateixa lletra, al estar formada per 7 dígits binaris. Aquest missatge codificat és enviat al receptor, i aquest, invertint el procés i reinterpretant els dígits binaris amb ASCII, obté el missatge original.

Tornem a imaginar que volem codificar el mateix missatge que abans, **HELLO**, però aquesta vegada utilitzant un sistema de substitució computeritzat. Com ja sabem, la substitució està basada en una clau ja acordada prèviament a la codificació, entre emissor i receptor. En aquest cas, les dues parts han arribat al acord d'utilitzar la clau **DAVID**, evidentment ja traduïda a ASCII. En el sistema computacional funciona parcialment diferent. Cada element del text original "s'afegeix" a l'element corresponent de la clau. Per a entendre què vol dir afegir dígits binaris, hem d'entendre dues regles bàsiques d'aquest sistema. Si els elements del text original i de la clau coincideixen, és a dir que són el mateix número, l'element del text original és substituït per 0 en el text xifrat. Si per contra, l'element del text original i de la clau

no coincideixen, no són el mateix número, l'element del text original és substituït per 1 en el text xifrat:

Missatge: HELLO

Missatge en ASCII: 1001000100010110011001001100100

Clau = DAVID

Text xifrat: 0001100000010000011010000001

El missatge codificat s'envia al receptor i utilitzant la mateixa clau per a invertir la substitució, aconsegueix la sèrie de dígits binaris del missatge original, ja només s'haurà d'utilitzar l' ASCII per a poder llegir-lo.

Al principi, la codificació per ordinador estava disponible per només aquells que tenien accés als ordinadors, principalment l'exèrcit i el govern. No obstant, l'any 1951 la computació comercial va començar a ser una realitat i en 1953 IBM va comercialitzar el seu primer ordinador (quatre anys més tard també va publicar el llenguatge de programació Fortran, que permetia que la gent pogués escriure programes d'ordinador).

Durant la dècada dels setanta els ordinadors es van anar tornant cada vegada més potents i accessibles. Les empreses es podien permetre tenir ordinadors que a la seva vegada els podien utilitzar per a codificar les comunicacions importants, com per exemple, les transferències bancàries o negocis comercials. Degut a aquest increment massiu de les telecomunicacions, els criptògrafs es van trobar nous problemes. Un d'aquests problemes era l'estandardització. És a dir, una empresa podria utilitzar un sistema d'encriptació en concret per a tenir seguretat en les comunicacions internes, però no podia enviar missatges secrets a una altre organització. És per això que l'Oficina Nacional d'Estàndards nord-americans va planejar resoldre el problema.

Encara que aquesta part de la història és interessant, la veritat és que el sistema que feien servir i com funcionava no és rellevant per a aquest punt, simplement anomenaré el nom i què va provocar aquesta estandardització.

L'any 1976 es va desenvolupar el DES (Data Encryption Standard), resolvent el problema de l'estandardització i animant a les empreses a utilitzar la criptografia per

a la seva seguretat. Aquest sistema era suficientment potent com per garantir que era impossible que una companyia amb un ordinador civil pogués penetrar en un missatge codificat amb DES, perquè el número de claus era massa gran.

Per molt que s'hagués solucionat el problema de l'estandardització encara hi havia un problema per a solucionar, i aquest, era un dels grans. El problema de la distribució de claus.

Com ja sabem, aquest problema ha estat des del principi de la criptografia. Per exemple, en la segona guerra mundial, quan els alemanys havien de distribuir el llibret amb les claus cada mes, o amb la xifra Vigenère, que entre emissor i receptor havien de compartir la clau. Independentment de quant bona sigui la teoria, després en la pràctica pot ser derrocada pel problema de la distribució de claus.

Malgrat que molts experts no pensaven que era possible solucionar aquest problema, a continuació us ensenyaré les dues primeres solucions que es van trobar a aquest problema.

3.1.1 Diffie-Hellman-Merkle

La primera solució a la distribució de claus va ser portada a terme per **Whitfield Diffie**. Diffie va néixer l'any 1944 a Washington, tot i que la major part de la seva infància la va passar a Queens, Nova York. Va estudiar matemàtiques al MIT (Massachusetts Institute of Technology) i després de graduar-se, va treballar en diferents llocs relacionats amb la seguretat informàtica, també conegut com ciberseguretat. Cap als anys setanta es va convertir en un dels pocs experts en seguretat vertaderament independents, un criptògraf no empleat pel govern o per una gran companyia.

En aquesta època ja estava molt interessat en el problema de la distribució de claus i era plenament conscient que qui trobés una solució passaria a la història com un dels millors codificadors de la història. Aquesta obsessió amb la distribució de les claus li venia donat per la seva visió d'un món interconnectat, era un visionari que creia que algun dia tothom tindria el seu propi ordinador i que aquests ordinadors estarien interconnectats mitjançant les línies telefòniques.

Hem de recordar que Internet no va néixer fins a finals dels anys vuitanta, i en aquest moment hi havia una versió molt primitiva de l'internet i encara estava en les primeres fases de desenvolupament. Diffie, era un visionari. Fins i tot, es preguntava com es podria comprar per internet, com una persona podria enviar un e-mail amb detalls de la seva targeta de crèdit i que només el venedor en particular pogués desxifrar aquest missatge. Diffie estava preocupat que si no es trobava solució a aquest problema, totes aquestes fantasies no s'arribarien mai a complir.

Diffie va ser convidat a donar una xerrada a un laboratori d'IBM. Va parlar sobre el problema de la distribució de claus i algunes estratègies per poder atacar el problema, però el públic es va mostrar molt escèptic per les seves idees extravagants i no va tenir gaire èxit entre la multitud. Per sort, a través d'un veterà de l'IBM, va aconseguir el contacte d'un criptogràf que també abordava el tema de la distribució de claus i Diffie va decidir que l'havia de conèixer i que havien de treballar junts. L'aliança entre aquests dos es convertiria en una de les associacions més dinàmiques de la criptografia.

Martin Hellman va néixer l'any 1946 en un barri jueu en el Bronx, Nova York. Va estudiar enginyeria elèctrica a Nova York i després de graduar-se va realitzar un màster a Stanford.

Diffie va convèncer a Hellman per a treballar junts i Hellman va acceptar. Van començar intentant resoldre el problema de la distribució de claus físicament. Al cap d'un temps, Ralph Merkle també se'ls va unir.

El problema de la distribució de claus és la típica situació de cercle viciós. Si l'emissor vol intercanviar un missatge secret per telèfon, primer l'haurà de codificar. Per a poder codificar-lo, l'emissor a d'utilitzar una clau, que a la vegada també és secreta, de manera que es genera el problema de transmetre la clau secreta al receptor per a poder transmetre el missatge secret. Abans que els dos puguin intercanviar un secret, és a dir, el missatge codificat, han de compartir un secret, la clau.

A partir d'ara, cada vegada que considerem un problema per a la distribució de claus farem servir els següents personatges, en Bernat, l'Alícia i l'Eva, que són tres personatges ficticis que s'han convertit en els estàndards de les discussions criptogràfiques. Normalment, suposarem que Alícia està enviant missatges secrets a

Bernat, o al revés, i Eva intenta assabentar-se. Cada vegada que l'Alícia vulgui enviar missatges a en Bernat, primer els haurà de codificar, utilitzant una clau diferent per a cada missatge. Contínuament Alícia es trobarà amb el mateix problema, haurà de transmetre les claus a Bernat de forma segura, sinó no podrà descodificar mai els missatges.

Una solució seria que quedessin una vegada a la setmana i s'intercanviessin suficients claus per a cobrir tots els missatges que podrien enviar durant la següent setmana. Intercanviar els missatges en persona és molt segur, però també té molts inconvenients. Si un dels dos no pot assistir per qualsevol problema, llavors tot el sistema falla. Una altra solució seria que contractessin a missatgers, però seria menys segur i més car. Totes les possibles solucions semblaven fallar, però Diffie i Hellman sabien que havia una que semblava desafiar al sistema.

Imaginem que Alícia vol enviar un missatge molt important a Bernat però sap que el sistema postal està controladíssim per l'Eva i suposarem que ha subornat a tot el sistema postal per als seus propis interessos, de tal manera que el sistema postal és corrupte. Per a poder enviar el missatge l'Alícia el col·loca dins d'una caixa de ferro, la tanca i col·loca un cadenat. Porta la caixa amb el cadenat i la carta a dins a correus i es queda amb la clau. No obstant, Bernat no la podrà obrir perquè no té la clau. Alícia podria pensar en posar la clau en una altre caixa de ferro, tancar-la amb un altre cadenat i enviar-la, però seguiria trobant-se amb el mateix problema. L'única manera d'evitar aquest problema és fent una copia de la clau, quedar amb Bernat i donar-li la copia. Fins ara, hem plantejat el mateix problema però canviant les interpretacions. Sembla ser que l'intercanvi de claus és inevitable. L'única manera que té en Bernat d'obrir la clau és amb una còpia de la clau, o en termes criptogràfics, l'única manera que té en Bernat de llegir el missatge és obtenint la clau per a desxifrar-lo. Llavors, podem afirmar que l'intercanvi de la clau és una part inevitable de la codificació, o no?

Imaginem-nos la següent situació. L'Alícia vol enviar un missatge molt important a en Bernat (quina sorpresa). Com abans, agafa el missatge i el posa dins de la caixa de ferro, posa un cadenat, es queda amb la clau i l'envia. Quan la caixa arriba, en Bernat afegeix el seu propi cadenat i torna a enviar la caixa a l'Alícia. Quan l'Alícia rep la caixa, aquesta està tancada pels dos cadenats. Retira el seu cadenat, deixant

només el cadenat d'en Bernat. Per acabar, torna a enviar una vegada més la caixa a en Bernat. I aquí està la gran diferència: ara en Bernat pot obrir la caixa perquè està tancada només pel seu propi cadenat. Per primera vegada apareix una petita prova de que l'intercanvi de claus podria no ser una part inevitable de la criptografia.

En temes criptogràfics la situació seria la següent: Alícia vol enviar un missatge a en Bernat. L'Alícia el codifica i l'envia a en Bernat, quan el missatge li arriba en Bernat, torna a codificar amb la seva pròpia clau i el torna a enviar. Una vegada l'Alícia el rep, ella retira la seva pròpia descodificació i el torna a enviar. Finalment, en Bernat retira la seva codificació i ja pot llegir el missatge original.

Pot semblar que el problema ja està solucionat, però en realitat no. El problema radica en que l'ordre de codificació i descodificació importa. L'ordre de codificació i descodificació és importantíssim. Hem d'obeir a la màxima "**l'últim que es posa és el primer que es treu**".

L'última fase de codificació ha de ser la primera en ser descodificada. És com si volguéssim treure'ns primer els mitjons amb les sabates posades. És impossible treure's els mitjons abans que les sabates. Hem d'obeir a la màxima.

És veritat que per exemple en la xifra del Cèsar l'ordre no importa, no obstant, les xifres de codificació fortes i complexes que es feien servir en els anys setanta sempre havien de complir la regla de "l'últim que es posa és el primer que es treu".

Encara que la història de la caixa tancada amb dos cadenats no funcionarà en la criptografia de la vida real, inspiraria a Diffie i Hellman a buscar un mètode pràctic per a resoldre el problema de les distribucions de claus.

La seva investigació es va centrar en els funcions matemàtiques. Una funció matemàtica és una correspondència entre dos conjunts de forma que cada element del conjunt inicial (la variable independent, la X, el Domini, com li vulguis dir) li correspon un únic element del conjunt final (variable independent, Y o la Imatge). La definició més senzilla i pràctica és que tota funció és una operació matemàtica que converteix un número en un altre. Llavors, podem considerar que totes les formes de codificació per ordinador són com les funcions, perquè converteixen un número, el text original, en un altre número, el text xifrat.

La majoria de les funcions estan classificades com a funcions de doble via, és a dir, que són fàcils de fer i desfer. No obstant, Diffie i Hellman no estaven interessats en aquests tipus de funcions. De fet, es van centrar en les funcions d'una via. Al contrari que les de doble via, aquestes són molt fàcils de fer però molt complicades de desfer. Diem que són funcions irreversibles. Per exemple, és molt fàcil barrejar pintures però és molt difícil tornar a separar-les. O per exemple, és molt fàcil arrugar un foli però és gairebé impossible tornar-lo en l'estat inicial, encara que amb una bona planxa de vapor queda prou bé.

Investigant en aquest camp de les funcions d'una via van trobar una branca de la matemàtica molt interessant, l'**aritmètica modular**. L'Aritmètica modular, també coneguda com aritmètica de rellotge, és una àrea de les matemàtiques on hi ha moltíssimes funcions d'una via. En l'aritmètica modular, els matemàtics consideren un grup finit de nombres disposats en un cercle, de manera molt similar a un rellotge.

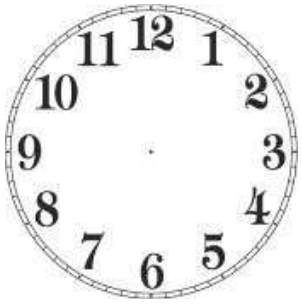


FIGURA 25: Rellotge de paret.

En la imatge superior podem apreciar un rellotge amb les seves respectives hores. En aquest cas, el rellotge és un modular 12 (mod 12), ja que va del 1 al 12. Si volem calcular 3+4, comencem des de la posició del 3 i avancem 4 llocs endavant fins arribar al 7, que és la mateixa resposta que l'aritmètica normal. Ara volem calcular 10+5, comencem des de la posició del 10 i avancem 5 llocs fins a arribar al 3, cosa que ja no és igual a la aritmètica normal.

$$2+3=5 \ (mod\ 12) \qquad 10+5=3 \ (mod 12)$$

El modular 12 és molt utilitzat en la vida quotidiana, ja que l'utilitzem per a les hores del dia. Si ara són les 7 del matí i tenim una reunió d'aquí a sis hores, direm que tenim una reunió a la una no a les tretze, per norma general.

Podem fer servir la modulació que vulguem, en aquest cas he fet servir la mateixa que fem servir per a les hores però en realitat podries fer servir el número que volguessis. Normalment, els matemàtics no s'imaginen l'aritmètica modular com a rellotges sinó que fan servir directament càlculs modulars. Primer, realitzem el càlcul desitjat en aritmètica normal. Segon, si volem saber la resposta en modular de x o (mod x), dividim el resultat obtingut anteriorment entre x i anotem la resta que ens queda, és a dir, nombres sencers, ens oblidem dels decimals. La resta que ens queda és la resposta en (mod x). Per a trobar la resposta 14 x 23 (mod 16), seguim els passos anteriors:

$$14 \cdot 23 = 322$$

$$322 \div 16 = 20, \ i \ resten \ 2$$

$$14 \cdot 23 = 20 \ (mod \ 16)$$

Les funcions en aritmètica modular tendeixen a comportar-se de manera irregular, convertint-les a vegades en funcions d'una via. Cosa molt obvia si ho comparem amb una simple funció d'aritmètica normal. Per exemple, agafem la funció 2^x i comparem els resultats entre l'aritmètica normal i la modular:

x	1	2	3	4	5	6	24
2^x	2	4	8	16	32	64	16777216
$2^x \ (mod \ 5)$	2	4	3	1	2	4	1

Si tenim 2^x i el resultat és igual a 16, és fàcil suposar que la x = 4, perquè 2 elevat a 4 dona 16. Però inclús si fem l'error de suposar que x és 3, calcularíem $2^3 = 8$ i ens adonaríem que estem equivocats, que el resultat és massa baix. Llavors tornaríem a provar amb un número més gran fins a arribar al resultat. En l'aritmètica normal podem provar números i adonar-nos si ens apropem o allunyem del resultat. En canvi, en l'aritmètica modular la mateixa funció es comporta irregularment.

L'única manera de saber el resultat d'una funció en aritmètica modular és fer una taula de valors. Les taules són molt útils quan els números són relativament petits, però ara imagina't haver de fer una taula de la funció $232^x \ (mod \ 23.456)$. L'aritmètica modular és un clar exemple de funcions d'una via. Jo et dono un resultat, 640, a mi

només m'ha costat uns segons en fer els càlculs i en canvi a tu et portarà mitja vida en calcular x.

$$232^{31} \ (mod\ 23.456) = 640$$

Al cap de dos anys de recerca van arribar a una possible estratègia pel problema de la distribució de claus. L'any 1976, Hellman va demostrar que Alícia i Bernat podien obtenir una clau sense haver de reunir-se. La seva idea estava basada en una funció d'una via de la forma $Y^x \ (mod\ P)$. Per a començar, Alícia i Bernat acorden uns valors per a Y i P. Poden utilitzar gairebé qualsevol valor però hi ha unes quantes restriccions, com per exemple que Y ha de ser un número més petit que P. Els valors no són secrets i aquest valors poden ser compartits per via telefònica, per posar un exemple. Encara que la línia de telefònica no sigui segura i l'Eva pugui saber què es diu en la conversa, és a dir, l'intercanvi d'informació, no podrà fer res amb aquesta informació i més endavant ho veurem. Sense reunir-se Alícia i Bernat hauran aconseguit establir una clau. Aquest procés es va aconseguir gràcies a que la clau secreta es va acordar mitjançant un intercanvi d'informació en una línia telefònica, però, i si l'Eva sabia en tot moment que estava passant, també sabrà la clau, no?

Fase Prèvia	Acorden que la funció és $7^x \ (mod\ 13)$.	
Fase 1	Escull un número, el 5 i el manté en secret. Direm al seu número A.	Escull un número, el 7 i el manté en secret. Direm al seu número B.
Fase 2	Col·loca el 4 en la funció i calcula el resultat de la funció $7^A \ (mod\ 13) = 7^5 \ (mod\ 13) = 16807 \ (mod\ 13) = 11$	Col·loca el 7 en la funció i calcula el resultat de la funció $7^B \ (mod\ 13) = 7^7 \ (mod\ 13) = 823543 \ (mod\ 13) = 6$
Fase 3	Al resultat li diu α i envia el resultat, 11, a en Bernat.	Al resultat li diu β i envia el resultat, 6, a l'Alícia
L'intercanvi	Podríem pensar que en l'intercanvi d'informació és un moment clau per a poder interceptar la informació i així poder atacar al sistema que estan utilitzant. L'Eva podria interceptar la trucada on l'Alícia i en Bernat s'intercanvien els valors de Y i de P i també els valors 6 i 9. No obstant, com que aquests números no són la clau realment és irrellevant que l'Eva els sàpiga, per tant no importa i no afecta a la seguretat del sistema.	

Fase 4	Amb el resultat que obté Bernat, Alícia calcula $\beta^A \pmod{13} = 6^5 \pmod{13} = 7776 \pmod{13} = 2$	Amb el resultat que obté Alícia, en Bernat calcula $\alpha^B \pmod{13} = 11^7 \pmod{13} = 19487171 \pmod{13}$
La clau	L'Alícia i en Bernat han arribat al mateix número, 2, i aquest, serà la seva clau.	

El sistema Diffie-Hellman-Merkle d'intercanvi de claus permet que l'Alícia i en Bernat estableixin un secret a través d'una conversació pública. Tot i que aquest sistema va comportar una revolució en el camp de la criptografia, el sistema no era perfecte, ja que tenia un inconvenient. Per a poder establir una clau es necessita un intercanvi mutu d'informació. Suposem que l'Alícia vol enviar un missatge a en Bernat però en Bernat està en Nova York, mentre que l'Alícia es troba a Barcelona. Per a que Alícia pugi codificar el seu missatge, necessita primer acordar una clau amb en Bernat, i és probable que quan l'Alícia vulgui enviar-li el missatge, en Bernat probablement estarà dormint. Poden fer dues coses, o bé l'Alícia s'espera a la resposta de Bernat, és a dir envia part de l'intercanvi de clau i espera a que s'aixequi o es connecten al mateix temps. El sistema de Hellman d'intercanvi de claus frena la espontaneïtat del e-mail, i en general de la comunicació per internet. Ara només calia esperar que arribés algú i s'inventés un sistema més eficaç per acabar d'una vegada per sempre amb el problema de la distribució de claus.

3.1.2 RSA (Rivest Shamir Adelman)

Les persones que van decidir acceptar el repte de trobar un sistema més eficaç per a la distribució de claus van ser Ronald Rivest, Adi Shamir i Leonard Adelman. Al principi van començar el projecte Rivest i Adelman, quan Rivest el va convèncer que podien haver certes matemàtiques interessants al darrere del problema de la distribució de claus, i junts, van intentar trobar la funció d'una via que tingués els requisits d'una xifra asimètrica. Adi Shamir se'ls uniria poc després de començar. Els tres treballaven en el vuitè pis del laboratori d'informàtica del MIT.

En poques paraules, formaven l'equip perfecte. Rivest era bàsicament un geni de la informàtica i tenia una habilitat desmesurada per aplicar les noves idees en llocs improbables. Sempre estava al dia amb els articles científics i és per això que estava constantment trobant noves possibles funcions d'una via que complissin els requisits

d'una xifra asimètrica. No obstant, totes les possibles funcions, d'una o altre forma, fallaven. Shamir, també informàtic, era capaç de distingir molt ràpidament l'essència del problema, ja que era molt intel·ligent. Ell també aportava noves funcions, però de la mateixa manera que Rivest, no arribaven gaire lluny. Per últim i no menys important estava Adelman, era un excel·lent matemàtic i era l'encarregat de trobar els erros en les idees de Rivest i Shamir, a més de tenir una enorme paciència i energia. Durant un any, Rivest i Shamir es van dedicar a trobar possibles solucions i Adelman, a tirar per terra les seves idees. Podríem dir que van començar a perdre una mica l'esperança, però el que no sabien és que el fracàs no és més que una part del procés de la investigació, i al cap d'un temps, van trobar allò que buscaven.

L'abril del 1977, després de celebrar el dia de pasqua tots junts, com que Rivest no podia dormir se'n va anar al sofà a llegir un llibre de matemàtiques, i com era d'esperar, s'adormí. Al cap d'una estona, com per art diví, va tenir una revelació i es va passar tota la nit formalitzant la seva idea. Avanç de que sortís el sol, Rivest ja havia escrit un article científic complert. Encara que la "revelació" l'havia tingut ell, considerava que sense l'ajuda de Shamir i Adelman, no ho hagués aconseguit mai i és per això que va finalitzar l'article anomenant-los a ells també. Entre els tres van decidir que el sistema es diria RSA, el qual es convertiria en la xifra més utilitzada de la criptografia moderna, inclús, avui en dia ho segueix sent, però d'això en parlarem més endavant.

Per a trobar la funció que complís les característiques de xifra asimètrica, buscaven principalment dues propietats:

1r. L'Alícia ha de crear una clau pública, per a que tothom (tot el món, si) pugui fer-la servir per a codificar els missatges dirigits a ella. Com que la clau pública és una funció d'una via han de trobar una funció que sigui impossible per a ningú invertir i descodificar els missatges d'Alícia.

2n. Això si, l'Alícia necessita descodificar els missatges que li envien. És per això que ha de tenir una clau privada, una informació que només sàpiga ella i que li permeti invertir el procés de la clau pública. Per tant, l'Alícia (i recordem que només l'Alícia) té el poder per a descodificar qualsevol missatge que hagi estat codificat prèviament amb la seva clau pública.

La peça fonamental de la xifra asimètrica de Rivest és que és una funció d'una sola via basada en el tipus de funcions modulars, l'aritmètica modular, ja descrites amb anterioritat. La funció de Rivest s'utilitza per a codificar un missatge, que en realitat aquest missatge és un número, el qual juntament amb la funció genera el text xifrat, un altre número.

Explicació RSA:

A continuació explicarem el procés a seguir per a codificar i descodificar en RSA.

Per a facilitar l'explicació, utilitzarem números petits, però tingues en compte que els valors utilitzats són molt i molt grans (en el següent exemple farem servir números d'una i dos xifres, un número ínfim si el comparem amb les 300 xifres que es fan servir per a garantir la seguretat de les transaccions bancàries), per a garantir la seguretat del sistema (més endavant veurem perquè han de ser números tan grans).

Per a poder fer la codificació del nostre missatge, prèviament hem d'escollir una sèrie de números, seguint unes normes, per tal de poder garantir la seguretat.

Comencem escollint dos números prims gegants, en aquest cas escollirem el 3 i el 13. Aquest nombres els anomenarem **p** i **q** respectivament (**p**= 3 i **q**=13). Llavors multipliquem els dos números primers i obtenim **N**, $N = p \cdot q$.

$$N = p \cdot q$$

$$N = 3 \cdot 13$$

$$N = 39$$

Una vegada tenim el número N, hem de fer una llista de 1 fins a N (en aquest cas de 1 fins a N=39) i treure tots els factors comuns de N. Això vol dir que només hem deixar en la taula aquells números que no tinguin cap factor en comú amb N.

El total de nombres que tinguem, serà el valor de φ, que en aquest cas és 24 (φ =24). Hi ha un altre mètode molt més ràpid per aconseguir el valor de φ .

$$\phi = (p - 1) \cdot (q - 1)$$

$$\phi = (3 - 1) \cdot (13 - 1)$$

$$\phi = (2) \cdot (12)$$

$$\phi = 24$$

Ara hem d'escollir la clau per a encriptar, que li posarem la lletra **e** (e= encryption key). Per a poder escollir el valor de **e** hem de fer servir la següent fórmula:

$$e = \frac{(x \cdot \phi + 1)}{d}$$

La lletra **d** és la clau de descodificació, per consegüent podem deduir que el número de codificació i descodificació estan estretament units per aquesta relació:

$$e \cdot d = x \cdot \phi + 1$$

Haurem de donar valors a **x** i **d** (si busquem **e**) per tanteig i observar què passa, fins a trobar el valor desitjat. Com sabrem quin valor busquem? Doncs bé, per a trobar **e** hem de seguir uns paràmetres:

- $1 < e > N$, és a dir, **e** ha de ser més gran que 1 però més petit que **N**, que en aquest cas és 39, $[2, 3, 4, \ldots, 39)$.
- Per últim, el número ha de ser coprim amb φ (24) i amb **N**(39). Després de tantejar, trobem que:

$$e = \frac{(6 \cdot 24 + 1)}{5}$$

$$e = \frac{(145)}{5}$$

$$e = 29$$

- Per tant, també trobem d, $d = 5$.
- Per a poder desxifrar el missatge, necessitem informació addicional a part de **e** i **N**, aquesta informació adicional només la podrà aconseguir aquell que sàpiga **q** i **p**, els dos nombres prims que multiplicats entre ells donen **N**. No obstant, la persona que tingui la informació dels nombres prims haurà de calcular un número especial, al qual li direm **d** (clau de descodificació).

Ja tenim la nostra clau pública, $(N, e) = (39, 29)$.

Com ja sabem, aquesta informació permetrà a qualsevol persona enviar-nos un missatge encriptat i només nosaltres serem capaços de poder invertir el procés.

Perquè una persona pugui codificar un missatge fent servir RSA, ha de seguir uns passos en concret: El missatge que farem servir serà ***xifrat***. Per a poder codificar una paraula, necessitem primer passar les lletres a números, i per a fer-ho podríem utilitzar un llenguatge ja utilitzat, com per exemple ASCII. Tot i això, m'he pres la molèstia d'inventar-me un llenguatge (molt senzill i no gaire funcional) per a poder mantenir una conversa segura utilitzant l'RSA. En la següent taula podeu veure els valors que han estat assignats per a les lletres de l'abecedari:

La taula la trobareu en annexos en la pàgina 85.

Una vegada establert l'idioma parlat, sabrem que ***xifrat*** passa a 240906180120 (en el món dels bits).

Per a calcular el nostra missatge codificat hem de fer sevir la fórmula $C = M^e (mod\ N)$, on **M** és el missatge original i **C** el missatge encriptat. Com molts pensareu, el valor de C serà massa gran com per a que una simple calculadora ho pugui calcular. És per això que codificarem el nostre missatge lletra per lletra, encara que és tediós, és l'únic que podem fer.

Codifiquem la lletra $M = x = 24$:

$$C = M^e (mod\ N)$$

$$C = 24^{29}\ (mod\ 39)$$

$$C = 106200365064067167761572429136211990 28224 (mod\ 39)$$

$$C = X = 33$$

Ja tenim la primera lletra codificada, $X = 33$. Ara només farà falta repetir el procés amb les lletres restants i el missatge ja estarà codificat.

És possible que calcular aquest números amb la calculadora no sigui possible, per tant utilitzarem un senzill truc per a poder-los calcular sense la necessitat de calculadores molt potents. Encara que en el nostre exemple el número que es generarà no serà excessivament gran, quan utilitzem la fórmula $C = M^e (mod\ N)$ per a codificar missatges més llargs, ens veurem obligats a fer-ho servir.

Sabem que $29 = 5 + 5 + 5 + 5 + 5 + 2 + 2$

$$29 = 5^5 + 2^2$$

$$C = M^e (mod\ N)$$

$$C = 24^5\ (mod\ 39) \cdot 24^5\ (mod\ 39) \cdot 24^5\ (mod\ 39) \cdot 24^5\ (mod\ 39) \cdot 24^5\ (mod\ 39) \cdot 24^2\ (mod\ 39) \cdot 24^2\ (mod\ 39) = 24^{29} (mod\ 39)$$

$$24^5\ (mod\ 39) = 33$$

$$24^2\ (mod\ 39) = 30$$

$$C = 33 \cdot 33 \cdot 33 \cdot 33 \cdot 33 \cdot 30 \cdot 30 \cdot (mod\ 39) = 35221853700\ (mod\ 39) = 33$$

$$C = X = 33$$

-Codifiquem la segona lletra, **i**, ($i = 09 = 9$).

Sabem que $29 = 5 + 5 + 5 + 5 + 5 + 2 + 2$

$$29 = 5^5 + 2^2$$

$$C = M^e (mod\ N)$$

$$C = 9^5\ (mod\ 39) \cdot 9^5\ (mod\ 39) \cdot 9^5\ (mod\ 39) \cdot 9^5\ (mod\ 39) \cdot 9^5\ (mod\ 39) \cdot 9^2\ (mod\ 39) \cdot 9^2\ (mod\ 39) = 9^{29} (mod\ 39)$$

$$9^5\ (mod\ 39) = 3$$

$$9^2\ (mod\ 39) = 3$$

$$C = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot (mod\ 39) = 2187\ (mod\ 39) = 3$$

$$C = i = 3$$

La segona lletra, **i**, es codifica en 3 ($I = 3$).

-Codifiquem la tercera lletra, **f**, ($f = 06 = 6$).

Sabem que $29 = 5 + 5 + 5 + 5 + 5 + 2 + 2$

$$29 = 5^5 + 2^2$$

$$C = M^e (mod\ N)$$

$$C = 6^5\ (mod\ 39) \cdot 6^5\ (mod\ 39) \cdot 6^5\ (mod\ 39) \cdot 6^5\ (mod\ 39) \cdot 6^5\ (mod\ 39) \cdot 6^2\ (mod\ 39) \cdot 6^2\ (mod\ 39) = 6^{29}\ (mod\ 39)$$

$$6^5\ (mod\ 39) = 15$$

$$6^2 \ (mod\ 39) = 36$$

$$C = 15 \cdot 15 \cdot 15 \cdot 15 \cdot 15 \cdot 36 \cdot 36 \cdot (mod\ 39) = 984150000 \ (mod\ 39) = 15$$

$$C = F = 15$$

La tercera lletra, **f**, es codifica en 15 ($F = 15$).

-Codifiquem la quarta lletra, **r**, ($r = 18$).

Sabem que $29 = 5 + 5 + 5 + 5 + 5 + 2 + 2$

$$29 = 5^5 + 2^2$$

$$C = M^e (mod\ N)$$

$$C = 18^5 \ (mod\ 39) \cdot 18^5 \ (mod\ 39) \cdot 18^5 \ (mod\ 39) \cdot 18^5 \ (mod\ 39) \cdot 18^5 \ (mod\ 39) \cdot 18^2 \ (mod\ 39) \cdot 18^2 \ (mod\ 39) = 18^{29} \ (mod\ 39)$$

$$18^5 \ (mod\ 39) = 18$$

$$18^2 \ (mod\ 39) = 12$$

$$C = 18 \cdot 18 \cdot 18 \cdot 18 \cdot 18 \cdot 12 \cdot 12 \cdot (mod\ 39) = 272097792 \ (mod\ 39) = 18$$

$$C = R = 18$$

La quarta lletra, **r**, es codifica en 18 ($R = 18$).

-Codifiquem la cinquena lletra, **a**, ($a = 01 = 1$).

Sabem que $29 = 5 + 5 + 5 + 5 + 5 + 2 + 2$

$$29 = 5^5 + 2^2$$

$$C = M^e (mod\ N)$$

$$C = 1^{29} \ (mod\ 39) = 1 \ (mod\ 39) = 1$$

La cinquena lletra, **a**, es codifica en 1 ($A = 1$).

-Per última vegada, codifiquem la sisena lletra, **t**, ($t = 20$).

Sabem que $29 = 5 + 5 + 5 + 5 + 5 + 2 + 2$

$$29 = 5^5 + 2^2$$

$$C = M^e (mod\ N)$$

$$C = 20^5 \ (mod\ 39) \cdot 20^5 \ (mod\ 39) \cdot 20^5 \ (mod\ 39) \cdot 20^5 \ (mod\ 39) \cdot 20^5 \ (mod\ 39) \cdot 20^2 \ (mod\ 39) \cdot 20^2 \ (mod\ 39) = 20^{29} \ (mod\ 39)$$

$$20^5 \ (mod\ 39) = 11$$

$$20^2 \ (mod\ 39) = 10$$

$$C = 11 \cdot 11 \cdot 11 \cdot 11 \cdot 11 \cdot 10 \cdot 10 \cdot \ (mod\ 39) = 16105100 \ \ (mod\ 39) = 11$$

$$C = T = 11$$

La sisena lletra, **t**, es codifica en 18 ($T = 11$).

El missatge codificat és **330315180111**.

Una vegada el missatge és codificat, s'envia i ens arriba el missatge codificat **330315180111**. Per a descodificar el missatge, simplement hem d'aplicar la següent fórmula: $M = C^d (mod\ N)$. Seguirem el mateix procediment que en la codificació però en comptes de potenciar el missatge original per la clau d'encriptació (**e**), potenciarem el missatge codificat per la clau de desxiframent (**d**). Recordem que **d** ja l'hem calculat i ens dona que és 5 $(d = 5)$.

-Comencem desxifrant el primer parell de nombres del missatge encriptat, en aquest cas el 33 ($C = 33$).

$$M = C^d (mod\ N)$$

$$M = 33^5 (mod\ 39)$$

$$M = 24$$

Hem obtingut que M és igual a 23 $(M = 23)$, anem a la taula i busquem quina lletra li correspon el número 23, i, sorprenentment, és la **x**. Haurem de repetir aquest procés per a poder trobar les lletres restants i per consegüent, revelarem la paraula original. En aquest cas, no haurem de descompondre la potència, ja que la potència de cinc de qualsevol número de dues xifres, és un resultat relativament petit ($99^5 = 9509900499$). Bé, potser tots els nombres de dues xifres no donen números petits.

-Desxifrem el segon parell de nombres del missatge encriptat, 03 ($C = 03 = 3$).

$$M = C^d (mod\ N)$$

$$M = 3^5 \ (mod\ 39) = 243 \ (mod\ 39)$$

$$M = 9 = 09$$

Sabem doncs que 03 codifica per a 09, que observant en la taula obtenim que 09 correspon a la lletra **i**.

-Desxifrem el tercer parell de nombres del missatge encriptat, 15 ($C = 15$) .

$$M = C^d (mod\ N)$$

$$M = 15^5 \ (mod\ 39) = 759375 \ (mod\ 39)$$

$$M = 6 = 06$$

Sabem doncs que 15 codifica per a 06, que observant la taula obtenim que 06 correspon a la lletra **f**.

-Desxifrem el quart parell de nombres del missatge encriptat, 18 ($C = 18$) .

$$M = C^d (mod\ N)$$

$$M = 18^5 \ (mod\ 39) = 1889568 \ (mod\ 39)$$

$$M = 18$$

Sabem doncs que 18 codifica per a 18 (pura casualitat), llavors observant la taula obtenim que 18 correspon a la lletra **r**.

-Desxifrem el cinquè parell de nombres del missatge encriptat, 01 ($C = 01 = 1$) .

$$M = C^d (mod\ N)$$

$$M = 1^5 \ (mod\ 39) = 1 \ (mod\ 39)$$

$$M = 1 = 01$$

Sabem doncs que 01 codifica per a 01 (sabem que 1 elevat a n, qualsevol número real, sempre és igual a 1: $1^n = 1 / n \epsilon R$), que observant la taula obtenim que 01 correspon a la lletra **a**.

-Desxifrem l'últim parell de nombres del missatge encriptat, 11 ($C = 11$) .

$$M = C^d (mod\ N)$$

$$M = 11^5 \ (mod\ 39) = 161051 \ (mod\ 39)$$

$$M = 20$$

Sabem doncs que 11 codifica per a 20 (pura casualitat), llavors observant la taula obtenim que 18 correspon a la lletra **t**.

Ajuntant totes les lletres obtenim la paraula **xifrat** (la paraula inicial). Hem passat de $xifrat \ \rightarrow \ 240906180120 \rightarrow 330315180111 \rightarrow xifrat$.

Hem de pensar que aquest missatge simplement ha estat codificat amb dos números relativament petits, i ja només amb aquestes xifres minúscules hem pogut comprovar la complicació que té aquest sistema asimètric. Doncs bé, l'RSA és un algoritme molt utilitzat pels bancs, però no us penseu que fan servir números prims d'una o dos xifres, ja que seria relativament senzill trobar els dos números que formen N. Els bancs utilitzen números prims de 300 xifres! Són números tan grans que tots els ordinadors del món junts tardarien milers d'anys en trobar els dos números prims.

3.2 Algoritmes de clau privada simètrics.

Hem de saber que no només existeixen els algoritmes asimètrics per al funcionament d'un sistema criptogràfic segur. És cert que la naturalesa dels asimètrics dificulta moltíssim el seu desxiframent, però això no impedeix que puguin haver altres **algoritmes simètrics**, és a dir, utilitzen el mateix procés per a encriptar i desencriptar, que siguin viables per a garantir la seguretat en les comunicacions o proteccions de dades. Un clar exemple d'aquest tipus és l'**AES** (Advanced Encryption Standard), un algoritme de xifratge per bloc simètric. Aquest algoritme, també conegut com Rijndael, va ser inventat per dos belgues, Vincent Rijmen i Joan Daem (el nom del algoritme com podem observar bé dels seus cognoms, al llarg d'aquest treball ens hem anat adonat que la majoria de les persones nombrades, tot i ser uns genis en els seus respectius camps, no eren gaire originals alhora de posar noms).

Per anar al origen de tot hem de remuntar-nos fins l'any 1997, quan l'Institut Nacional de Normes i Tecnologia, NIST (sigles en anglès per National Institute of

Standards and Technology), va realitzar un concurs obert amb l'objectiu de trobar el millor algoritme per a garantir la seguretat de la informació del govern dels Estats Units. A més, es van establir unes condicions per a poder participar: l'algoritme havia de ser de domini públic, que fos de xifrat simètric i que com a mínim suportés blocs de 128 bits. Al cap de molts processos de selecció, el dia 2 de novembre de 2002 es va anunciar al guanyador, l'algoritme **Rijndael**.

Degut a la complexitat d'aquest sistema d'encriptació, ens limitarem a explicar de manera molt superficial el funcionament de l'algoritme.

Una vegada aclarit tot, comencem amb l'explicació. Primer de tot, què és un algoritme de xifratge per bloc simètric?. Encara que a primera vista pugui semblar màgia negra, el que ens està volent dir és que l'algoritme agafa un bloc o text i el transforma en text xifrat o bloc xifrat, de la mateixa llargada, en aquest cas que com a mínim sigui capaç de xifrar i desxifrar textos de 128 bits d'allargada. A més, que sigui simètric, com ja hem dit anteriorment, significa que utilitza el mateix procés per a codificar i descodificar, però en sentit contrari. Per exemple, jo tinc un fil de llana i decideixo fer una barretina per al cagatió. Una vegada passat el Nadal el cagatió ja no necessita la barretina i vull aprofitar el fil de llana, per tant per a obtenir el fil de llana que jo tenia al principi, hauré de seguir el mateix procés per a fer la barretina però a la inversa, al contrari. Doncs L'AES fa el mateix, agafa el text xifrat (la barretina) i seguint el mateix procés per a xifrar-lo però a la inversa (desfent la barretina tal i com l'havia fet), obtinc de nou el text original (el fil de llana). Per a poder fer i desfer els textos, necessita a més una clau (en el conte de la barretina direm que és el coneixem de fer i desfer la barretina). Aquesta clau és la que li permetrà al algoritme xifrar i desxifrar aquell text en concret. És per això que aquest sistema també es coneix com algoritme de clau privada, ja que tant l'emissor com receptor necessiten saber i utilitzar la clau.

L'AES té tres possibles llargades de claus, 128 bits, 192 bits, 256 bits. El govern dels Estat Units classifica la seva informació en tres categories: Confidential, Secret i Top Secret. Totes les llargades de clau es poden fer servir per a protegir la informació de categoria Confidential i Secret. Informació de tipus Top Secret requereix una longitud de clau de 192 o 256 bits.

Generalment, la majoria de sistemes criptogràfics, codifiquen els missatges en línia, com quan escrivim. En el cas de l'AES, realitza una disposició diferent. En comptes de tenir una llarga línia de bits, els organitza en una taula de quatre per quatre(també conegut com **matriu**). Col·loca el missatge, 128 bits, en quatre files i columnes, 16 bits.

b_{00}	b_{04}	b_{08}	b_{12}
b_{01}	b_{05}	b_{09}	b_{13}
b_{02}	b_{06}	b_{10}	b_{14}
b_{03}	b_{07}	b_{11}	b_{15}

De manera simplificada, en aquest moment l'algoritme substituirà els bits, permutarà les files i barrejarà les columnes. Tot això amb l'objectiu de convertir el missatge original en una massa de bits incomprensible, per a poder garantir la seguretat. Al final d'aquestes substitucions i permutacions, l'algoritme afegirà una clau, Add *Round key*, una clau obtinguda a partir de la clau principal, i, a tot això li direm que és una **ronda** (o volta). L'AES de clau 128 bits realitza 10 rondes abans d'obtenir el missatge xifrat, la clau de 192 bits realitza 12 rondes i la de 256 bits realitza 14 rondes.

Aquest algoritme va ser aprovat per l'Agència de Seguretat Nacional dels Estats Units (NSA) i fins al dia d'avui, Rijndael segueix sent el sistema de codificació estàndard del govern dels Estats Units.

4. Conclusions

A mesura que hem anat avançant en aquest treball, hem pogut veure l'evolució que ha patit la criptografia, i el seu antagonista, el criptoanàlisi, des de l'Antic Egipte fins a l'actualitat, amb els ordinadors i l'internet. Alhora que viatjavem a través del temps per les diferents èpoques de la història, hem après les bases de la criptografia, els principis més bàsics (la transposició i la substitució), els primers algoritmes i algunes tècniques més complexes, des de la xifra Vigenère, els discos de xifres fins a l'Enigma.

A part d'explicar i comprendre la criptografia en el seu àmbit més teòric, també hem vist quines implicacions i conseqüències ha tingut i té en el nostre dia a dia. A més, ens hem adonat que és present sempre, encara que de vegades, no la veiem.

Deixant a banda el debat de la codificació per les masses, és a dir la propietat intel·lectual i/o privada de l'individu, protecció i anonimat, m'agradaria que aquest treball portés a pensar com seria el món sense ella i el seu antagonista, quan d'important arriba a ser en la nostra vida diària i fins a quin punt estem desprotegits dels que aprofiten la criptografia i el criptoanàlisi per al seu benefici propi.

Aquest treball m'ha ensenyat moltes coses, des de l'àmbit personal fins a l'àmbit educatiu. He après a ordenar les idees, a triar què és important, la importància de les explicacions ben estructurades, com fer un treball i l'esforç diari que suposa, tan mental com físicament. Gràcies a ell he descobert com funciona la transmissió d'informació, enviar i rebre missatges bàsicament, i com ha anat evolucionant al llarg de la història. Tot i adonar-me que contra més t'endinses en un camp més t'adones que no saps res i la quantitat de coses que et falten per aprendre, considero que gràcies a aquest treball he après moltes coses sobre la criptografia i el criptoanàlisi.

També sóc conscient de la dificultat intrínseca a l'hora de plasmar la informació no és fàcil, però estic content amb els resultats assolits. Considero que els coneixements assolits a partir d'aquest treball m'ajudaran en un futur a fer treballs d'aquesta mena.

5. Agraïments

Aquest treball no hagués estat possible sense l'ajuda del meu tutor. M'agradaria donar-li les gràcies per l'ajuda rebuda i pels coneixements que m'ha donat, relacionats o no amb el treball. També m'agradaria agrair la feina i ajut que he rebut per part dels meus pares, sense ells probablement aquest treball tindria moltes traves i faltes d'ortografia, per suposat.

5. Bibliografia i webgrafia

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

Rejewski, Marian (1980). "An Application of the Theory of Permutations in Breaking the Enigma Cipher" [agost, 2020]

The Mansion Bletchley ParkSherwood Drive BletchleyMilton Keynes MK3 6EB. https://bletchleypark.org.uk/our-story/the-path-of-a-message/dissemination [agost, 2020]

British Librery. https://www.bl.uk/people/alan-turing [agost, 2020]

B.J.Copeland, july 20th 1998. https://www.britannica.com/biography/Alan-Turing [agost, 2020]

https://ca.wikipedia.org/wiki/Idioma_copte

Diccionario de Arte I (en castellà). Barcelona: Spes Editorial SL (RBA), 2003, p.162 (Biblioteca de Consulta Larousse). https://ca.wikipedia.org/wiki/Dem%C3%B2tic [setembre, 2020]

MCDERMOTT, Bridget, 2006, *Decodificar y descifrar los jeroglíficos egipcios: cómo leer el idioma sagrado de los faraones*. Blume.[setembre, 2020] https://ca.wikiorg/wiki/Jerogl%C3%ADfic

https://ca.wikipedia.org/wiki/Hier%C3%A0tic [setembre, 2020]

Royal Society, retrieved 30 August 2017. "Portrait of Thomas Young" [setembre, 2020]

https://en.wikipedia.org/wiki/Jean-Fran%C3%A7ois_Champollion

https://ca.wikipedia.org/wiki/Accadi

Voight, Laura, may 16th 1950. https://www.brown.edu/Research/Breaking_Ground/bios/Kober_Alice.pdf [setembre, 2020]

University of Cambridge, the life of John Chadwick. https://www.classics.cam.ac.uk/research/projects/mycep/decipherment/chadwick [setembre, 2020]

The editors of encyclopaedia Brittanica, september 2nd 2020, Michael Ventris. https://www.britannica.com/biography/Michael-Ventris [setembre, 2020]

National Inventors Hall of Fame. https://www.invent.org/inductees/ronald-rivest [setembre, 2020]

National Inventors Hall of Fame. https://www.invent.org/inductees/leonard-adleman [setembre, 2020]

National Inventors Hall of Fame. https://www.invent.org/inductees/adi-shamir [setembre, 2020]

Short Tech Stories, june 23rd 2017 https://hackernoon.com/how-does-rsa-work-f44918df914b [octubre, 2020]

http://mathaware.org/mam/06/Kaliski.pdf

Rouse, Margaret, april 2020. https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard [octubre, 2020]

Tutorials point. https://www.tutorialspoint.com/cryptography/block_cipher.htm

FIGURA 1:

https://estaticos-cdn.prensaiberica.es/clip/ee3c5424-5704-49d5-b237-60429d5de726_16-9-aspect-ratio_default_0.jpg

FIGURA 2:

https://www.enlacejudio.com/wp-content/uploads/2019/05/microdots-450_1000.png

FIGURA 3: https://www.revista.unam.mx/wp-content/uploads/img1-69.jpg

FIGURA 4:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 5:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 6:

https://media.britishmuseum.org/media/Repository/Documents/2017_5/25_11/86de7a98_7847_4682_89f8_a77e00c15e4f/preview_ppa451198.jpg

FIGURA 7:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 8:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 9:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 10:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 11:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 12:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 13:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 14:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 15:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 16:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 17:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 18:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 19:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 20:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 21:

https://upload.wikimedia.org/wikipedia/commons/thumb/6/6d/%D0%A2%D1%8C%D1%8E%D1%80%D0%B8%D0%BD%D0%B3.jpg/1280px-%D0%A2%D1%8C%D1%8E%D1%80%D0%B8%D0%BD%D0%B3.jpg

FIGURA 22:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 23:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 24:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

FIGURA 25:

Singh, Simon. The code book: the secret history of codes and code-breaking. Debate. 2000. ISBN: 848306278X

6. Annexos

Taula RSA:

Lletres reals	Valor assignat
A	01
B	02
C	03
D	04
E	05
F	06
G	07
H	08
I	09
J	10
K	11
L	12
M	13
N	14
O	15
P	16
Q	17
R	18
S	19
T	20
U	21
V	22
W	23
X	24
Y	25
Z	26
Espai	00

6.1 El Desxiframent de les llengües perdudes i escriptures antigues

S'ha de dir que aquest apartat del treball de recerca és possible que no segueixi el tema principal del tema, malgrat això, m'agradaria aturar-me per a explicar els desxiframents dels jeroglífics egipcis i el misteri del lineal B.

El desxiframent de les escriptures antigues no forma part de la batalla evolutiva entre la criptografia i el criptoanàlisi, perquè encara que hi ha arqueòlegs desxifradors, no hi ha que siguin codificadors. En la majoria dels casos que s'enfronta un desxifrador arqueològic són textos on els escribes no tenien la intenció d'ocultar deliberadament el significat del text, sinó que hem sigut nosaltres que amb el pas del temps hem perdut la capacitat d'interpretar-los. Tot i no tenir res a veure amb el tema principal, els principis que es segueixen per a resoldre aquestes "xifres" són els mateixos mètodes que faríem servir per a desxifrar una xifra convencional. De fet, molts desxifradors militars s'han sentit atrets per el desafiu de desentranyar una escriptura antiga. És possible que aquesta motivació per a desxifrar escriptures antigues vingui de la curiositat i la fama que això suposa en comptes de la necessitat de supervivència i/o l'anonimat de desxifrar xifres militars.

6.1.1 Els jeroglífics egipcis

Probablement, el desxiframent dels jeroglífics egipcis és un dels més famosos. Per una banda, el desxiframent dels jeroglífics ha aconseguit crear un pont entre els milers d'anys que ens separen de la civilització egípcia. Per l'altre, va permetre l'estudi de l'evolució d'una llengua i una escriptura d'un període de més de tres mil anys.

Els jeroglífics més antics es remunten fins a l'any 3000 a.C. Aquesta forma d'escriure va perdurar durant gairebé tres mil cinc cents anys. Encara que aquests símbols elaborats resulten ideals per als murs i les parets dels temples, suposen un problema. Aquesta escriptura és massa complicada i suposa massa esforç per a fer-la servir diàriament. Per exemple, per a un mercader que ha d'apuntar les seves transaccions necessita una escriptura fàcil, ràpida i pràctica, i cap d'aquestes característiques es trobaven en els jeroglífics. És per això que paral·lelament als jeroglífics evolucionava la **hieràtica**, una simplificació dels símbols jeroglífics, més ràpida i senzilla d'escriure. Durant el segle VI a.C, la hieràtica va ser reemplaçada

per una escriptura encara més simple, el **demòtic**. Els jeroglífics, la hieràtica i el demòtic eren essencialment la mateixa escriptura.

Les tres formes de escriptures eren fonètiques, és a dir, tots els caràcters representen sorolls diferents, igual que les lletres del nostre alfabet. Aquestes escriptures es van fer servir per a tots els àmbits de la vida egípcia, durant més de tres mil anys fins que en el segle IV de la nostra era, en menys d'una generació, les escriptures van desaparèixer. L'església cristiana és la responsable de l'extinció de les escriptures egípcies, van ser prohibides perquè l'església volia esborrar qualsevol connexió amb el passat pagà d'Egipte. Les escriptures antigues van ser substituïdes pel **copte**, escriptura basada en el grec però que inclou sis lletres pròpies de l'escriptura demòtica per a representar diversos sorolls egipcis que no s'expressaven en grec. Va ser tal el domini del copte que en poc menys d'un segle, va desaparèixer l'habilitat per a llegir jeroglífics, la hieràtica i el demòtic. Encara que al principi la llengua egípcia es seguia parlant, al cap del temps va evolucionar fins a convertir-se en la llengua copte. Però al segle XI, l'escriptura i l'idioma copte van ser apartats i silenciats per l'expansió dels àrabs, trencant l'última connexió amb les antics regnes d'Egipte i perdent el coneixement, i per tant la capacitat de llegir als antics faraons.

L'interès pels jeroglífics no va sorgir fins el segle XVII, quan el papa Sixte V va reorganitzar la ciutat i en cada intersecció va col·locar obeliscs comprats a Egipte. Com que en els obeliscs hi havia jeroglífics, els estudiosos van intentar desxifrar-los, però el punt de partida on començaven ja era erroni. Estaven basant els seus estudis en una suposició falsa; pensaven que els jeroglífics representaven emagrames, símbols que representen idees (nosaltres per exemple escrivim fent ús de fonogrames, caràcters que representen fonemes, soroll parlat). Els estudiosos estaven convençuts de que eren semagrames en part per dues raons. La primera, perquè un historiador grec descrivia els jeroglífics com si fossin idees, i la segona, perquè en 1652, el jesuïta alemany Athanasius Kircher va publicar un diccionari d'interpretacions al·legòriques, utilitzant el seu diccionari per a produir una sèrie de traduccions fantasioses que ara sabem que no tenien cap mena de sentit. Encara que en l'actualitat ens semblin traduccions absurdes, l'impacte que va generar en altres aspirants desxifradors va ser immens. No només era un egiptòleg, sinó que també era considerat el pare de la vulcanologia i l'inventor de la llanterna màgica

(precursor del cinema). Era altament conegut i respectat. És per això que les seves idees, per molt que fossin o semblessin estúpides, van ser respectades i van influir profundament en els futurs egiptòlegs.

No va ser fins un segle i mig després de Kircher, l'estiu de 1798, que l'antic Egipte tornà a ser sotmesa a un minuciós anàlisi. Napoleó Bonaparte va enviar un equip d'historiadors, científics i dibuixants per a que investiguessin tot el que veien per la recent conquerida Egipte. Aquests acadèmics van trobar amb la pedra més famosa de la història de l'arqueologia, *la Pedra Rosseta*. Es trobava incrustada en un mur i tenia un conjunt d'inscripcions: era el mateix text repetit tres vegades, amb grec, demòtic i amb jeroglífics. Acabaven de trobar un puntal criptoanalític similar als puntals de Bletchley Park. La Pedra Rosseta era potencialment un dels mitjans per a desxifrar i descobrir els antics símbols egipcis.

Encara que la pedra va ser trobada pels francesos, aquesta va caure en mans dels britànics. L'any 1802, la pedra es va instal·lar en el Museu Britànic.

La traducció del grec va ser molt fàcil i en poc temps es va saber que en la Pedra Rosseta hi havia un decret del consell general de sacerdots egipcis emès l'any 196 a.C. Llavors, si les altres dues inscripcions tenien el mateix decret, el desxiframent del text en jeroglífic i en demòtic hauria de ser bufar i fer ampolles, relativament parlant. No obstant, hi havia encara tres obstacles principals. Primer, la Pedra Rosseta es trobava en condicions molt dolentes, estava molt danyada. Segon, les dos escriptures restants expressaven l'antiga llengua egípcia, la qual ningú havia parlat durant vuit segle. Encara que fos possible trobar les relacions d'algunes paraules gregues amb símbols egipcis, seguiria sent impossible establir el soroll de les paraules egípcies. Un dels primers estudiosos que va qüestionar el prejudici dels jeroglífics, que eren una escriptura pictòrica, va ser Thomas Young.

Young va néixer l'any 1773 a Milverton, Somerset. Des de ben petit ja es sabia que era un geni. Amb només catorze anys ja parlava grec i llatí, a més, havia estudiat el grec, llatí, francès, italià, hebreu, àrab i unes quantes llengües més. Tot i que li apassionaven les llengües, va estudiar medicina en Cambridge.

Young es centrà més en la part de la investigació, creant experiments per a explicar el funcionament de l'ull humà. Va establir que la percepció dels colors no és més que el resultat de distints receptors. També li interessava molt la física. Va publicar *La*

teoria ondulatòria de la llum, un article sobre la naturalesa de la llum, teoria que contradeia a la teoria proposada per Isaac Newton, deia que la llum no era una ona sinó una partícula. Va aportar molts més avenços a molts més camps però tampoc em vull esplaiar massa.

En el moment que Young va escoltar parlar de la Pedra Rosseta, es va convertir en la seva obsessió. A l'estiu de 1814 va començar a estudiar la pedra. Young es va centrar en un conjunt de jeroglífics emmarcats amb una línia, denominats **cartutxos**. Es pensava que aquests jeroglífics emmarcats havien de representar alguna cosa molt important. Pensava que possiblement era el nom del faraó Ptolemeu, perquè apareixia en el text grec, Πτολεμαῖος. Si estava en lo cert, li permetiria descobrir lafonètica dels jeroglífics, perquè el nom d'un faraó es pronuncia més o menys igual en qualsevol idioma. El **cartutx** de Ptolemeu es repeteix sis vegades al llarg del text, a vegades en la versió denominada normal i a vegades en una versió més llarga i elaborada. Va suposar que la versió més llarga seria el nom del faraó amb els seus títols i per tant es va fixar en la versió normal, endevinant el valor sonor de cada jeroglífic.

Tabla 13. El desciframiento de Young de  , el cartucho de Tolomeo (versión normal) de la Piedra Rosetta.

Jeroglífico	Valor sonoro de Young	Valor sonoro verdadero
	p	p
	t	t
	opcional	o
	lo o ole	l
	ma o m	m
	i	i o y
	osh o os	s

Encara que en aquell moment no ho sabia, Young va aconseguir establir la correlació entre la majoria dels jeroglífics i el seu valor sonor correcte. Si ens fixem en el conjunt de jeroglífics, podem observar que els dos primers jeroglífics, una pedra i un quadrat, apareixen un a sobre de l'altre, en l'ordre fonètic correcte. L'escriba havia col·locat els jeroglífics d'aquesta manera per pura estètica, i, casualment estaven en l'ordre fonètic correcte. Moltes vegades, els escribes escrivien d'aquesta manera per a evitar espais en blanc i mantenint així l'harmonia visual; inclús intercanviaven la posició de les lletres contradient qualsevol regla ortogràfica, simplement per augmentar la bellesa d'una inscripció. Després d'haver

desxifrat el nom del faraó Ptolemeu, va trobar un altre cartutx en una inscripció copiada del temple de Karnak, a Tebes. Va pensar que potser era el nom d'una reina ptolemaica: Berenice.

Va repetir el procés anterior, seguint la mateixa estratègia.

Tabla 14. El desciframiento de Young de  , el cartucho Berenika del templo de Karnak.

Jeroglífico	Valor sonoro de Young	Valor sonoro verdadero
	bir	b
	e	r
	n	n
	i	i
	opcional	k
	ke o ken	a
	terminación femenina	terminación femenina

Dels tretze jeroglífics combinant els dos cartutxos, Young havia desxifrat la meitat perfectament i un quart estaven parcialment bé. A més, també havia trobat el símbol de la terminació femenina. Encara que no podia saber quan d'èxit havia tingut, la aparició de **M** en els dos cartutxos, representant a la **i** en les dos ocasions, indicava que anava per bon camí, donant-li la suficient confiança per a continuar. No obstant, la seva investigació es va veure interrompuda de cop. Sembla ser que tenia massa respecte a l'argument de Kricher i no estava disposat a tirar per terra el paradigma de Kircher. Va justificar els seus avenços dient que només els noms de la dinastia ptolemaica descendents de Lagus, un general d'Alejandro Magno, havien de ser lletrejats perquè no hi havia un semagrama natural en els jeroglífics.

Finalment, va acabar perdent l'interès pels jeroglífics però abans de concloure, va resumir el seu treball en un article per a la Enciclopèdia Britànica.

Coetàniament a Young, hi havia un jove que estava disposat a posar fi en la cursa del desxiframent dels jeroglífics, Jean-François Champollion. Tot i no arribar als trenta anys d'edat, ja portava gairebé dos dècades estudiant els jeroglífics.

L'obsessió de Champollion va començar amb només deu anys, quan el matemàtic francès Jean-Baptiste Fourier, que havia sigut un dels estudiosos que havien anat a Egipte, va ensenyar a Champollion la seva col·lecció d'antiguitats egípcies, moltes

de les quals estaven adornades amb unes inscripcions que ningú podia entendre. Fourier li va explicar que ningú podia entendre aquesta escriptura i llavors Champollion li va prometre que algun dia resoldria el misteri. Amb només disset anys va presentar el seu primer article titulat “Egipte sota els Faraons”. Era tan innovador l’article que va ser escollit per a l’Acadèmia de Grenoble. En assabentar-se que s’havia convertit en un professor adolescent, es va emocionar tant que va perdre el coneixement.

Champollion dominava el llatí, el grec, el copte, l’hebreu, l’àrab, el xinès, el persa i varies llengües més. Tot aquest coneixement només per a poder assaltar als jeroglífics. La seva obsessió amb els jeroglífics va arribar fins al punt que quan un amic seu va mencionar que Alexander Lenoir, un conegut egiptòleg, havia publicat un desxiframent complert dels jeroglífics, Champollion es va sentir tan malament que va tornar a perdre el coneixement (sembla ser que no només era un bon egiptòleg, sinó que també era un crack amb els desmais). Per sort, els avenços de Lenoir eren tan fantasiosos com les temptatives de Kircher.

L’any 1822, Champollion va aplicar l’estratègia de Young a altres cartutxo. El naturalista britànic W.J. Bankes havia portat un obelisc amb inscripcions gregues i jeroglífiques, i havia publicat una litografia d’aquests texts bilingües, que incloïen cartutxos de Ptolemeu i Cleopatra. Champollion va aconseguir assignar valors sonors a jeroglífics individuals. Les lletres **p, t, o** i **e** apareixien en els dos noms; en quatre dels casos les lletres estaven representades pels mateixos jeroglífics, menys en un cas, la **t**. Encara que hi havia una discrepància, Champollion va suposar que el soroll **t** podia ser representat per dos jeroglífics, de la mateixa manera que en català el fonema **/k/** pot ser representat per les grafies c, q, qu, g i k, com per exemple, vaca i enquesta. Va seguir desxifrant cartutxos que no tenien traducció bilingüe, substituint sempre que podia els valors sonors que ja havia obtingut dels cartutxos de Ptholemeu i Cleopatra. També va resoldre un cartutx que contenia un dels noms més importants dels temps antics, Alexandre. Champollion suposava que era Alexandre perquè semblava llegir-se com **a-l-?-s-e-?-t-r-?**, **alksentrs** que és Alexandre però en egipci. També es va adonar que els escribes no els hi agradava utilitzar les vocals i a vegades les ometien: els escribes deurien pensar que a la gent no li resultaria problemàtic omplir els vuits que faltaven amb vocals. Tots els progressos que havia fet fins ara no eren més que una extensió del treball de Young.

Tots els noms que havia desxifrat encara eren estrangers, cosa que recolzava la teoria de que només es recorria a la fonètica per a les paraules que estaven fora del lèxic egipci tradicional.

El 14 de setembre de 1822, Champollion va rebre uns documents procedents del temple d'Abú Simbel, els quals contenien cartutxos que precedien al període de dominació grecoromana. Aquests cartutxos eren molt importants perquè eren suficientment antics com per a contenir noms egipcis tradicionals i, si aquests apareixien lletrejats serien una prova essencial per a desmuntar la teoria que diu que només els noms estrangers és lletregen. En concret, es va centrar en un cartutx en especial, un que només contenia quatre jeroglífics:  .

Els dos primers eren símbols desconeguts, però els dos últims al final, se sabia que representaven dos vegades la **s**, perquè apareixia en el cartutx d'Alksentrs (Alexandre). En aquest moment va ser quan Champollion va fer servir el seu ampli ventall de llengües que havia estudiat i coneixia molt bé. Va recórrer al copte, descendent directe de la llengua egípcia antiga, el qual havia deixat de ser llengua viva en el segle XI, encara que existia una forma fossilitzada en la litúrgia de l'Església cristiana copte. Champollion havia aprés el copte quan era un adolescent, i el dominava tant que l'utilitzava per a escriure en el seu diari. No obstant, fins al moment, no es pensava que el copte podria ser també la llengua dels jeroglífics.

Champollion es va preguntar si el primer símbol del cartutx podia ser una ideografia que representés el sol (un dibuix del sol seria el símbol de la paraula "sol"). Llavors, va suposar que aquesta ideografia podria tenir el valor sonor de la paraula copte per a sol, **ra**. Això li donà la seqüència **ra-?-s-s**. Només havia un nom faraònic possible. Tenint en compte l'omissió de les vocals i suposant que la lletra que faltava era **m**, sens dubte hauria de ser **Ramsés**, un dels faraons més importants i antics de la història egípcia. Es va adonar que inclús els noms faraònics antics s'escrivien fonèticament. Champollion havia demostrat que els escribes a vegades treien partit al principi d'un tipus d'endevinalla. En aquestes endevinalles les paraules llargues es descomponen en els seus components fonètics, que després són representats per mitjà d'ideografies.

Encara que aquest cartutx era com els altres, el seu desxiframent va demostrar clarament quatre principis fonamentals dels jeroglífics. Primer, la llengua de la escriptura està com a mínim relacionada amb el copte, perquè si per exemple els escribes haguessin parlat el grec el cartutx es pronunciaria com **helios-mses**. El cartutx només té sentit quan els escribes parlant un tipus de copte, llavors es pronuncia com a **ra-mses**. Un examen d'altres jeroglífics va demostrar que efectivament es tractava de copte. Segon, les ideografies s'utilitzaven per a representar algunes paraules. Tercer, la major part del que escrivien ho escrivien utilitzant un alfabet fonètic relativament convencional. Quart, la fonètica és l'ànima dels jeroglífics.

Champollion va publicar tots els seus descobriments en el llibre *Précis du systéme hiéroglyphique*. Per primera vegada en catorze segles era possible llegir la història dels faraons.

6.1.2 El misteri del lineal B

La història del lineal B comença amb les excavacions de Sir Arhtur Evans, un dels arqueòlegs més importants del principi del segle XX. Evans era un arqueòleg que estava interessat en el període de la història de Grècia descrit per Homer en els seus poemes èpics, la *Ilíada* i la *Odissea*.

Hi havia dubtes sobre la certesa de les històries d'Homer, però l'any 1872 l'arqueòleg alemany Heinrich Schliemann, va trobar la ciutat de Troia, fins ara considerada una fantasia, prop de la costa occidental de Turquia, convertint els mites de Homer en realitat. Entre el 1872 i 1900, els arqueòlegs s'havien encarregat de descobrir i trobar més proves referents a la rica època prehel·lènica, antecessors de l'era clàssica de Pitàgores, Plató i Aristòtil en uns sis-cents anys. El període prehel·lènic va des del 2800 fins al 1100 a.C, sent els últims quatre segles els de més esplendor. Els arqueòlegs s'havien centrat entorn Micenes, on havien excavat una gran varietat d'artefactes i tresors, però no havien trobat cap forma d'escriptura, cosa que desconcertava a Evans. Sir Arthur no podia acceptar que en una societat tan sofisticada podria ser analfabeta i va decidir dedicar el seu temps a demostrar que la civilització micènica tenia alguna forma d'escriptura.

La recerca va començar amb els comerciants d'antiguitats d'Atenes, on només va trobar algunes pedres gravades, semblaven ser segells que es remuntaven a l'era prehel·lènica. No va treure gairebé res de bo, però li va donar la motivació necessària per a continuar amb la recerca. Sabia que en Creta, concretament en Cnossos, era el punt més important d'un Imperi que dominava l'Egeu, l'imperi Minoic. Va començar a excavar a principis del març de 1900 i els resultats van ser gairebé imminents. A finals de març va començar a desenterrar allò que estava buscant, encara que al principi no ho sabia. Va descobrir una tauleta d'argila amb una inscripció i pocs dies després va trobar moltes més tauletes.

Les tauletes es podien dividir en tres categories: la primera sèrie de tauletes, dataven entre el 2000 i el 1650 a.C, eren dibuixos, probablement ideografies, relacionats amb els segells comprats als comerciants. La segona sèrie datava entre 1750 i 1450 a.C, havien caràcters inscrits que consistien en simples línies, i aquesta escriptura va rebre el nom de **Lineal A**. La tercera sèrie de tauletes, dataven des de 1450 fins a 1375 a.C, tenien una escriptura semblant a la del Lineal A però perfeccionada, pel que va ser anomenada **Lineal B**. Com que la majoria de tauletes trobades eren Lineal B, i com que semblava que era l'escriptura relativament més recent, Evans i els seus companys van decidir que el Lineal B oferiria la millor possibilitat de desxiframent.

La majoria de les tauletes semblava que contenien inventaris. Amb tantes columnes de caràcters numèrics era relativament fàcil deduir el sistema numeral, però el sistema de caràcters fonètics era una situació completament diferent. A primera vista només es va poder establir dos fets útils del Lineal B: Primer, la direcció de la escriptura és d'esquerra a dreta, ja que qualsevol espai al final d'una línia quedava generalment a la dreta. Segon, hi havia 90 caràcters diferents, implicant que l'escriptura era gairebé sens dubte sil·làbica.

Hem de fer un incís per a explicar perquè sabien que l'escriptura era sil·làbica. Doncs bé, pels lectors que us ho estigueu preguntant, aquí va l'explicació: Les escriptures purament alfabètiques tendeixen a tenir entre 20 i 41 caràcters (per exemple, el rus té 36 símbols o signes i el àrab 28). En canvi, en l'altre extrem de la balança, les escriptures basades en ideografies tendeixen a tenir entres centenars i milers de símbols o signes (segons el document "Hanyu Da Zidian" el número de

caràcters que conté el mandarí és 54.678). Les escriptures sil·làbiques ocupen el punt mig, entre 50 i 100 caràcters sil·làbics.

El problema fonamental era que ningú podia estar segur en quin idioma estava escrit el Lineal B. Inicialment, es pensava que podria ser una forma escrita del grec, perquè set caràcters tenien molta similitud amb l'escriptura xipriota clàssica, que es sabia que era una forma d'escriptura grega utilitzada entre el 600 i 200 a.C. Van començar a sorgir dubtes sobre la credibilitat d'aquesta hipòtesi perquè si la consonant més freqüent en el grec és la **s**, i el caràcter final més freqüent en la escriptura xipriota és la síl·laba **se**; com que estem parlant d'una escriptura sil·làbica, una consonat ha d'estar representada per una combinació de consonant-vocal, en la qual la vocal roman muda. Aquest caràcter, **se**, apareix en l'escriptura del Lineal B, però gairebé mai a final de paraula, indican que el Lineal B no podia ser el grec. Els consens general era que el Lineal B havia de ser una escriptura més antiga i que representava una llengua encara desconeguda i extinta.

Sir Arthur era un gran partidari de la teoria que el Lineal B no era un forma escrita del grec i creia que representava la llengua nativa de Creta. Estava convençut que hi havia una forta evidència arqueològica que ho demostraria. Per exemple, els seus descobriments suggerien que l'imperi Minoic era molt més avançat que la civilització micènica de la península. Evans creia que com l'imperi Minoic era molt ric i pròsper, per consegüent, haurien de tenir una llengua pròpia, en compte d'adoptar l'idioma de la civilització rival.

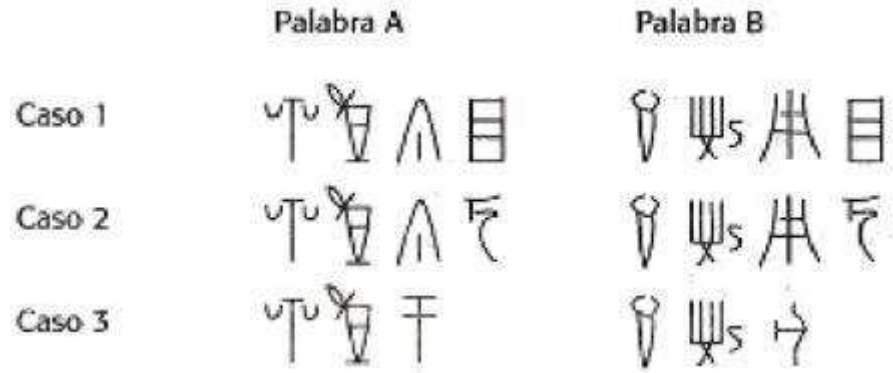
Encara que la seva teoria era àmpliament acceptada, hi havia una minoria que no estava d'acord. Sir Arthur va fer ús de tota la seva influència per a castigar a tot el que no estava d'acord amb els seus ideals referents amb el Lineal B. Estava començant una època de "terror" dirigida per Evans. Inclús va obligar a un professor de la universitat de Cambridge a retirar-se de l'Escola Britànica d'Atenes quan es va pronunciar a favor de la teoria de que el Lineal B és una forma escrita del grec. La controvèrsia del "grec contra no-grec" acabava de començar i duraria fins l'últim dia.

Durant les següents quatre dècades, tots els intents d'atacar al Lineal B va fracassar. L'any 1941, Sir Arthur va morir a l'edat de 90 anys. No va viure el suficient per a veure el desxiframent del Lineal B.

Després de la seva mort, l'arxiu de tauletes del Lineal B i les seves pròpies notes arqueològiques van quedar disponibles per a un cercle molt restringit d'arqueòlegs, tot aquell que estigués a favor de la seva teoria. No obstant, a mitjans de la dècada dels quaranta, Alice Kober va aconseguir el material i va començar un anàlisi meticulós i imparcial de l'escriptura. Kober semblava una professora corrent, no obstant la seva passió per a la investigació era immesurable. Va centrar-se en el Lineal B i estava disposada a desxifrar-lo. Sabia però que per a poder atacar el Lineal B hauria de seguir una estratègia completament nova. Es va centrar exclusivament en l'estructura de l'escriptura en conjunt i en la construcció de paraules individuals.

Poc després de començar a investigar s'adonà que hi havia unes paraules en concret que formaven trios, és a dir que apareixia la mateixa paraula en tres formes lleugerament diferents. Aquests trios mantenien l'arrel, que eren idèntiques però tenien tres terminacions diferents. Degut a aquesta evidència va deduir que aquesta llengua havia de ser altament declinable, és a dir, les terminacions de les paraules canvien per a determinar el gènere, el temps, etc. Per exemple, l'anglès és lleugerament declinable perquè s'afegeix una **s** en la tercera persona del singular. Normalment, les llengües antigues tendeixen a ser molt més rígides, però aquest no és el cas del Lineal B.

Kober va publicar un article en el que descrivia aquesta naturalesa declinable en dos grups en concret. Cada grup conserva la seva arrel però tenen diferents terminacions.



Per a simplificar la tasca del desxiframent, a cada símbol del Lineal B se li va assignar un número de dos xifres.

Tornem als trios però aquesta vegada escrits amb números.

	Palabra A	Palabra B
Caso 1	25-67-37-57	70-52-41-57
Caso 2	25-67-37-36	70-52-41-36
Caso 3	25-67-05	70-52-12

A primera vista podem deduir que els dos primers signes en els dos casos són l'arrel, ja que es repeteix i es manté constant independentment del cas. No obstant, el tercer signe no és el que ens podríem esperar. Comencem a fer suposicions: si el tercer signe formés part de l'arrel, aquest signe s'hauria de mantenir constant independentment del cas. Però això no és així, en la Paraula A, el cas 1 i 2, el tercer signe és el 37, però en el cas 3 el tercer signe és el 05. En la paraula B el tercer signe per als casos 1 i 2 és el 41 i en el cas 3 el signe és el 12. Llavors, si el tercer

signe no forma part de l'arrel, podem esperar que formi part de la terminació, però aquesta possibilitat ens segueix donant problemes. Per a un cas en concret, la terminació hauria de ser la mateixa independentment de la paraula, però per als casos 1 i 2 el tercer signe és 37 en la paraula A, però 41 en la paraula B, i per al cas 3 el tercer signe és 05 en la paraula A i 12 en la paraula B.

Els tercers signes desafiaven les expectatives perquè no semblaven que formaven ni de l'arrel ni de la terminació. Kober va posar fi a aquest problema quan va proposar la teoria de que cada signe representa un síl·laba, probablement una combinació d'una consonant seguida d'una vocal. Va proposar llavors que la tercera síl·laba podria ser la síl·laba d'unió, representant part de l'arrel i part de la terminació. La consonant formaria part de l'arrel i la vocal de la terminació.

Per a contrastar la seva teoria i credibilitat va donar un exemple de la llengua accadi. Aquesta llengua també té síl·labes d'unió i és altament declinable. *Sadanu* és un nombre accadi de cas 1, que canvia a *sadani* en el segon cas i a *sadu* en el tercer cas. És evident que les tres paraules consten d'una arrel , **sad-**, i una terminació, **-anu** en el cas 1, **-ani** en el cas 2 i **-u** en el cas 3., la síl·laba d'unió és la mateixa en els dos primers casos però diferent en el tercer cas. Aquest és exactament el mateix patró que es pot observar en el Lineal B: el tercer signe en cada una de les paraules del Lineal B estudiades per Kober havien de ser sí o sí síl·labes d'unió.

Només amb la identificació de la naturalesa declinable i l'existència de la síl·laba unió en el Lineal B significava que Kober havia progressat més que ningú en el desxiframent d'aquesta llengua. No obstant, en aquest punt també és podia fer una deducció encara major. En l'exemple accadi, la síl·laba d'unió canvia de **-da** a **-du**, però la consonant és manté constant. De manera similar, les síl·labes 37 i 05 del Lineal B en la paraula A han de compartir la mateixa consonant, així com les síl·labes 41 i 12 en la paraula B. Per primera vegada començaven a sorgir pistes de la fonètica dels caràcters. També va poder establir altres relacions entre els caràcters. Les paraules A i B haurien de tenir la mateixa terminació en el primer cas. No obstant, la síl·laba d'unió canvia de 37 a 41.

Això vol dir que les síl·labes 37 i 41 representen síl·labes amb consonants diferents però amb la mateixa vocal, explicant també perquè els signes són diferents, si bé mantenen la mateixa terminació per a les dues paraules. De la mateixa manera, per

al cas 3 les síl·labes 05 i 12 han de tenir una vocal en comú però consonants diferents.

Encara que no va poder identificar quina vocal era en cap dels casos, Kober havia establert unes relacions rigoroses entre uns caràcters en concret. Va resumí aquest resultats en una taula de relacions. Kober no tenia ni idea de quina síl·laba era representada per el signe 37, però si sabia que compartia consonant amb el signe 05. Va seguint aplicant aquest mètode fins a construir una taula amb deu signes, dos vocals i cinc consonants. Per desgràcia, Kober no va viure lo suficient per a treure-li partit al seu magnífic treball i a l'edat de 43 anys, l'any 1950, va morir de càncer de pulmó.

Just abans de morir, Kober va rebre una carta de Michael Ventirs, un arquitecte anglès obsessionat amb el lineal B des de petit. Ventris va néixer el 12 de juliol de 1922 a Weathampstead, Hertfordshire. La seva infància la va passar a Suïssa, on va aprendre alemany i francès. A més, la seva, mare li parlava amb polonès i als vuits anys ja el parlava fluidament. Tenia una habilitat innata per aprendre noves llengües, podia aprendre a parlar qualsevol llengua en menys de dos setmanes. Tal era la seva habilitat, que podia parlar en dotze idiomes diferents perfectament.

Des de ben petit es va apassionar per les escriptures antigues. L'any 1936, a través d'una conferència va descobrir el lineal B, del qual es va enamorar. Casualment aquella conferència va ser donada per Sir Arthur Evans. A partir d'aquesta conferència es va obsessionar profundament en el misteri del lineal B, el qual l'acompanyaria fins la mort.

Tot i que Ventris va estudiar i treballar com arquitecte, la seva passió pel lineal B no va parar, i, va dedicar tot el seu temps lliure a estudiar l'escriptura minoica. Quan Kober va publicar el seu treball a Ventris li va agradar i interessar moltíssim, fins al punt que li va escriure per a demanar-li més detalls. Per desgràcia Alice va morir abans de que ella li pogués respondre, però per sort, les seves idees i treballs seguien intactes. Ventirs va estudiar meticulosament les idees de Kober. Va trobar la taula de Kober i la va ampliar trobant noves paraules que compartissin l'arrel i la síl·laba d'unió. Al cap d'un any aproximadament, s'adonà que hi havia una excepció en la relga que diu que tots els signes són síl·labes.

Fins ara, es pensava que els signes del lineal B representaven una combinació d'una consonant amb una vocal (CV), cosa que suposaria un problema per a les paraules que no fossin divisibles seguint la norma CV, ja que són imparelles. Ventris suposà que els minoics ho van solucionar afegint una **i** muda per a crear un nombre parell de síl·labes, de manera que la paraula es pogués escriure en una combinació de síl·labes CV. Per exemple, si agafem la paraula **visible** i la separem en parells de lletres obtenim vi-si-bl-e . Com podem observar, les síl·labes no segueixen la norma CV, hi ha una síl·laba que consta de dos consonants i una **e** al final sola. Si volguéssim seguir la fórmula del lineal B (CV), separaríem la paraula afegint una **i** muda de la següent forma: vi-si-bi-le. Ara sí és segueix la norma CV i la lletra **i** de la segona síl·laba és muda, per tant la paraula es pronunciaria de la mateixa manera. Malgrat això, la paraula **invisible** segueix sent problemàtica. Aquesta vegada és necessari inserta vocals mudes després de la **n** i de la **b** i també és necessari fer alguna cosa amb la vocal **i** que està al principi del la paraula: i-ni-vi-si-bi-le. La **i** al principi de paraula no pot ser fàcilment convertida en una síl·laba CV. Encara que aquesta suposició podria ser vàlida, Ventris va descartar aquesta teoria perquè inserir una consonant muda al principi d'una paraula per aconseguir una síl·laba CV donaria peu a moltes confusions (imagineu-vos què complicat seria saber si al principi de la paraula la primera lletra és muda o no, en resum, masses problemes).

Una vegada Ventris descarta la possibilitat d'una vocal muda, arriba a la conclusió que ha d'haver signes del lineal B que representin vocals soles, per a que puguin ser utilitzades a principi de paraula. Aquests signes haurien de ser fàcils de trobar ja que només apareixen al principi de les paraules. Va calcular la freqüència de cada signe al principi, en el mig o al final de les paraules. Va observar que hi havia dos signes en particular, 08 i 61, apareixien predominantment al principi de les paraules i va concloure que no representen síl·labes, sinó paraules.

Es va passar els dos anys següents completant la taula de Kober fins a arribar a la taula següent:

		Vocales				
		1	2	3	4	5
Consonantes	I					57
	II	40		75		54
	III	39				03
	IV		36			
	V		14			01
	VI	37	05		69	
	VII	41	12			31
	VIII	30	52	24	55	06
	IX	73	15			80
	X		70	44		
	XI	53				76
	XII		02	27		
	XIII					
	XIV			13		
	XV		32	78		
	Vocales puras		61			08

La taula consta de cinc columnes vocals i quinze línies de consonants, amb cinc quadrícules addicionals de les vocals soles. Amb la taula podies relacionar tots els signes, podies saber si dos signes compartien o no vocals o consonants sense saber quines eren les lletres que en realitat compartien. Per exemple, observant la línia XI podem saber que els signes 53 i 76 comparteixen la mateixa consonant, però que contenen vocals diferents, 1 i 5. Fins ara no s'havia atrevit a assignar valors sonors a ningun dels signes. No obstant, això estava apunt de canviar.

Analitzant les paraules i les freqüències dels signes, Ventris s'havia adonat que havien tres paraules que apareixien amb moltíssima freqüència: **08-73-30-12, 70-52-12**, **69-53-12**. Va suposar que aquestes paraules probablement serien noms de ciutats, i, seguint aquesta suposició va començar a fer les següents deduccions: Ventris havia especulat que el signe 08 és una vocal, per tant, el nom de la ciutat hauria de començar amb una vocal. L'únic nom de ciutat significativa que semblava encaixar era **Amnisos**, una important ciutat portuària. Si aquesta suposició era correcte, llavors el signe 73 representaria **-mi-** i el signe 30 representaria **-ni-**. Com que aquests dos signes comparteixen vocals haurien d'aparèixer en la columna de la mateixa vocal. Si apareixien, el signe final 12, representaria **-so-**.

Ciutat 1= 08-73-30-12 = a-mi-ni-so = Amnisos

Només era una suposició, però les repercussions en la taula eren enormes. Per exemple, el signe 30, que semblava representar la síl·laba **-ni-**, està en la primera columna de vocals i en la vuitena de consonants. Per consegüent, tota la resta de signes en la columna 1 de vocals contindrien la vocal **i**, i tots els signes de la fila vuit de consonants tenen la consonant **n**.

Ventris analitza la segona ciutat i s'adona que apareix el signe 12, **-so-**. Els altres dos signes, 70 i 52, estaven en la mateixa columna de vocals que el signe 12 (**-so-**), implicant que aquests signes tenen també la vocal **o**. Llavors per a la segona ciutat col·loquem la síl·laba **-so-** i les vocals **o** al seu lloc corresponen i les lletres restants les deixem com una incògnita:

Ciutat 2 = 70-52-12 = ?o-?o-so = ?

Si ens fixem on està el signe 52 en la taula, podem observar que es troba en la mateixa fila que el signe 30, signe que ja hem analitzat anteriorment i que sabem que la consonant és la **n**. Per tant ja tenim **?o-no-so** i amb una mica de coneixement de ciutats de la zona podem concloure que la ciutat 2 és en realitat Cnossos, **Cnosos** en grec (Knosos en lineal B).

Aplicant tota la informació aconseguida fins ara, podem desxifrar parcialment la tercera ciutat:

Ciutat 3 = 69-53-12 = ??-?i-so

L'únic nom que semblava encaixar era **Tulisos** (tu-li-so), una important ciutat en el centre de Creta. Ventris acabava de descobrir tres noms de llocs i els valors sonors de vuit signes diferents:

Ciutat 1= 08-73-30-12 = a-mi-ni-so = Amnisos

Ciutat 2 = 70-52-12 = ko-no-so = Cnosos

Ciutat 3 = 69-53-12 = tu-li-so = Tulisos

Ara Ventris podia deduir els valors consonàntics i vocàlics de molts dels signes de la taula, només si es trobaven en la mateixa línia i columna que els vuit signes desxifrats. La majoria de signes es van resoldre parcialment i uns quants completament.

Ventris estava descobrint paraules que constituïen una clara prova a favor del grec com a llengua del Lineal B. També havia descobert que rarament les paraules del Lineal B acaben en **s**, però potser és una omissió consensuada d'escriptura. Els escribes simplement no es molestaven en posar la **s** final, permetent que el lector acabés d'omplir la òbvia omissió. Ventris no va tardar gaire en desxifrar altres paraules, que també semblaven que s'assemblaven al grec, però encara no estava absolutament convençut que el Lineal B fos una escriptura del grec. Creia que potser totes les paraules que havia desxifrat eren paraules importades de la llengua minoica però res més.

A més, per a reforçar la seva hipòtesis, va trobar paraules que no tenien sentit. Va seguir desxifrant noves paraules i va començar a descobrir encara més paraules gregues, com per exemple: *poimen* (pastor), *khalkeus* (bronzista) i *khrusoworgos* (orfebre). Inclús va poder traduir un par de frases senceres. Ara ja no tenia cap dubte que la silenciosa escriptura del Lineal B que, per primera vegada en tres mil anys estava tornant a xiuxiuejar el grec.

Per donar a conèixer el seu descobriment, va sol·licitar aparèixer en la emissora BBC per a parlar del misteri dels escrits minoics. Aprofitant també aquesta oportunitat per a fer públic el seu descobriment.

Entre els seus oients es trobava John Chadwick, un filòleg clàssic que des dels anys trenta havia estat interessat. Durant la guerra, havia passat un temps a Alexandria descodificant codis italians, i, uns anys després es traslladà a Bletchley, on s'encarregà d'atacar les xifres japoneses. Chadwick ja havia intentat desxifrar el Lineal B des de feia temps amb uns amics de la universitat, però no havien aconseguit pràcticament res. Una de les raons per la qual no va avançar en el desxiframent del misteri del Lineal B és perquè no tenien suficient mostra per a poder treballar, no tenien accés a suficients dades per a poder utilitzar diferents mètodes criptoanalítics amb èxit.

Chadwick li va sorprendre moltíssim escoltar l'afirmació de Ventris que deia que ja havia aconseguit desxifrar frases del Lineal B. De la mateixa manera que la majoria d'estudiosos que van escoltar la transmissió van considerar que no era més que el treball d'un aficionat, Chadwick també ho va donar per suposat (quan en realitat no era l'afirmació "tonta" d'un aficionat). No obstant, com a professor de grec que era,

sabia que molta gent li preguntaria sobre l'afirmació de Ventris, és per això que va decidir informar-se en el treball realitzat per Ventris per a poder contestar a l'assetjament de preguntes que tindria en els pròxims dies. Va aconseguir les notes del treball de Ventris i les va llegir en detall, esperant però que estiguessin plenes de contradiccions. Per sorpresa seva, en un par de dies va passar a ser un escèptic del seu treball a un dels primers seguidors de la teoria del Lineal B de Ventris.

Chadwick es va posar en contacte amb Ventris per a oferir-li l'ajuda necessària per acabar de desxifrar per complert el Lineal B. Ventirs no tenia un profund coneixement del grec arcaic, per tant, moltes de les paraules que desxifrava no els hi trobava significat, perquè no formaven part del seu vocabulari grec. L'especialitat de Chadwick en canvi era la filologia grega, l'estudi de l'evolució històrica de la llengua grega, i, per tant, podia demostrar que aquelles problemàtiques encaixaven amb les teories de les formes gregues més antigues. En resum, Ventris i Chadwick formaven l'equip perfecte per atacar el Lineal B.

El grec del Lineal B és 500 anys més antic que el grec de l'època d'Homer, que té 3000 anys d'antiguitat. Per a poder traduir-lo, Chadwick necessitava extrapolar del grec antic establert, les paraules del Lineal B, seguint de molt a prop les tres maneres que es desenvolupa una llengua: Primer, la pronunciació evoluciona amb el temps. Per tant, hi haurà paraules que variïn la seva escriptura lleugerament. Per exemple, la paraula "abocadors de bany" canvia de *lewotrokhowoi* en el Lineal B a *loutrokhooi* en l'època d'Homer. Segon, la gramàtica també canvia. En el Lineal B la terminació del genitiu és **-oio**, però aquesta és reemplaçada en el grec clàssic per **-ou**. Finalment, el lèxic pot canviar enormement al llarg dels segles, algunes paraules neixen i altres moren. Per exemple, en el Lineal B la paraula *harmo* significa "roda", però en el grec posterior significa "carro".

Treballant durament i ajudant-se, no van trigar gaire en poder demostrar el seu domini de l'escriptura. Fins i tot s'intercanviaven breus notes en Lineal B.

L'any 1953 van redactar les conclusions del seu treball en un article anomenat "Prova a favor del dialecte grec en els arxius micènics", publicat en *The Journal of Hellenic Studies*. A partir d'aquest moment, arqueòlegs de tot el món es van adonar que estaven presenciant una revolució.

Sense voler, Ventris i Chadwick havien contradit totes les afirmacions de Sir Arthur Evans i de la seva generació. Primerament, estava el fet que el Lineal B era una escriptura del grec. Segon, si els minoics de Creta escrivien en grec significava que probablement també el parlaven, obligant als arqueòlegs i historiadors a canviar les seves opinions sobre la història minoica. A més, ara semblava que la força dominant de la zona era Micenas i que la Creta minoica era un estat menor on es parlava la llengua dels seus veïns més poderosos. No obstant, hi ha evidències que diuen que abans de 1450 a.C, Minos va ser un estat verdaderament independent amb una llengua pròpia. Per tant, el Lineal A representa probablement la llengua pròpia dels minoics, i el Lineal B és la transformació del Lineal A per a que funcionés com una escriptura del grec, imposada per la conquista dels micènics.

L'any següent, van decidir escriure un informe de tres volums que recollissin tot el seu treball. L'obra es va titular *Documents in Mycenaean Greek* i va ser finalitzada en l'estiu de 1955, llesta per a ser publicada la tardor d'aquell mateix any. Per desgràcia, unes setmanes abans de la impressió, el 6 de setembre de 1956, Michael Ventris va morir en un accident de cotxe. John Chadwick va homenatjar al seu company i amic: "El treball que va realitzar segueix viu i el seu nom serà recordat mentre s'estudiï la llengua i civilització de la antiga Grècia".