La criptografia als conflictes bèl·lics

Creació d'una eina per la criptoanàlisi de la màquina Enigma

Treball de Recerca

Autor:

David Reyes Hernández

Tutora:

Núria Capdevila

Àrea de Matemàtiques i Tecnologia

Institut Rovira - Forns

13 de desembre de 2024

AGRAÏMENTS

Vull agrair a la meva tutora, la Núria Capdevila, el seu suport durant aquest treball i les seves aportacions i suggeriments que han servit com a guia per poder fer-ho el més entenedor i precís possible. També vull agrair a l'Òscar Font haver-me proporcionat la idea en la qual es basa aquesta investigació, i animar-me a buscar la manera de fer-ho realitat.

Per últim, donar les gràcies a la família i els amics que m'han fet costat durant tot el procés, sense ells aquest projecte no hagués pogut ser una realitat.

RESUM

L'objectiu d'aquesta investigació és estudiar la influència i funcionament de la màquina Enigma sobre la disciplina científica que és la criptografia.

Per tal de comprendre com s'arribà a manufacturar Enigma, s'ha fet una recerca històrica del funcionament dels sistemes de xifratge previs al seu desenvolupament. A través d'aquests s'ha pogut obtenir un enteniment complet de la criptografia, analitzant tant els objectius d'aquesta com la metodologia que van emprar els pioners en el seu estudi.

A continuació, s'han desenvolupat diversos codis digitals simuladors d'Enigma, per tal d'obtenir dades experimentals sobre les seves vulnerabilitats i proposar una millora d'aquesta. Finalment, s'analitza si el sistema millorat es podria utilitzar avui dia, comparant-ho amb les pràctiques criptogràfiques modernes i digitals.

Paraules clau: Criptografia, Enigma, xifratge, simuladors.

ABSTRACT

The aim of this research is to study the influence and functioning of the Enigma machine on the scientific discipline that is Cryptography.

In order to understand how Enigma was manufactured, a historical investigation of the operation of the encryption systems prior to its development has been carried out. Through these, it has been possible to obtain a complete understanding of the Cryptography, analyzing both the objectives of it and the methodology used by the pioneers in its study.

Once all this has been studied, there has been the development of several Enigma simulator computer codes, in order to obtain experimental data on their vulnerabilities and propose an improvement of it. Finally, it is analyzed whether the improved system could be used today, comparing it with modern and digital cryptographical practices.

Keywords: Cryptography, Enigma, encryption, simulators.

Taula de continguts

1. Introducció

La criptografia és una de les disciplines matemàtiques i tecnològiques més antigues, malgrat que és també una de les més desconegudes. Des de l'origen de la humanitat, la voluntat d'amagar comunicacions ha estat present en tots els àmbits socials i, sobretot, en l'àmbit polític.

En la Segona Guerra Mundial, es va dur a terme el salt criptogràfic més important de la història a través de la Màquina Enigma, un sistema de xifratge alemany amb un rendiment objectivament superior als que empraven els països enemics com els Estats Units, Anglaterra o la Unió Soviètica. Finalment, Enigma, malgrat la seva modernitat, fou desxifrada pels britànics i va ser la principal via de captura de missatges nazis, que va permetre la victòria dels aliats.

Aquests esdeveniments poden portar el lector a fer-se la següent pregunta: Què hauria passat si, en un conflicte amb més de 55 milions de morts, la màquina Enigma s'hagués mantingut indesxifrable? És clar que totes les conclusions serien especulatives, però, el que sí que és clar és que els nazis alemanys no haguessin perdut un gran avantatge respecte a la resta de forces bèl·liques.

És per això que la motivació d'aquest treball és analitzar experimentalment els errors de la màquina Enigma, i comprovar si es podria proposar una millora del funcionament d'aquesta. En conseqüència, també cal determinar si, aplicant aquests canvis, la màquina seria realment "indesxifrable".

A més, cal tenir en compte que estem realitzant aquesta investigació quan la criptografia des de la creació de la màquina Enigma ha avançat exponencialment. Aquesta ja està present en els nostres sistemes informàtics, i constitueix el pilar fonamental de la transmissió de dades per Internet. Això motiva a qüestionar-se si Enigma segueix mantenint una vigència avui dia, o si, al contrari, els sistemes criptogràfics han avançat en gran manera, deixant-la inservible per a qualsevol aplicació moderna.

1.1 Objectius de treball

A continuació es llisten els objectius que s'han plantejat per desenvolupar la recerca:

- Estudiar la influència de la criptografia a la nostra societat i, sobretot, als principals conflictes bèl·lics de la nostra història.
- Examinar la progressió dels mètodes de xifratge a través d'un Marc Teòric que englobi tots els tipus de comunicacions xifrades històricament i la seva metodologia.
- Entendre i ser capaç d'analitzar el funcionament de la Màquina Enigma i el procediment emprat perquè les seves comunicacions foren interceptades i desxifrades.
- Crear un simulador complet de la màquina Enigma a través d'un codi *Python.*
- Elaborar un programa de *Python* per poder criptoanalitzar Enigma, i proposar millores sobre el seu funcionament.
- Avaluar a partir de les dades obtingudes la vigència d'aquesta Enigma millorada actualment.

1.2 Metodologia i estructura del treball

El desenvolupament d'aquest Treball de Recerca consta de dues parts diferenciades, el "Marc Teòric" i el "Marc Pràctic" o "Treball de Camp".

En la primera part es fa un estudi històric de la disciplina criptogràfica que és essencial i codependent amb el procés d'elaboració de la part pràctica.

Per tant, es busca una informació verídica, agafada de fonts diverses i verificades. Entre aquestes es poden destacar el llibre "Història de la Criptografia" de Manuel J. Prieto, escriptor cèlebre de divulgació històrica que, en aquesta obra, tracta de manera cronològica l'evolució de la disciplina criptogràfica amb gran rigor científic. A més, cal afegir també les aportacions de l'Òscar Font, que és un dels dos únics posseïdors a Espanya d'una màquina Enigma militar, a més d'un expert en criptografia de primer nivell, amb el qual he pogut mantenir una correspondència i que ha donat la idea sobre la qual se sustenta aquest Treball de Recerca. La resta d'informació ha estat extreta de webs i articles en línia degudament assenyalats a la bibliografia del treball i citats, quan hagi estat necessari, al cos d'aquest.

D'aquesta manera s'ha pogut analitzar l'ús i funcionament d'una quantitat adequada i heterogènia de mètodes de xifratge, que serveixen com a precursors per entendre com s'arriba fins a Enigma i la seva creació i funcionament.
Aquesta investigació se centra sobretot en com s'utilitzaren aquests mètodes en les situacions de conflicte bèl·lic, ja que és en aquests casos on la criptografia va proliferar i arribar al seu màxim exponent. Això passà pel motiu que era essencial l'intercanvi d'informació rellevant entre cadascun dels bàndols sense que aquesta fos interceptada per l'altre, ja que, si això fos així, estratègies rellevants serien compromeses i no es podrien dur a terme com eren planificades.

Pel que fa a la segona part, el Treball de Camp es tracta de l'elaboració d'un mètode d'anàlisi de les principals vulnerabilitats d'Enigma, que disminueixen la seva seguretat envers els sistemes de programació actuals.
L'objectiu de tot això és veure com es podria evitar el desxifratge del dispositiu mitjançant la maquinària actual, analitzant com va ser desxifrat pels britànics en el passat, i proposant una millora d'aquest en l'actualitat.

En conclusió, aquest Treball de Recerca consisteix en una breu anàlisi de la progressió de la disciplina criptogràfica, centrant-se sobretot en la màquina Enigma. Així s'avalua la seguretat actual dels mètodes de criptoanàlisi inventats a la Segona Guerra Mundial, per proposar millores que els proporcionin immunitat contra el desxifratge del segle XXI.

Per dur a terme aquesta anàlisi ja esmentada s'utilitza el llenguatge de programació *Python* per poder programar el funcionament del sistema i ser capaços així de fer certes simulacions a partir de les quals podem comprovar la seva efectivitat i extreure les nostres conclusions finals.

2. Què és la criptografia?

Segons l'Enciclopèdia Britànica, la criptografia és "la pràctica de xifrar i desxifrar missatges en codi secret en ordre de fer-los il·legibles per a tothom excepte el seu receptor" (AA.VV, 2024).
Què significa això? Per entendre-ho millor, primer hem de definir els conceptes de "xifratge" i "codificació", que no són sinònims.
Ambdós es refereixen a l'acció de fer un missatge incomprensible per a qualsevol humà, però la diferència radica en la presència d'una "clau".

En el cas del xifratge, el missatge es fa inintel·ligible a través d'un mètode determinat, i, per revertir el procés, és a dir, desxifrar-ho, el receptor ha de tenir una clau determinada, que l'emissor ha de proveir. En conseqüència, per interceptar-se la comunicació, s'ha de conèixer el mètode de xifratge emprat i la clau en qüestió.
Si ens referim a codificació, trobem només la correspondència entre un element i un altre. Per exemple, nosaltres podem decidir que la paraula "poma" és el número "67", i anotar això en un diccionari de codis, de manera que si l'emissor i receptor el tenen, poden entendre el significat del missatge. Per tant, la seguretat de la comunicació depèn només en el secret d'aquest diccionari.

Per això, podem concloure que el xifratge és més segur que la codificació. A més, aquesta última, històricament, ha causat més problemes logístics, ja que la seva efectivitat és directament proporcional a l'extensió del codi, cosa que provoca que sigui més pesat transportar i transmetre el diccionari que el conté.
El problema que té l'ús del xifratge és que sovint comporta raonaments matemàtics complexos, i, per tant, no està a l'abast de tothom.

La criptografia estudia aquestes dues pràctiques, i també la combinació entre elles. Dins d'això, apareix també el concepte de criptoanàlisi i la figura del criptoanalista, la persona que es dedica a interceptar i trencar el secret darrere d'aquests missatges.
La presència d'individus que vulguin accedir a certes comunicacions privades obliga l'emissor a millorar el xifratge o codificació que utilitza, i en conseqüència provoca que la disciplina criptogràfica avanci.

També cal aclarir una confusió que esdevé sovint: l'esteganografia, és a dir, el procés que es fa amb l'objectiu d'ocultar la seva existència a ulls de tothom excepte l'emissor i el receptor, no és part de la criptografia, ja que no s'està xifrant el contingut, només amagant-ho a través d'un mecanisme o procediment extern al mateix missatge. Així i tot, aquesta pràctica se sol mesclar sovint amb els mètodes criptogràfics i la veurem també a la part teòrica d'aquest treball.

El concepte que engloba totes aquestes disciplines diferents, és a dir, la criptografia, la criptoanàlisi i l'esteganografia, és la "Criptologia". Aquest terme és massa general, i per clarificar el màxim possible el contingut a explicar, no serà emprat d'aquí en endavant.

2.1 Usos i aplicacions

Les aplicacions de la criptografia a la nostra societat són pràcticament infinites, ja que aquesta apareix sempre que l'humà necessiti encobrir la seva comunicació. Per tant, podríem dir que la criptografia és una conseqüència de la voluntat humana de transmetre i rebre missatges, i que per això té un origen molt pròxim a la creació de l'escriptura en si mateixa.
Aquesta disciplina ha adquirit una gran validesa històrica, sobretot per la seva influència global a causa del seu ús en els grans conflictes bèl·lics, des del seu ús per part de l'emperador romà Juli Cèsar a l'Antiguitat Clàssica, fins als espies de la Stasi a la Guerra Freda. La seva fama és causada per tots aquests esdeveniments històrics que posteriorment s'analitzaran amb més profunditat, però la criptografia en l'actualitat és un element clau que de vegades utilitzem sense saber-ho.

Per exemple, les nostres dades mèdiques o personals de caràcter legal, als països de la Unió Europea, han de ser protegides, per llei, aplicant mesures com el xifratge. També les empreses tecnològiques que desenvolupen les *apps* que utilitzem quotidianament compten amb fortes barreres criptogràfiques per tal de protegir les dades dels seus usuaris. Si s'entra a *WhatsApp*, es pot observar que en qualsevol dels xats hi ha una advertència que et notifica que els missatges són xifrats d'extrem a extrem, per tal que la comunicació no esdevingui compromesa.

3. Història de la criptografia

3.1 El xifratge a l'època clàssica

3.1.1 Primeres aparicions

Es considera com a primera evidència de l'ús de la criptografia una escriptura del segle XIX aC a la tomba del noble egipci Khnumhotep II, situada a la ciutat de Menet Khufu. En aquesta s'havien utilitzat jeroglífics amb modificacions, i, en alguns casos, canviats de posició. Així i tot, aquests canvis no tenien l'objectiu d'amagar el missatge, sinó de donar-li una major bellesa estètica, ja que en ell es relataven els actes més notoris de la vida del cap egipci.

El primer text que es xifraria amb voluntat criptogràfica, és a dir, de fer intel·ligible el seu contingut, arribaria segles més tard, al voltant de l'any 1500 aC a la ciutat de Mesopotàmia. En aquest cas, es va voler ocultar la recepta d'un vernís emprat en la manufactura de ceràmiques mitjançant la modificació dels símbols de l'escriptura cuneïforme, creada pels sumeris [Figura 1].

Figura 1: Exemple d'escriptura cuneïforme. (2014). Mj2Artesanos.es

3.1.2 Ús a la societat grecoromana

Als principis de l'època clàssica trobem diversos casos d'esteganografia que Heròdot d'Halicarnàs (historiador grec) va descriure a les seves *Històries*. Els més destacats són el transport d'un missatge amagat al ventre d'una perdiu que un caçador portà al seu destinatari i l'escriptura d'un missatge a la calba d'un home, de

manera que quan els cabells li creixessin passés desapercebut i el receptor només hagués de rapar-li el cap per fer-lo visible.

De totes maneres, posteriorment, al segle V aC, els espartans construirien el que es considera el primer dispositiu criptogràfic de la història: l'escítala [Figura 2].

Figura 2: Escítala espartana. (n.d). Wikimedia Commons

El sistema que es desenvolupà és senzill, però efectiu en el context de l'època: es donava una vara exactament igual a emissor i receptor (amb el mateix nombre de cares). L'emissor enrotllava una tira de cuir al voltant d'aquesta i escrivia el missatge de forma horitzontal en les diferents fileres, de manera que en desenrotllar el cuir només quedes una successió de caràcters il·legible. El destinatari només havia d'enrotllar la tira en la seva vara i podria llegir el missatge en clar sense problemes.

Concloent amb aquesta època, hem de parlar del mètode que porta per nom el d'un dels més rellevants militars i polítics de l'Antiga Roma, Juli Cèsar. Aquest fou el primer que pensà a alterar el missatge a enviar avançant o retrocedint tots o alguns dels seus caràcters un nombre definit de lletres en l'alfabet en ús [Figura 3].

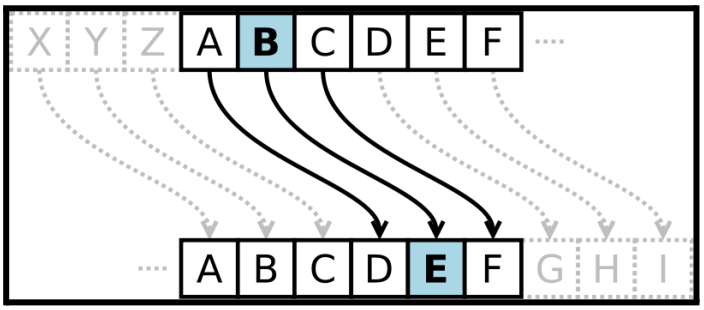


Figura 3: Exemple de xifratge Cèsar en l'alfabet català. (n.d). Wikimedia Commons

D'aquesta manera naixé el xifratge Cèsar, que serviria de base per criptografia posterior, més prolífera i complexa.

3.2 La criptografia al món àrab

L'expansió de l'islam i de la societat musulmana als segles X i XI arribà al seu punt àlgid, conformant el seu imperi les penínsules Ibèrica i Aràbiga i part notable d'Àsia i Àfrica. Això causà l'apogeu de les comunicacions xifrades, per protegir-se de la intercepció dels nombrosos enemics que l'exèrcit islamista cultivà.

Al marge d'això, els musulmans, que volien continuar exercint el seu domini geogràfic i polític incontestable, plantejaren també maneres de desxifrar els missatges emesos pels bàndols contraris, és a dir, de fer criptoanàlisi.

Cal destacar que, fins al moment, els únics mètodes criptogràfics que s'havien vist eren els anomenats de substitució, és a dir, canviar lletres per algun tipus de simbologia o els de transposició, com el xifratge Cèsar, desplaçant aquestes lletres un nombre *n* de posicions. Aquests es creien segurs i no patirien innovacions.

Tot canviaria quan Abu Yusuf Yaqub ibn Ishaq Al-Kindi, savi àrab amb més de 270 obres de diverses disciplines científiques i culturals, elaborà un tractat que anomenà *En desxifrar correspondència encriptada*, on desvelaria el primer procediment criptoanalista de la història. Aquest seria l'anàlisi de freqüències, que es tractaria de l'estudi de la quantitat de vegades que cada caràcter apareix a un idioma concret, per desxifrar un text a partir de l'abundància de cadascun dels símbols o lletres que han substituït aquests. Per tant, si es coneixia la freqüència de la lletra "A", es podia conèixer el missatge si s'estudiava conjuntament amb la freqüència de "B", "C", "D"... [Figura 4].

Freqüència alta		Freqüència mitjana		Freqüència baixa	
Lletra	*Freqüència %*	*Lletra*	*Freqüència %*	*Lletra*	*Freqüència %*
E	16.78	R	4.94	Y	1.54
A	11.96	U	4.80	Q	1.53
O	8.69	I	4.15	B	0.92
L	8.37	T	3.31	H	0.89
S	7.88	C	2.92	G	0.73
N	7.01	P	2.76	F	0.52
D	6.87	M	2.12		

Figura 4: Freqüència de les lletres abundants en els textos escrits en castellà. Extret de RODRÍGUEZ SANTOS, Alberto. Criptografia: Métodos Clásicos. Epsilones.[1]

[1] Citació completa a la bibliografia [18]

3.3 La criptografia a l'Època Medieval i al Renaixement

3.3.1 Homofonia al xifratge de substitució

Arran dels descobriments d'Al-Kindi, a Europa Medieval apareixen dues grans figures que idearien nous mètodes per evitar aquest mètode criptoanalista: el monjo Roger Bacon i Gabriel de Lavinde, secretari del papa Clement VII.

Aquest últim, amb l'objectiu de protegir les comunicacions del seu superior, pensà en l'ús d'homòfons en els seus nomenclàtors, és a dir, els símbols que utilitzaven per encobrir les paraules del missatge.

Era molt freqüent l'ús de diversos homòfons en les paraules més abundants, per així fer inservible l'anàlisi de freqüències. Moltes vegades, també hi incloïen símbols nuls, sense cap significat, per complicar encara més aquest procés.

3.3.2 El xifratge polialfabètic

A principis del segle XVI, l'any 1518, es publicaria *Polygraphia* (Trithemius, 1518), de la mà de Johannes Trithemius, monjo abat del poblat alemany de *Sponheim*. En aquest treball, l'erudit en matemàtica i astrologia exposaria el seu mètode revolucionari que serviria de base per la criptografia moderna, a partir del xifratge polialfabètic, cosa que faria que fos considerat com a pare d'aquesta disciplina.

El xifratge polialfabètic és el tipus de xifratge on s'utilitzen diversos alfabets per produir la substitució de les lletres o caràcters d'un missatge. En el cas de Trithemius, ell presentaria un mètode en el qual cadascun dels alfabets es desplaçaria una posició (basant-se així en el xifratge Cèsar) i el nombre d'alfabets vindria determinat pels caràcters de la paraula a xifrar. Així crearia la *tabula recta*, on l'alfabet original és l'eix horitzontal i el nombre que correspon amb cadascun dels alfabets desplaçats és l'eix vertical.

D'aquesta manera, si volguéssim xifrar la paraula "CASA" [Figura 5], hauríem d'agafar el primer alfabet, invariat, on la lletra "C" seria la mateixa. Per la segona lletra, la "A", agafaríem el segon alfabet desplaçat una posició, que correspon amb la "B" i viceversa. Així obtindríem "CBUD" com a paraula xifrada.

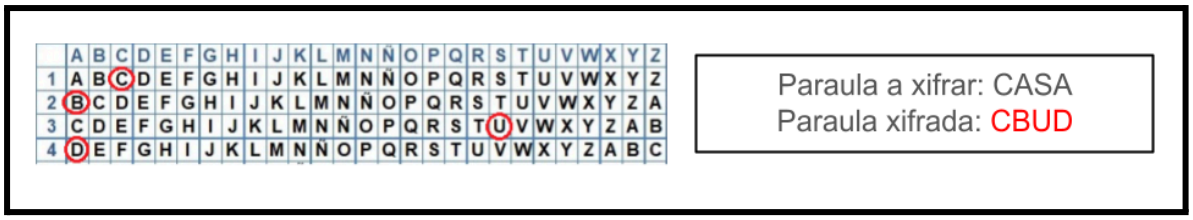


Figura 5: Exemple del xifratge polialfabètic de Trithemius en l'alfabet espanyol. Elaboració pròpia.

Cal destacar que les lletres iguals, amb aquest mètode, no se substitueixen pel mateix caràcter, com passa amb "CASA", on la lletra "A" es correspon primer amb la "B" i després amb la "D". En conseqüència, el xifratge polialfabètic es desfà definitivament de l'anàlisi de freqüències.

La variant més rudimentària d'aquest tipus de xifratge vindria de la mà de Leone Battista Alberti el 1404, el qual fou el primer a fer ús del polialfabetisme en un xifratge el qual funcionava a partir de dos discs superposats [Figura 6]. D'aquesta manera s'indicava la correspondència entre les diferents lletres, alineant una de les del disc interior amb una del disc exterior i anar canviant això en cada paraula del missatge, informant el receptor d'això.

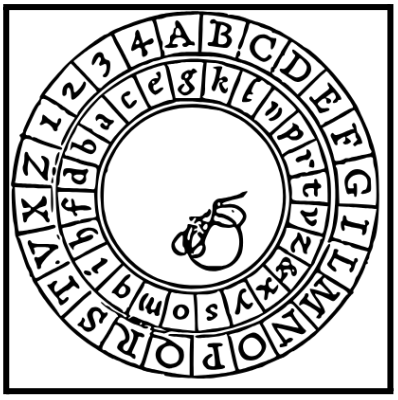


Figura 6: Disc d'Alberti. (n.d). Wikimedia Commons.

De totes maneres, aquest presentà un error que no trobem en el cas de Trithemius, i és que, pel seu correcte funcionament, emissor i receptor han de tenir discs idèntics, i la pèrdua d'aquests posa en gran perill la comunicació.

El mètode de xifratge polialfabètic que adquirí la fama més gran fou el de Blaise de Vigènere, diplomàtic francès, que es creà a partir dels mencionats en aquest apartat.

En aquest cas, trobaríem la *tabula recta* de Trithemius, però en presència d'un altre clau, al marge dels desplaçaments de cada alfabet. Per xifrar el nostre missatge, hem d'escollir una paraula clau qualsevol, i posar-la, repetida les vegades que sigui necessari, a sota del nostre missatge, fins que abasti tota la seva llargària [Figura 7].

Missatge:	B	O	N	D	I	A
Missatge amb clau:	R	I	U	R	I	U

Figura 7: Missatge convertit amb la clau "Riu". Elaboració pròpia.

Per exemplificar, volem xifrar el missatge "Bon dia", i volem emprar la clau "Riu" per fer-ho. Llavors, el nostre missatge aplicant la clau seria "RIURIU".

Per emprar el xifratge de Vigènere hauríem de modificar la *tabula recta*, fent que l'eix vertical, en comptes de ser el nombre de l'alfabet, sigui un altre alfabet original. D'aquesta manera, si la primera lletra del nostre missatge en clau, "B", es correspon amb "R", que és la primera lletra del missatge amb clau, la intersecció entre aquestes dues lletres a la taula, serà el primer caràcter al nostre missatge xifrat, i així continuaríem fins al final de la frase [Figura 8].

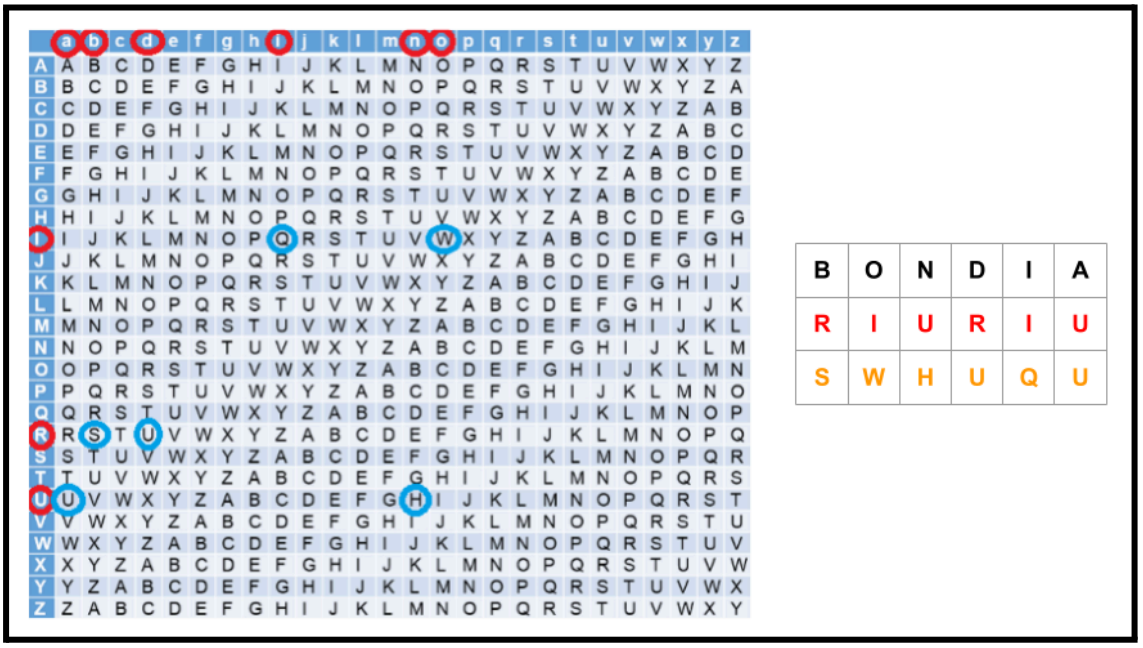


Figura 8: Exemple de xifratge Vigènere amb la frase "Bon dia" i la clau "Riu". Elaboració pròpia.

Així obtindríem el missatge xifrat “SWUHUQU”, el qual, per ser desxifrat, el receptor hauria de conèixer el procediment de la *tabula recta* i la clau inventada per l’emissor. Amb això, faria el mateix que en el xifratge però de manera inversa, agafar la primera lletra del missatge en clau, marcar-la en un dels eixos i, en aquella fila o columna, buscar la lletra del missatge xifrat. Una vegada trobada i marcada, la lletra del missatge en clar seria la que correspon a l’eix oposat del qual hem marcat prèviament [Figura 9].

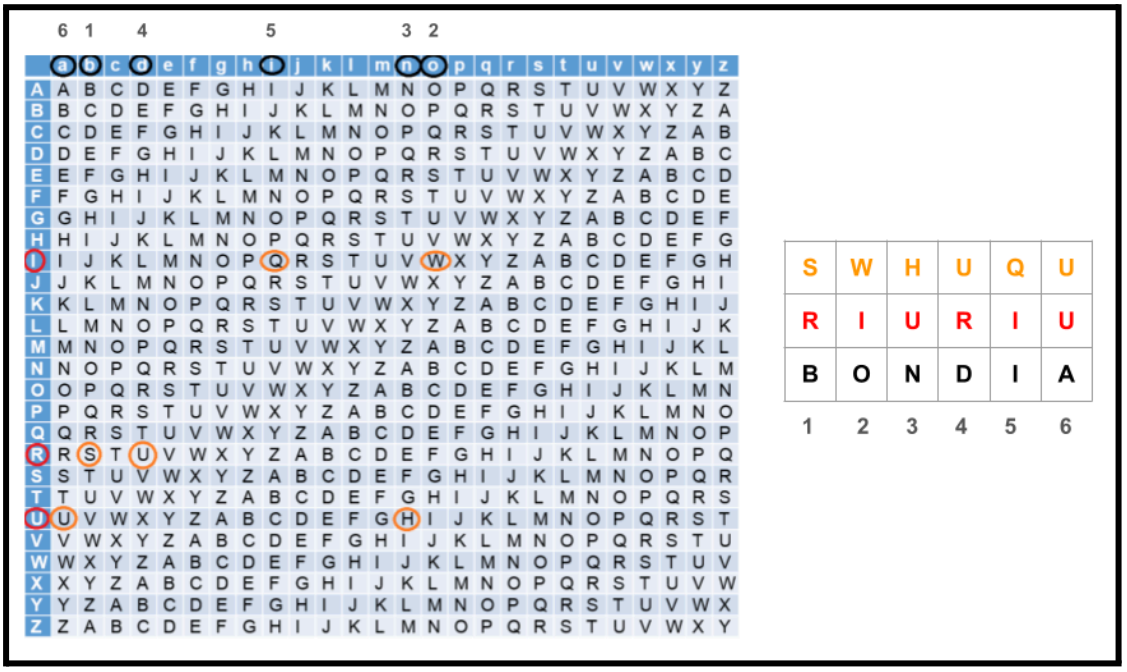


Figura 9: Exemple de desxifratge Vigènere amb el missatge xifrat “SWHUQU” i la clau “Riu”. Elaboració pròpia.

Aquest sistema criptogràfic robust i sense precedents a l’època va ser considerat durant un llarg temps com una “xifra indesxifrable”, ja que per poder fer una criptoanàlisi exitosa era necessari saber la quantitat de desplaçaments en cadascun dels alfabets i, a més, la clau addicional que l’emissor hi afegia al missatge, coses que feien, com ja hem mencionat prèviament, obsolet l’anàlisi de freqüències.

Així i tot, al segle XIX, Frederich Kasiski va aconseguir elaborar un mètode efectiu per trencar el xifratge Vigènere, cosa que li va treure la fama esmentada i forçà noves innovacions sobre el xifratge polialfabètic. A més, en aquesta època s’esbrinà que el xifratge Vigènere fou erròniament atribuït, i el seu creador real fou Giovan Battista Bellaso, criptòleg italià que el publicà abans que Vigènere en el seu treball “*La cifra”* (Battista Bellaso, 1553).

3.4 La criptografia a la Primera Guerra Mundial

3.4.1 Context històric de la Primera Guerra Mundial

Després d'haver vist els inicis d'aquesta ciència relativament nova que és la criptografia, i els pilars en les quals es fonamenta, tant pel xifratge (substitució, transposició, polialfabetisme…) com per la criptoanàlisi (anàlisi freqüencial), ara arribem a l'època en la qual la disciplina començà a popularitzar-se. Aquesta passaria a esdevenir la cara oculta de la Primera Guerra Mundial, disputada entre les Potències Centrals (Alemanya, Àustria-Hongria i Itàlia) i la Triple Entesa (Regne Unit, França i Rússia), entre els anys 1914 i 1918, amb la victòria de les últimes. El conflicte causà, aproximadament, 8 milions de morts.

3.4.2 El codi Morse

Una de les innovacions mundials més conegudes i popularitzades fou el codi Morse, creat pels estatunidencs Samuel Morse i Alfred Vail l'any 1835, malgrat que la seva aplicació en l'àmbit militar fou en la Gran Guerra[2].

Aquest sistema de comunicació va ser elaborat per a donar ús al telègraf, inventat també pel mateix Morse, que permetia la transmissió d'impulsos elèctrics a través de línies de tensió. El codi desenvolupat passaria a ser un referent gràcies a la seva simplicitat, on la traducció alfabètica es basa en la duració dels polsos elèctrics que el receptor capta per part de l'emissor.

Les línies representen un pols llarg, en contraposició amb els punts, que en representen un de curt [Figura 10].

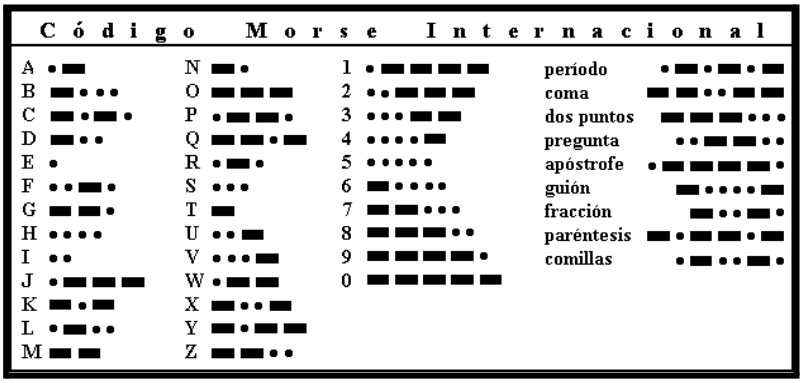


Figura 10: Codi Morse Internacional. (n.d). Promotora Española de Lingüística.

[2] *Gran Guerra*: Nom que fou utilitzat per denominar la Primera Guerra Mundial.

Així i tot, el codi era molt vulnerable i no servia per evitar la intercepció del missatge en clar, per tant, l'única rellevància real per la criptografia va ser el precedent establert per l'emissió de missatges de manera quasi instantània en distàncies llargues que el codi Morse i el telègraf permetien.

3.4.3 La ràdio i el principi de Kerckhoffs

El telègraf llavors donà pas a la invenció de la ràdio, és a dir, al dispositiu capaç de transmetre impulsos elèctrics sense cables a partir de la propagació en l'aire d'ones electromagnètiques.
Aquesta màquina, creada per l'italià Guillermo Marconi, funcionaria per primera vegada l'any 1897, enviant un missatge a un receptor situat a sis quilòmetres de l'emissor.
L'èxit de l'aparell provocaria la substitució de tots els aparells de comunicació militars per la ràdio, ja que els seus beneficis eren exponencialment majors. L'únic problema era que qualsevol persona amb coneixement del funcionament i la possessió d'un aparell radiofònic podia interceptar qualsevol senyal on s'estigués emetent una conversació o un missatge amb informació delicada i confidencial. Aquí és on entra el paper de la criptografia, i la renovació d'aquesta disciplina.

Normalment, tant els alemanys com els anglesos, russos i francesos empraven una combinació de xifratge i codificació als seus missatges amb informació bèl·lica. L'exposició dels missatges feia que els criptògrafs s'adherissin al principi de la criptografia formulat per Auguste Kerckhoffs, que diu: "La seguretat d'un algoritme no ha de residir en la complexitat del seu xifratge, sinó en el secret de la seva clau" (Kerckhoffs, 1883).

Principalment, el que Kerckhoffs vol dir amb això és que si suposem que l'enemic coneix el procés d'encriptació i desencriptació del nostre sistema, l'únic que ens protegeix d'ell és la clau emprada. Per tant, per establir una comunicació segura la clau ha de ser canviada amb regularitat i ha de ser complexa. Si això està garantit, no és de gran rellevància el fet que els nostres missatges siguin escoltats o que, fins i tot, es conegui el mètode criptogràfic emprat i el seu funcionament.

A continuació veurem els múltiples mètodes emprats pels diversos bàndols al conflicte.

3.4.4 El xifratge Playfair

Inventat per Charles Wheatstone, científic britànic, l'any 1854, el xifratge Playfair porta el nom de qui el presentà a les institucions militars angleses, Lyon Playfair, que promogué el seu ús i aplicacions bèl·liques.
Per la seva baixa complexitat, aquest només serviria per transmetre missatges estratègics no essencials durant la guerra.

Aquest mètode de xifratge es basa en una espècie de matriu o taula de 5 files i 5 columnes on s'ha de disposar una clau de manera que cap de les lletres es repeteixi, és a dir, si la lletra següent ja ha estat col·locada, l'ometem i la seguim escrivint [Figura 11].
Una vegada fet això, en els forats restants, s'escriu l'alfabet de l'idioma en el qual s'ha escrit la clau en el seu ordre i, de nou, sense cap lletra repetida (incloent-hi les presents al cos del de la clau) [Figura 12].

R	E	V	O	L
U	T	I	N	

Figura 11: Clau en anglès "Revolution" en la matriu de 5x5. Elaboració pròpia

R	E	V	O	L
U	T	I	N	A
B	C	D	F	G
H	J	K	M	P
Q	S	W	X	Y

Figura 12: Clau en anglès "Revolution" amb xifratge Playfair. Elaboració pròpia.

A continuació i a partir de la taula obtinguda, es xifra el missatge. Per exemplificar, voldrem xifrar el missatge en clar "Invasion incoming". Per fer-ho, hem de dividir-ho en grups de dues lletres de manera que quedi "In-va-si-on in-co-mi-ng".
Finalment, haurem de xifrar cadascuna de les divisions seguint les següents regles:

- Si les dues lletres estan a la mateixa fila, se substitueixen per la lletra a la seva dreta [Figura 13].
- Si les dues lletres estan a la mateixa columna, se substitueixen per la lletra de sota [Figura 14].

- Si les dues lletres no pertanyen a la mateixa fila ni a la mateixa columna, se substitueixen per les lletres de les arestes contràries del rectangle que formen entre si [Figura 15]

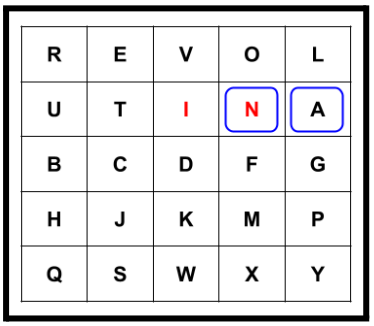


Figura 13: "IN" se substitueix per "NA". Elaboració pròpia.

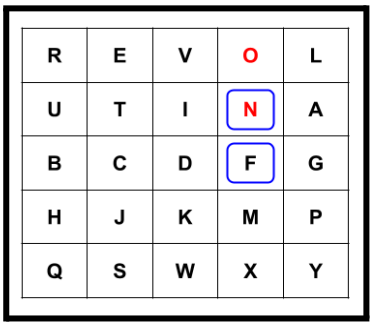


Figura 14: "ON" se substitueix per "NF". Elaboració pròpia.

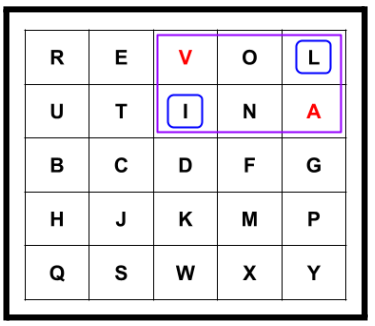


Figura 15: "VA" se substitueix per "LI". Elaboració pròpia.

Llavors obtindríem el nostre missatge xifrat: "NALITWNF NAFENKAF". Per desxifrar-ho, el receptor hauria de seguir el mateix procés (coneixent la clau) i, una vegada amb la matriu feta, dividir el missatge en grups de dos. Amb tot això, hauria de seguir les mateixes regles, però les dues primeres de manera inversa, és a dir:

- Si les dues lletres estan a la mateixa fila, se substitueixen per la lletra a la seva esquerra.
- Si les dues lletres estan a la mateixa columna, se substitueixen per la lletra de dalt.
- Si les dues lletres no pertanyen a la mateixa fila ni a la mateixa columna, se substitueixen per les lletres de les arestes contràries del rectangle que formen entre si.

3.4.5 El telegrama Zimmermann

Aquest telegrama encriptat i codificat pel Ministeri d'Afers Exteriors alemany porta el nom d'Arthur Zimmermann, el cap d'aquesta entitat i l'emissor d'aquest missatge clau el dia 16 de gener de 1917 que desencadenaria la unió dels EUA a la guerra, deixant enrere la seva posició neutral.

Aquesta comunicació, que volia ser establerta amb l'ambaixada alemanya als Estats Units, va ser interceptada pels anglesos, a través d'una unitat militar criptogràfica establerta, anomenada la "Room 40" o Sala 40. Aquest grup de persones estava conformat per tota mena de científics, enginyers i matemàtics que es dedicaven a

capturar els missatges enemics i desxifrar-los, i també a millorar les mateixes comunicacions aliades.

És per això, que en rebre el telegrama, no els hi va ser complicat fer una criptoanàlisi del mètode de xifratge, ja que els mètodes alemanys no eren en gran manera complexos. En comptes de millorar l'aspecte criptogràfic, aquests varen decidir crear un codi complex, alternativa més accessible per l'individu sense nivell avançat en matemàtiques.
El problema arribà quan, abans de ser enviat el telegrama esmentat, l'exèrcit anglès havia capturat un dels llibres de codis que havia deixat enrere un vaixell alemany vençut. És a dir, els alemanys no tenien massa protecció, i eren inconscients d'això.

El missatge en clar no va tardar massa a ser desvelat al govern estatunidenc per part de la intel·ligència britànica. El text en qüestió traçava un pla per reprendre atacs imminents contra submarins dels països aliats, però proposant que, al mateix temps, Mèxic declarés la guerra als EUA, amb suport dels alemanys, per així mantenir-los ocupats i al marge del gran conflicte, cosa que mantenia les opcions de la victòria alemanya.

En assabentar-se d'això, el president Woodrow Wilson declarà la seva unió al bàndol aliat en contra d'Alemanya i els països que la recolzaven al conflicte per motiu d'una amenaça contra el país impossible d'ignorar.
En conseqüència, aquest cas històric constitueix un gran exemple del motiu pel qual desenvolupar un xifratge robust té molts més beneficis que desenvolupar un codi extens.

3.4.6 El xifratge Vernam

Aquest xifratge estatunidenc fou creat l'any 1917 per Gilbert Sandford Vernam, treballador d'AT&T (principal empresa de telecomunicacions dels EUA), a través del codi binari i les portes lògiques, amb l'objectiu d'implementar-ho en els telègrafs perquè es poguessin xifrar i desxifrar missatges de manera automàtica, sense error humà.
Les portes lògiques canvien l'estat binari d'un estat lògic a través de l'aritmètica booleana, és a dir, les lleis matemàtiques dels estats elèctrics. Per entendre aquest sistema criptogràfic, només hem de saber que els valors només poden prendre els

valors naturals 0 i 1, on 0 representa manca de voltatge i l'1 en representa presència d'aquest i també les equivalències d'aquests valors en passar per la porta lògica *XOR* o "*Exclusive OR*[3]".
Dins de la porta entren dos valors "A" i "B", els quals representen el nostre missatge i la nostra clau, que ha de ser de la mateixa extensió.

A continuació, s'ha d'utilitzar la taula de Baudot[4], que determina l'equivalència de lletres i nombres en valors binaris.
Una vegada s'obté, s'ha de convertir la primera lletra del missatge a codi binari, i el mateix amb la primera lletra de la clau. Una vegada es tenen ambdós nombres, el primer dígit del primer es correspondrà amb el primer dígit del segon, i així successivament, passant tots aquests per la condició *XOR*.

Per exemple, si es té el missatge "Míssil" i la clau "Segura", llavors el telègraf ha de substituir la primera lletra del missatge "M" pel seu nombre binari (11100) i la primera lletra de la clau "S" també (00101). En obtenir-los, es passa cada parella de dígits per la porta. Com podem veure, els primers dos són un "1" i un "0", per tant, s'obtindrà un "1" com a sortida. Si es fa això amb tots els dígits emparellats, obtindrem el nombre "11001" que, si consultem la taula de Baudot, es correspon amb la lletra "B". Si es repeteix tot això amb totes les lletres del missatge i la clau, s'obté el missatge xifrat "BU32NZ" [Figura 16]. Per desxifrar-ho, la màquina només ha de fer el mateix procés amb el missatge encriptat i la clau.

Missatge	Clau	Missatge en binari	Clau en binari	Codi binari en passar per XOR	Lletra xifrada
M	S	11100	00101	11001	B
I	E	00110	00001	00111	U
S	G	00101	11010	11111	3
S	U	00101	00111	00010	2
I	R	00110	01010	01100	N
L	A	10010	00011	10001	Z

Figura 16: Xifratge del missatge "Míssil" amb el mètode Vernam, a través de la clau "Segura". Elaboració pròpia.

[3] Veure Annex 1. Codi binari [Figura 1]
[4] Veure Annex 1. Codi binari [Figura 2]

3.5 La criptografia a la Segona Guerra Mundial

3.5.1 Context històric de la Segona Guerra Mundial

La Segona Guerra Mundial fou un conflicte bèl·lic on participaren totes les potències mundials, dividides en dos bàndols: les Potències de l'Eix (Alemanya, Itàlia i Japó) i els Aliats (Estats Units, Regne Unit i Unió Soviètica), entre els anys 1939 i 1945.
El conflicte va deixar entre 50 i 70 milions de morts, culminant amb el bàndol aliat sent capaç de frenar i erradicar l'ascens feixista liderat pels nazis a Alemanya.

3.5.2 La màquina Enigma

La innovació criptogràfica més rellevant d'aquesta època fou la màquina Enigma, creada pels alemanys, per esmenar el seu error amb el codi Zimmerman. Mentre les altres potències mundials van seguir emprant els mètodes ja coneguts, o simples variants d'aquests, la intel·ligència alemanya va engendrar la vertadera revolució criptogràfica, que, segons ells, donava lloc a un xifratge, en la pràctica, impossible de desxifrar.

Enigma es compon de quatre parts principals:

- El teclat, on s'escriu el missatge, tant sigui per ser xifrat o desxifrat.
- El panell endollable, que canvia la lletra polsada per una altra, predeterminada per l'operador de la màquina, abans que aquesta arribi als rotors [Figura 17]. Normalment, s'intercanviaven deu parells de lletres, encara que podien ser més.
- Els rotors, els quals són cinc, però a l'encriptació n'hi participen tres, els quals tenen 26 posicions possibles per cada lletra de l'alfabet anglès. Aquests, en rebre una lletra, en retornen una d'altra diferent i avancen posicions periòdicament [Figura 18].
- El reflector, que en rebre el senyal de la lletra del tercer rotor (el final), intercanvia la lletra i fa que el senyal reboti i passi de nou pels tres rotors.

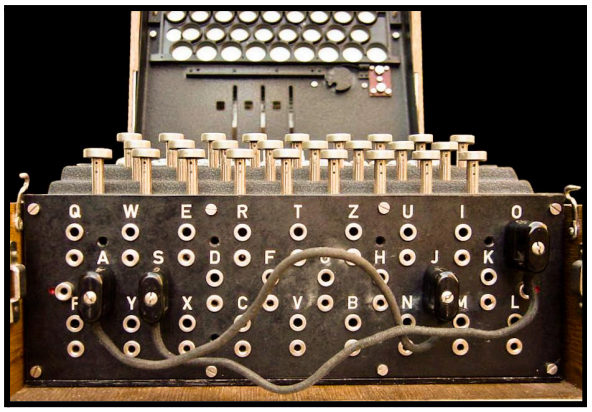


Figura 17: Panell endollable d'una màquina Enigma, on les connexions dels cables determinen els intercanvis de lletres. (n.d). Wikimedia Commons.

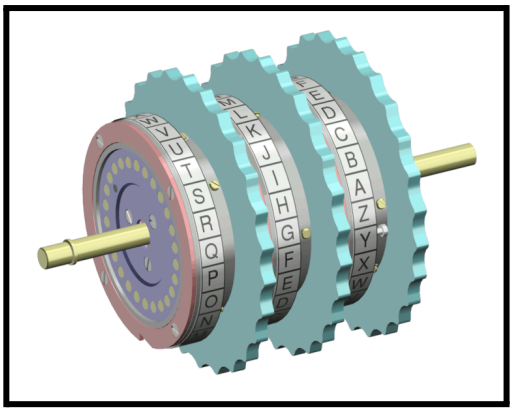


Figura 18: Esquema dels rotors presents a les màquines Enigma. (n.d). Wikimedia Commons.

A partir d'aquestes característiques, podem saber que la màquina empra un sistema de xifratge polialfabètic robust, ja que la presència dels tres rotors, que van avançant posicions, fa que les lletres s'intercanviïn sense cap patró visible, evitant la correlació entre el xifratge de cadascuna d'elles. A més, el fet d'establir un intercanvi previ de lletres a través del panell endollable afegeix una barrera més de seguretat.

De la mateixa manera, l'operador que ha de desxifrar el missatge ha de ser coneixedor de les connexions del panell endollable i de les posicions inicials dels rotors utilitzats per xifrar-lo. És per això que els militars alemanys distribuïen cada cert temps aquesta informació en forma de "fulls d'ajustos" als operaris d'Enigma, ja que aquesta havia de ser canviada cada cert temps per garantir la seguretat del sistema, perquè les dades en qüestió representen la clau del mètode criptogràfic.

3.5.3 Els rotors d'Enigma

La part més complexa del mecanisme d'Enigma és, sens dubte, els seus rotors. Cadascun d'ells està compost d'una part exterior i interior. A la seva part exterior trobem els nombres de l'1 al 26, per cada lletra de l'alfabet anglès, però, a la seva part interior trobem el cablejat [Figura 19], que connecta les correspondències de lletres de manera independent a la part exterior.

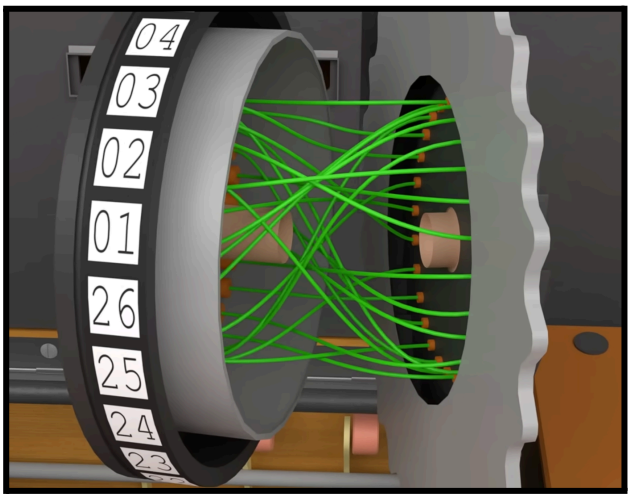


Figura 19: Animació del cablejat d'un rotor d'Enigma. Extreta de JaredOwens Animation "https://www.youtube.com/@JaredOwen".

D'aquesta manera, ens trobem que l'exterior serveix només per saber quantes vegades cada rotor ha canviat de posició, mentre que la part interna és la que estableix les connexions entre lletres, on cadascuna d'aquestes pot correspondre's amb qualsevol de les 26 lletres de l'alfabet.

A més, els tres rotors estan connectats entre si mitjançant pols elèctrics [Figura 20], cosa que fa que la lletra faci un camí completament diferent per cada rotor, depenent de les seves configuracions independents.

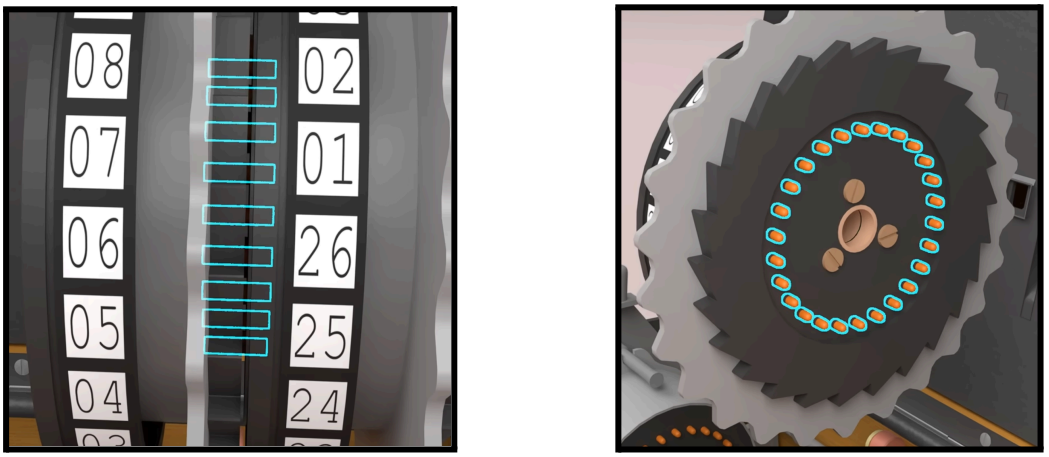


Figura 20: Els pols elèctrics d'Enigma, que permeten el flux d'electricitat entre els rotors. Extreta de JaredOwens Animation "https://www.youtube.com/@JaredOwen".

A més, aquests rotors també tenen una posició de "notch" o gir. En el cas del primer rotor, trobem que rota cada vegada que s'insereix una lletra, el segon gira cada

vegada que el primer fa una volta completa i el tercer, cada vegada que el segon completa una volta, sent el que ho fa amb menys freqüència.

Aquesta rotació la fan conjuntament també els pols elèctrics, d'aquesta manera les connexions i, per tant, les correspondències entre lletres canvien constantment. Així ens assegurem que si teclegem la mateixa lletra diverses vegades, els "outputs" seran diferents.

3.5.4 El reflector, la vulnerabilitat més gran d'Enigma

La part on els alemanys van pensar que podien multiplicar notablement les possibles configuracions de la màquina fou el reflector. Des d'un punt de vista teòric, això és cert, ja que la presència d'aquest les augmenta (vegeu Anàlisi combinatòria d'Enigma), però des d'un punt de vista pràctic, és totalment perjudicial per a la seguretat criptogràfica de la màquina.

Si imaginem el flux elèctric que recorre els rotors d'Enigma, podem observar que aquest fa tot el recorregut amb la mateixa configuració [Figura 21]

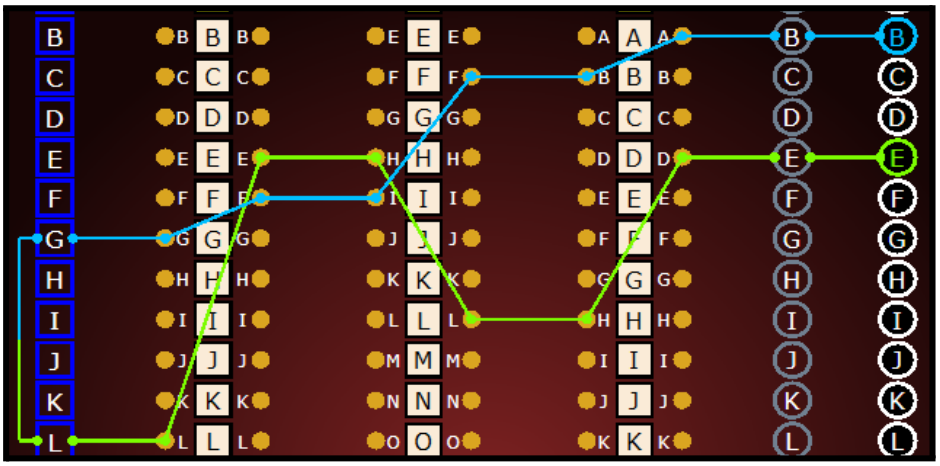


Figura 21: Diagrama de circuit elèctric d'Enigma, on verd és el camí inicial i blau el camí després del reflector. (n.d). EnigmaZone (ZoeZap Software).

Per tant, a través d'això es pot determinar que com el reflector canvia el recorregut a un totalment diferent de l'inicial, una lletra a Enigma mai es podrà codificar com a ella mateixa, dada que esdevindria clau pels criptoanalistes que desxifraren la màquina.

3.5.5 Les "cribs", eines per la criptoanàlisi d'Enigma

La clau per poder realitzar un atac exitós a Enigma són les "cribs", patentades per Alan Turing, matemàtic anglès pioner en el desxiframent de la màquina. La seva definició més estricta és "qualsevol text pla que sabem o sospitem que està en qualsevol punt d'un missatge xifrat" (Ellsbury, 1998). Per exemplificar això, podríem exposar una situació en què interceptem diversos missatges d'una comunicació en la qual sabem que, diàriament, es transmeten estudis meteorològics.

En conseqüència d'això, sabem amb gran certesa que paraules com "pluja", "assolellat", o "precipitacions" estaran al cos del missatge. Si agafem "pluja" com a referència, podem escollir diverses combinacions de 5 caràcters al text xifrat per ser examinades, on, amb alguna de les possibles combinacions d'Enigma, la paraula pugui ser desxifrada, i es desveli tota la configuració del missatge [Figura 22].

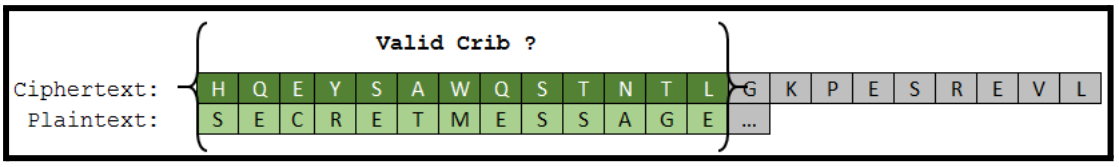


Figura 22: Exemple de "crib" amb el sintagma "Secret Message". (2019). 101computing.net[5]

El problema que trobem amb això és que els missatges xifrats d'Enigma, per prevenir aquesta pràctica, mancaven d'espais, llavors, les nostres configuracions de 5 caràcters serien moltes en un missatge mínimament llarg.

Aquí és on entra en joc la demostració exposada prèviament, on es veu que, per la presència del reflector, la màquina no pot codificar la mateixa lletra que s'ha introduït, per tant, es poden descartar totes les combinacions on una de les lletres de la paraula "crib" correspongui a la mateixa en el text xifrat, reduint exponencialment la quantitat de possibilitats [Figura 23].

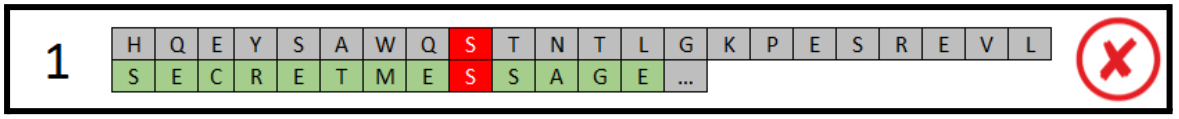


Figura 23: Exemple de "crib" incorrecta, ja que aquesta i el text xifrat comparteixen la lletra "S" a la mateixa posició. (2019). 101computing.net[6]

[5] Citació completa a la bibliografia [38]
[6] Citació completa a la bibliografia [38]

Turing [Figura 24], coneixedor d'aquests factors i després d'una anàlisi profunda dels textos d'Enigma, descobrí l'ús de la fórmula "Heil Hitler", que es repetia sempre al final dels missatges enviats a través de la màquina. Aquesta fou la seva "crib" definitiva, a través de la qual va poder desenvolupar un algoritme capaç d'obtenir les diferents claus d'Enigma emprades mitjançant la computació, amb la creació de la màquina Bombe [Figura 25], un "dispositiu mecànic de càlcul que explotava algunes de les debilitats en l'algoritme d'Enigma per desxifrar els missatges" (Corcoles Briongos, 2013).

Figura 24: Retrat d'Alan Turing, 1936. (n.d). Wikimedia Commons.

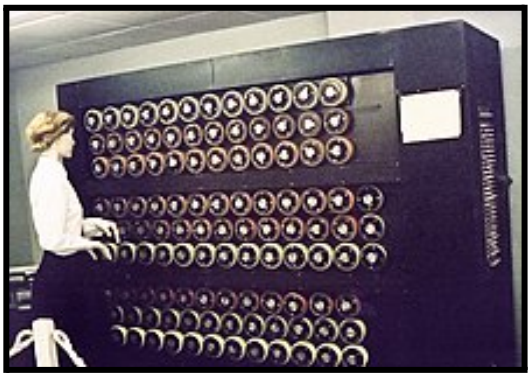


Figura 25: Màquina Bombe anglesa. (n.d) Wikimedia Commons.

3.5.6 Anàlisi combinatòria d'Enigma

Enigma fou l'únic xifratge que es considerà realment "indesxifrable" si s'emprava de manera correcta, en tota la història de les comunicacions xifrades en l'àmbit bèl·lic. De forma teòrica, podem calcular matemàticament la quantitat de possibilitats de configuració que té la màquina, a través de la combinatòria.

Primerament, tenim 3 rotors de 5 els quals hem d'escollir. L'ordre d'aquests importa, ja que no és el mateix escollir els rotors 1,3 i 4 que els rotors 4, 3 i 1, per tant, estem davant d'una variació de *m = 5 i n = 3*.

$$V_{m,n} = \frac{m!}{(m-n)!} = \frac{5!}{(5-3)!} = 60\ possibles\ combinacions\ de\ rotors$$

Aquests rotors també tenen 26 possibles posicions inicials. En aquest cas, de la mateixa manera, ens importa l'ordre, però la posició inicial de diversos rotors pot ser la mateixa, per tant, estaríem davant de variacions amb repetició de *m = 26 i n = 3.*

$$VR_{m,n} = m^n = 26^3 = 17576\, possibles\ posicions\ inicials\ dels\ rotors$$

Finalment, també hem de tenir en compte els 10 intercanvis de lletres del panell endollable. Aquesta és la part més complexa, ja que hem de considerar un nombre de combinacions que va decreixent a mesura que es realitzen els parells de connexions. És a dir, la primera combinació serà l'agrupació de 26 lletres en parells de 2, però una vegada ja tenim la primera connexió, ens trobem davant de 24 lletres que s'han d'agrupar en parells de 2, i així successivament fins a assolir les 10 parelles de connexions. En conseqüència, l'expressió per calcular la probabilitat és definida pels següents coeficients binomials:

$$\binom{26}{2} \cdot \binom{24}{2} \cdot \binom{22}{2} \cdot \binom{20}{2} \cdot \ldots \cdot \binom{8}{2}$$

Sabent que $\binom{m}{n} = \frac{m!}{n!(m-n)!}$:

$$\frac{26!}{2!(26-2)!} \cdot \frac{24!}{2!(24-2)!} \cdot \frac{22!}{2!(22-2)!} \cdot \frac{20!}{2!(20-2)!} \cdot \ldots \cdot \frac{8!}{2!(8-2)!}$$

Que ens dona un resultat aproximat de $5,46999 \cdot 10^{20}$ combinacions, encara que aquestes no són reals, ja que tenim en compte els parells dobles, és a dir, per exemple, hem tingut en compte els aparellaments A-E i E-A, quan, realment, són el mateix. Per evitar això, hem de dividir el resultat per les permutacions de les 10 parelles.

$$\frac{5,46999 \cdot 10^{20}}{10!} \approx 1,5073827 \cdot 10^{14} possibles\ combinacions\ del\ panell\ endollable$$

També s'ha de tenir en compte el reflector, el qual podia convertir qualsevol lletra en qualsevol altra de les 26 de l'alfabet, per tant, tenim la successió del coeficient binomial $\binom{26}{2}$, que ha de ser dividit entre les permutacions de 13, ja que l'ordre dels

parells no importa (que “A” es converteixi en “E” no vol dir que “E” es converteixi en “A”) (Miller, 2019):

$$\frac{26!}{2^{13}\cdot 13!} \approx 7,9058535\cdot 10^{12}\ possibles\ configuracions\ del\ reflector$$

Finalment, si multipliquem els tres càlculs dels rotors, les posicions inicials, el panell endollable i el reflector, obtenim la quantitat total de possibles configuracions de la màquina Enigma:

$$1,2567744\cdot 10^{33}\ possibles\ configuracions$$

Com es pot veure, la quantitat és gegant, fent d’Enigma una màquina teòricament molt robusta. Així i tot, com ja hem vist, el mètode de cribs vulnera exponencialment aquesta seguretat, sent el reflector el culpable d’això. Si decidim retirar el reflector, es perden moltes possibles configuracions, però a la vegada ens immunitzem davant aquest tipus d’atac. Això és el que s’analitza al Marc Pràctic d’aquest treball.

3.6 La criptografia en l'actualitat

3.6.1 El xifratge asimètric o de clau pública

Fins ara, tots els xifratges que hem vist s’anomenen “simètrics”, o de clau privada, ja que s’utilitza la mateixa clau per xifrar i desxifrar els missatges, la qual han de conèixer l’emissor i el receptor de manera secreta, per garantir la seguretat de la comunicació.

Tot això canviaria amb el sorgiment d’Internet, un món on tota (o quasi tota) la informació està a l’abast de milions i milions de persones. Per exemple, en una compra d’una botiga en línia, la connexió entre el seu ordinador i el servidor de la web ha de ser molt segura, ja que és molt probable que s’hagin d’introduir dades bancàries.

En aquest moment és quan trobem un problema, ja que és impossible que el servidor en qüestió enviï la clau de xifratge a l’ordinador que fa la compra, sense ser exposat al fet que el missatge amb la clau sigui interceptat i aquesta sigui compromesa.

En aquests casos, s'empra un sistema criptogràfic "asimètric" o de clau pública, on la clau per encriptar els missatges és coneguda per tots els dispositius que entren a la pàgina, però la clau de desxifratge és només coneguda pel servidor on arriben les dades.

D'aquesta manera, ens assegurem que qualsevol usuari pugui introduir les seves dades a la nostra pàgina, però que aquestes només puguin ser llegides pel servidor al qual estan destinades. Això és conegut com a xifratge "HTTPS" [Figura 26], que és estàndard a totes les webs que es visiten a la xarxa.

Figura 26: Exemple del xifratge "HTTPS" que es troba a les webs d'Internet. (n.d). Wikimedia Commons.

4. Disseny experimental

4.1 Hipòtesi i objectius

Després d'haver vist tota l'evolució de la criptografia des de l'antiguitat fins avui dia, no es pot evitar pensar quin marge de millora hi ha.
L'objectiu principal d'aquest treball és, en conseqüència, executar algun atac de criptoanàlisi envers Enigma, a través de l'elaboració d'un codi amb l'eina Python, per tractar de detectar les vulnerabilitats de la màquina i proposar una possible millora.

El punt concret a analitzar experimentalment serà la diferència d'iteracions (nombre de combinacions a provar) que l'ordinador requereix per desxifrar diversos missatges d'Enigma a través de la força bruta parcial (amb alguns paràmetres coneguts) en dos casos: una màquina Enigma sense reflector (només passa pels tres rotors una vegada) i una original, amb reflector.

La hipòtesi d'aquesta experimentació dedueix que la màquina Enigma sense reflector hauria de ser la més fàcil de desxifrar per força bruta. Així i tot, això no vol dir que sigui menys segura, ja que, com va determinar Alan Turing, una de les vulnerabilitats de l'Enigma original radicava en el seu reflector, ja que aquest l'exposava a un atac criptoanalista pel mètode de les "cribs".
Per tant, si la nostra hipòtesi es compleix, el nostre objectiu ha de ser proposar una nova Enigma, sense reflector, que iguali a l'Enigma estàndard en termes de seguretat contra la força bruta. D'aquesta manera, dissenyarem un dispositiu protegit contra aquestes dues formes d'atac, la força bruta i les "cribs"

Finalment, es podrà avaluar si, amb aquestes millores, aquest "Enigma modern" tindria vigència, és a dir, una seguretat considerable per poder ser emprat actualment.

Per fer tot això, primer s'ha d'elaborar un codi simulador complet d'Enigma, que s'anirà modificant depenent dels paràmetres criptoanalistes que s'hagin d'analitzar.

El motiu pel qual no realitzem una comparació amb una força bruta total és perquè aquest seria totalment impossible encara amb la potència computacional que posseïm avui dia, com analitzarem posteriorment a través de la Teoria de la Complexitat.

4.2 Els paràmetres d'Enigma constants i variables durant l'estudi

Prèviament a explicar els procediments que s'han dut a terme per fer aquest experiment, cal determinar una sèrie de paràmetres en relació amb la codificació de la màquina Enigma que cal tenir en compte per l'enteniment d'aquesta.
En primer lloc, treballarem amb les dades del model Enigma M3, un dels utilitzats al conflicte mundial, que consta de tres rotors, la configuració predeterminada dels quals és la següent [Figura 27]:

Rotor 1	
Alfabet 1	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Wiring 1	EKMFLGDQVZNTOWYHXUSPAIBRCJ
Rotor 2	
Alfabet 2	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Wiring 2	AJDKSIRUXBLHWTMCQGZNPYFVOE
Rotor 3	
Alfabet 3	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Wiring 3	BDFHJLCPRTXVZNYEIWGAKMUSQO

Figura 27: Configuració dels rotors de l'Enigma M3. Elaboració pròpia a partir de les dades extretes de CryptoMuseum.com[7]

Com es pot veure, cada rotor consta de dos paràmetres principals, un alfabet, que es correspon amb les posicions del rotor, i un wiring, que representa les correspondències internes entre parells de lletres dins del rotor.

En conseqüència, si agafem com a exemple el Rotor 1, la lletra A es correspondria amb "E" i viceversa. La qüestió és que aquestes configuracions poden canviar les seves posicions inicials, desplaçant-se cap a la dreta i patint una variació de la configuració predeterminada. És així com es canvien les claus o configuracions d'Enigma per un missatge, que en aquesta investigació es descobriran a través de la força bruta.

[7] Citació completa a la bibliografia [37]

Per tant, per la resta d'aquest Treball de Recerca cal tenir en compte els conceptes de posició dels rotors (alfabets) i posició del wiring dels rotors (wiring).

També s'emprarà la configuració predeterminada del reflector de l'Enigma M3, on "A" es correspon amb "Y" i "B" amb "R", i així successivament [Figura 28]:

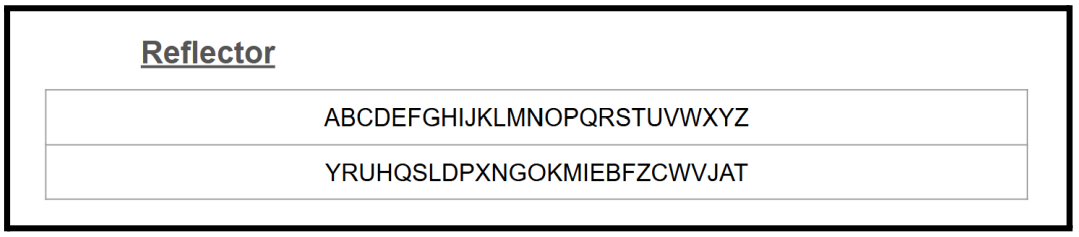


Figura 28: Configuració del reflector de l'Enigma M3. Elaboració pròpia a partir de les dades extretes de CryptoMuseum.com[8]

4.3 Enigma: del mecanisme físic al mecanisme digital

En aquest punt s'exposa el funcionament i les parts del codi de Python que s'ha desenvolupat per crear un simulador de la màquina Enigma. Aquest, com la mateixa màquina, només pot rebre "inputs" o missatges en majúscules i sense espais, i només amb lletres que pertanyin a l'alfabet anglès.

El sistema és iteratiu i funciona a través de bucles, cosa que significa que es repeteix cíclicament per aconseguir totes les lletres del missatge codificades, per finalment ajuntar-les i donar a l'usuari la comunicació xifrada en qüestió.

L'explicació del programa pot semblar complexa, és per això que s'exposa per parts diferenciades, primer fent una explicació de les variables que es modifiquen perquè el programa funcioni, i després el bucle principal el qual les modifica.

La traducció d'un sistema elèctric a un codi digital és difícil, i més si es treballa amb el tipus de màquina on diversos elements funcionen en conjunt per assolir l'objectiu. En el cas d'Enigma, es treballa amb els rotors, el panell endollable i el reflector, que s'ajunten pel funcionament del nostre codi[9] simulador de la màquina.

En primer lloc, per crear cadascun dels rotors, s'han de tenir en compte diversos aspectes:

[8] Citació completa a la bibliografia [37]
[9] Veure Annex 2: Codi del simulador d'Enigma en Python

- La variació de les posicions dels rotors (1-26).
- El “wiring intern” d’aquests i l'equivalència amb les posicions de cada rotor.
- El control del nombre d'“inputs”, per girar cada rotor a la seva posició de “notch”.

En conseqüència, cada rotor té dues llistes amb la informació de les posicions (alfabet1, 2, 3) i equivalències del wiring intern (rotor1, 2, 3eq) [Figura 29]:

```
##ROTORS
alphabet1 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
rotor1eq = [12, 7, 4, 17, 22, 26, 14, 20, 15, 23, 25, 8, 24, 21, 19, 16, 1, 9, 2, 18, 3, 10, 5, 11, 13, 6]

alphabet2 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
rotor2eq = [3, 17, 7, 26, 14, 16, 25, 6, 22, 15, 5, 1, 10, 4, 11, 19, 9, 18, 21, 24, 2, 12, 8, 23, 20, 13]

alphabet3 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
rotor3eq = [2, 4, 6, 8, 10, 12, 3, 16, 18, 20, 24, 22, 26, 14, 25, 5, 9, 23, 7, 1, 11, 13, 21, 19, 17, 15]
```

Figura 29: Llistes de posicions i equivalències de cada rotor. Elaboració pròpia.

S’han convertit ambdues llistes dels rotors (vegeu Paràmetres d’Enigma) en els nombres de la seva posició de l’alfabet. En conseqüència, la lletra final quedarà en notació numèrica, que serà convertida a la seva correspondència alfabètica a través del codi ASCII (“American Standard Code for Information Interchange”). Això es pot veure més clarament a través de la següent taula [Figura 30]:

Posició	A (1)	B (2)	C (3)	D (4)	E (5)
Wiring Rotor	E (5)	K (11)	M (13)	F (6)	L (12)

Figura 30: Equivalències entre les 5 primeres posicions del rotor i el seu wiring intern. Elaboració pròpia.

En el codi, el primer rotor que hem definit té aquestes equivalències. Aquesta taula ens permet veure que si el senyal entra per la posició “A” del rotor, que es correspon amb “1”, el seu wiring intern farà que aquesta equivalgui amb la lletra “E”, que és la número 5 de l’alfabet, i el mateix passarà respectivament amb la resta de parells de lletres.

Convertim les lletres equivalents a nombres, ja que ens és més fàcil treballar només amb variables numèriques durant tot el codi, i després convertir-les a la seva respectiva lletra de l'alfabet.

També cal crear una funció que pugui rotar aquestes llistes (simulant el gir dels rotors físics) [Figura 31]:

```
##ROTACIÓ D'UNA LLISTA (PER PODER REALITZAR EL GIR DELS ROTORS)
def rotar_lista(lista):
    if lista:

        return lista[1:] + [lista[0]]
    return lista
```

Figura 31: Funció de gir de llistes. Elaboració pròpia.

Aquesta funció serveix per a totes les llistes i pot ser executada en qualsevol part del codi, per tant, serà emprada seguint les condicions de rotació específiques de cada mòdul. És a dir, la funció serà emprada pel primer rotor en cada iteració, pel segon rotor quan aquest hagi completat una volta, i pel tercer quan el segon n'hagi completat una.

Posteriorment, establim el reflector, el qual és fix, per tant, només necessita una llista que defineixi la seva equivalència respecte a l'alfabet original, sense una que controli les posicions [Figura 32]:

```
##REFLECTOR
reflector = [25, 18, 21, 8, 17, 19, 12, 4, 16, 24, 14, 7, 15, 11, 13, 9, 5, 2, 6, 26, 3, 23, 22, 10, 1, 20]
```

Figura 32: Llista d'equivalència del reflector. Elaboració pròpia.

En la creació del panell endollable, s'han establert dues llistes, on cada lletra de la primera llista correspon amb la que es troba a la mateixa posició a la segona, i a l'inrevés [Figura 33]:

```
##STECKERBRETT
steckerbrett = ["A","D","R","T","Y","U","O","P","S","G"]
steckerbrett2 = ["L","K","M","I","J","N","Z","H","F","W"]
```

Figura 33: Llista d'equivalència del panell endollable o "Steckerbrett". Elaboració pròpia.

Finalment, tenim el “loop” o bucle principal, on es desenvolupa la connexió entre aquestes funcions quan es rep l’“input” o senyal, és a dir, la simulació de com passaria el senyal elèctric per tot el circuit cada vegada que es polsés una tecla a Enigma.

En aquesta part, el sistema, per cada lletra que hi ha al missatge, es canvia en el següent ordre per aconseguir l’“output”:

1. La lletra es modifica al panell endollable
2. La posició de la lletra a l’alfabet original es correspon amb la lletra de l’alfabet del primer rotor que es trobi a aquesta posició
3. S’intercanvia per la lletra que correspongui amb el wiring del primer rotor
4. Els punts 2 i 3 es repeteixen pels rotors restants
5. La lletra corresponent s'intercanvia al reflector
6. El senyal fa el camí invers dels passos 2, 3 i 4
7. Finalment, la lletra es torna a intercanviar al panell endollable

Aquest recorregut es pot veure millor representat al següent diagrama de flux [Figura 34]:

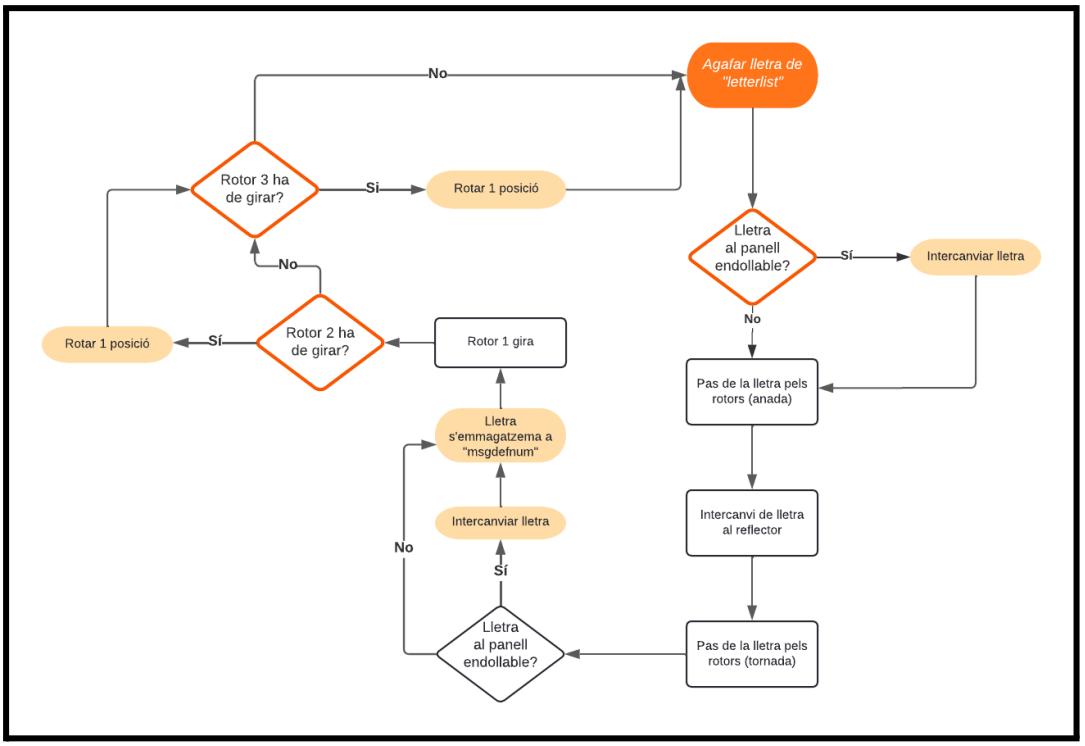


Figura 34: Diagrama de flux del “loop” del codi Python. Elaboració pròpia.

En aquest bucle s'empren diferents variables d'emmagatzematge que s'especifiquen a continuació:

- "letterlist": Emmagatzema totes les lletres que componen el missatge que introdueix l'usuari.
- "msgdefnum": Emmagatzema totes les lletres que componen el missatge xifrat en format numèric.
- "msgdeflletra": Emmagatzema totes les lletres que componen el missatge xifrat una vegada convertides a la seva correspondència alfabètica.

En cada iteració del bucle es comprova també si cadascun dels rotors ha de girar, i, quan ja no queden més lletres per codificar a la llista "letterlist", el bucle finalitza i tots els caràcters emmagatzemats a "msgdefnum" s'uneixen per formar un únic missatge, que serà l'"output", on sortirà el missatge finalment quan hagi passat pel procés criptogràfic [Figura 35].

```
for num in msgdefnum:
    num = chr(65+num)
    msgdeflletra.append(num)

print("Missatge codificat:",''.join(msgdeflletra))
```

Figura 35: Codi que imprimeix l'"output" del missatge. Elaboració pròpia.

Des de la interfície d'usuari, això es veu de la següent manera [Figura 36]:

```
Introdueix el missatge: HOLA
Missatge codificat: MLNM
```

Figura 36: Interfície d'usuari del Simulador. Elaboració pròpia.

Paral·lelament, s'ha desenvolupat també el codi de la màquina Enigma sense la presència d'un reflector, que és el mateix que l'explicat en aquest apartat, però eliminant del "loop" els passos 5, 6 i 7, per tal que el recorregut de l'intercanvi de lletres sigui exclusivament lineal, és a dir, que el senyal no retorni de nou pels rotors.

Per tant, s'han fabricat els dos codis simuladors d'ambdues màquines necessàries per a l'experiment, l'Enigma original i l'Enigma a la qual li retirem el reflector.

4.4 Teoria de la complexitat: Paràmetres a estudiar

La Teoria de la Complexitat dels sistemes computacionals avalua la quantitat de recursos que necessita un computador per realitzar un procés informàtic, sigui en qüestions de temps o de memòria.

Per tant, ens permet analitzar, a través de càlculs matemàtics, la quantitat de recursos necessaris amb la maquinària informàtica actual per la realització d'una criptoanàlisi sobre Enigma.

En primer lloc, sabem que la clau de l'Enigma estàndard amb reflector pot tenir un total de $1.2567744 \cdot 10^{33}$ configuracions (vegeu Anàlisi combinatòria d'Enigma).

Actualment, el processador més potent del mercat, l'AMD Threadripper Pro 7985WX (2024), es constitueix de 64 nuclis (unitats de processament), que funcionen a una freqüència de 5,1 GHz, és a dir:

$$5,1GHz \cdot \frac{10^{12}Hz}{1GHz} = 5,1 \cdot 10^{12}Hz = 5,1 \cdot 10^{12} processos\ per\ segon$$

Per tant, tenint en compte el nombre de configuracions d'Enigma i el nombre de processos que aquesta CPU pot fer per segon, tenim que:

$$\frac{1.2567744 \cdot 10^{33}}{5,1 \cdot 10^{12}} = 2,4642145 \cdot 10^{20} segons = 2,85188993 \cdot 10^{15}\ dies$$

En conseqüència, sabem que per realitzar un atac de força bruta a Enigma necessitaríem segles per poder comprovar totes les combinacions possibles. És per això que encara es pot considerar un sistema lineal segur davant la força bruta.

En el cas d'aquest Treball de Recerca, no disposem dels recursos ni del temps per realitzar un atac d'aquestes característiques, és per això que només realitzarem un atac de força bruta parcial, és a dir, només basant-nos en un paràmetre de la màquina i assumint que en coneixem la resta. Així podrem fer una extrapolació prou precisa de com seria la diferència d'iteracions entre les dues Enigmes que hem dissenyat davant d'un atac de força bruta.

En aquest cas farem la comparativa amb els mateixos textos ("inputs") en dues situacions diferents:

- Es coneixen tots els paràmetres excepte les equivalències del wiring dels dos primers rotors (part interna del rotor).

- Es coneixen tots els paràmetres excepte les posicions inicials dels dos primers rotors (part externa del rotor).

4.5 El codi per la criptoanàlisi d'Enigma

Una vegada desenvolupats ambdós simuladors d'Enigma i determinats els paràmetres que s'han d'estudiar, cal convertir el codi ja creat en una eina de desxifratge per força bruta. Cal destacar que l'eina en qüestió no funciona de forma autònoma, és a dir, que al marge de necessitar una sèrie de paràmetres coneguts, també necessita conèixer el missatge xifrat i el missatge en clar. Per tant, no funcionaria només si tenim un text xifrat per Enigma, sense conèixer la resta de paràmetres.
Així i tot, ens proporciona les dades que necessitem per aquest experiment, ja que només volem saber la quantitat d'iteracions necessàries per arribar del missatge en clar al missatge xifrat, o a la inversa (ja que serien les mateixes).

L'atac per força bruta parcial es perpetra a través de l'addició d'un mòdul de criptoanàlisi sobre el programari ja existent [Figura 37]:

```
while True:
    control1 = 0
    control2 = 0
    rotacions = rotacions + 1

    alphabet1 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
    rotor1eq = [5, 11, 13, 6, 12, 7, 4, 17, 22, 26, 14, 20, 15, 23, 25, 8, 24, 21, 19, 16, 1, 9, 2, 18, 3, 10]
    alphabet2 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
    rotor2eq = [1, 10, 4, 11, 19, 9, 18, 21, 24, 2, 12, 8, 23, 20, 13, 3, 17, 7, 26, 14, 16, 25, 6, 22, 15, 5]
    alphabet3 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
    rotor3eq = [2, 4, 6, 8, 10, 12, 3, 16, 18, 20, 24, 22, 26, 14, 25, 5, 9, 23, 7, 1, 11, 13, 21, 19, 17, 15]

    for i in range (1, step):
        alphabet1 = rotar_lista(alphabet1)

    for i in range (1, rotacions):
        if rotacions == 26:
            step = step + 1
            rotacions = 1
            break
        elif rotacions == 0:
            break
        else:
            alphabet2 = rotar_lista(alphabet2)
```

Figura 37: Mòdul de criptoanàlisi per a les posicions inicials. Elaboració pròpia.

Aquest fragment de codi és un bucle que itera sobre totes les possibles configuracions de posició inicial dels dos primers rotors d'Enigma. La manera en què funciona és provant les 26 possibles configuracions de les posicions del segon rotor per cadascuna de les 26 possibles del primer rotor.

El codi funciona de la mateixa manera per les equivalències del wiring, ja que només cal canviar “alphabet1” per “rotor1eq” i “alphabet2” per “rotor2eq” en els bucles “for” per aconseguir aquest resultat [Figura 38]:

```
while True:
    control1 = 0
    control2 = 0
    rotacions = rotacions + 1

    alphabet1 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
    rotor1eq = [5, 11, 13, 6, 12, 7, 4, 17, 22, 26, 14, 20, 15, 23, 25, 8, 24, 21, 19, 16, 1, 9, 2, 18, 3, 10]
    alphabet2 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
    rotor2eq = [1, 10, 4, 11, 19, 9, 18, 21, 24, 2, 12, 8, 23, 20, 13, 3, 17, 7, 26, 14, 16, 25, 6, 22, 15, 5]
    alphabet3 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
    rotor3eq = [2, 4, 6, 8, 10, 12, 3, 16, 18, 20, 24, 22, 26, 14, 25, 5, 9, 23, 7, 1, 11, 13, 21, 19, 17, 15]

    for i in range (1, step):
        rotor1eq = rotar_lista(rotor1eq)

    for i in range (1, rotacions):
        if rotacions == 26:
            step = step + 1
            rotacions = 1
            break
        elif rotacions == 0:
            break
        else:
            rotor2eq = rotar_lista(rotor2eq)
```

Figura 38: Mòdul de criptoanàlisi per a les equivalències del wiring. Elaboració pròpia.

Per concloure, es col·loca al final del codi un condicional que determina quan una de les configuracions provades és la que proporciona el missatge correcte [Figura 39]:

```
if ''.join(msgdeflletra) == "Missatge xifrat":
    print("Missatge desxifrat correctament per força bruta")
    print("Iteracions necessàries: ", iteracions)
    quit()
```

Figura 39: Condicional per a la finalització de l’atac de força bruta parcial. Elaboració pròpia.

En el condicional, “Missatge xifrat” és el missatge que hem xifrat prèviament, amb qualsevol de les dues màquines Enigma. Per tant, l’“input” que hem d’introduir en executar el codi és el missatge en clar.

El codi, posteriorment, anirà provant totes les possibles configuracions dels dos primers rotors (ja sigui en el cas del wiring o de les posicions inicials) i anirà xifrant el missatge en clar amb totes aquestes configuracions. Quan es doni el cas que alguna d’aquestes configuracions doni el text xifrat equivalent al missatge xifrat que

hem introduït al condicional, el codi pararà i ens donarà la quantitat d'iteracions que han estat necessàries per arribar a aquest resultat.

La variable d'iteracions anirà sumant una unitat cada vegada que es produeixi un intercanvi de lletra en cadascuna de les proves de configuracions recurrents, tant pel programa de l'Enigma sense reflector com pel de l'Enigma completa.

D'aquesta manera, obtenim quatre codis diferents: dos que serviran per atacar els textos xifrats amb l'Enigma original, un sense conèixer les posicions inicials i un altre sense conèixer les posicions del wiring, i uns altres dos per atacar els d'Enigma sense reflector, de la mateixa manera[10].

També cal destacar que en aquests codis s'ha eliminat el panell endollable, ja que, en assumir que ja coneixem la resta de paràmetres aliens als rotors, aquest no afecta en l'estudi del nostre experiment. En conseqüència, els textos introduïts han d'haver estat xifrats sense cap configuració d'aquest panell.

4.6 Textos a estudiar

A continuació s'especifiquen els textos que s'empraran per a la criptoanàlisi d'Enigma, i com seran xifrats prèviament:

- Text 1:

> "L'atac d'ahir sobre les illes de Hawaii ha causat grans danys a les forces militars i navals estatunidenques. Lamento dir-los que moltes vides estatunidenques s'han perdut. A més s'ha sabut que vaixells estatunidencs han estat torpedinats en alta mar entre San Francisco i Honolulu." (Franklin Roosevelt, 8 de desembre de 1941).

- Text 2:

> "Ens proposem iniciar el primer de febrer la guerra submarina sense restricció. Malgrat això, intentarem mantenir als Estats Units d'Amèrica neutrals. En cas de no tenir èxit, proposem una unió amb Mèxic sobre les següents bases: fer la guerra junts, fer la pau junts, ajuda financera abundant i l'enteniment per la nostra

[10] Veure Annex 4: Codis de criptoanàlisi d'Enigma

part que Mèxic reconquerirà el territori perdut a Nou Mèxic, Texas i Arizona.” (Telegrama Zimmerman, 16 de gener de 1917)

Cadascun d’aquests textos ha de ser xifrat per les dues màquines Enigma, per una banda, canviant la configuració del wiring de la predeterminada, i, per l’altra, canviant la configuració de les posicions inicials de la predeterminada[11]. La resta de valors es mantindran iguals per a tots els casos.

Aleshores, la resta de paràmetres es mantenen constants exceptuant els que es volen analitzar (wiring i posicions), com s’havia establert prèviament a l’apartat Teoria de la Complexitat.

4.7 Resultats de la criptoanàlisi

Les següents taules mostren les dades que s’han recollit dels codis de criptoanàlisi, per dos textos diferents en ambdós casos especificats a l’apartat Teoria de la Complexitat. Es mostren el nombre d’iteracions, és a dir, d’intercanvis de lletres que un ordinador ha de fer per tal d’arribar a desxifrar el missatge final trobant la configuració d’Enigma que s’havia emprat per xifrar-lo, a través de la força bruta.

	Iteracions sobre el wiring	
	Força bruta amb reflector	Força bruta sense reflector
Text 1	561.099	240.471
Text 2	319.074	136.746

	Iteracions sobre posicions inicials	
	Força bruta amb reflector	Força bruta sense reflector
Text 1	300.762	128.898
Text 2	1.265.061	542.169

Com es pot veure, els resultats varien depenent del wiring o les posicions inicials que emprem, ja que la força bruta parteix dels valors predeterminats de configuració de l’Enigma M3. Si es comencés la força bruta partint d’uns altres valors, aquests

[11] Veure Annex 3: Missatges xifrats per la criptoanàlisi

resultats també canviarien, independentment que es tracti del mateix missatge xifrat. Així i tot, es pot observar que sempre es manté una diferència aproximada de la meitat d'iteracions, pel mateix text, entre l'Enigma amb reflector i la que no en té.

Per tant, es pot determinar que si s'utilitza la força bruta parcial sobre un missatge xifrat amb les mateixes configuracions de wiring o posició inicial dels dos primers rotors, aquest text xifrat amb l'Enigma sense reflector necessitarà la meitat d'iteracions per ser desxifrat que el mateix text xifrat amb l'Enigma original.

4.8 Anàlisi dels resultats i propostes de millora

Com es pot observar, en tots els casos, s'ha comprovat experimentalment que ambdós textos, per ser desxifrats, necessiten més iteracions per força bruta en l'Enigma amb reflector que en la que aquest no està present, com era l'esperat en la nostra hipòtesi inicial.

En conseqüència, per proposar una millora d'aquesta, s'ha de buscar una manera de fer una Enigma sense reflector que tingui el mateix nombre de configuracions a analitzar que el dispositiu en la seva forma estàndard, que ja s'ha determinat al Marc Teòric, per no estar exposats al mètode criptoanalista de les "cribs".

L'única proposta que es pot fer per intentar igualar tal xifra de configuracions és l'addició de rotors a l'Enigma sense reflector, per augmentar el nombre d'intercanvis de lletres. Teòricament, podem proposar aquest tipus de millora a través de combinatòria.

En primer lloc, si traiem el reflector de l'anàlisi combinatòria d'Enigma, ens queda la multiplicació de les següents operacions:

$$Emprem\ k\ rotors,\ els\ quals\ poden\ tenir\ 26\ posicions\ inicials\colon\ 26^{k}$$

$$Connectem\ els\ 10\ intercanvis\ del\ panell\ endollable\colon 1,5073827{\cdot}10^{14}\ configuracions$$

Ja que ja havíem obtingut les possibles configuracions del panell endollable prèviament (vegeu Anàlisi combinatòria d'Enigma) i hem d'emprar tants rotors com es necessitin (no els hem d'escollir de 5 possibles, com a l'Enigma militar de la Segona Guerra Mundial), ens queda la següent equació, on igualem el paràmetre "k" amb les possibles configuracions de la màquina Enigma amb reflector ($1{,}2567744{\cdot}10^{33}$):

$$26^{k} \cdot 1,5073827 \cdot 10^{14} = 1,2567744 \cdot 10^{33}$$

I obtenim que:

$$k \cdot log(26) = log(\frac{1,2567744 \cdot 10^{33}}{1,5073827 \cdot 10^{14}})$$

$$k \approx 13,37$$

Per tant, podem afirmar que amb 14 rotors augmentaríem la quantitat de configuracions possibles de l'Enigma militar emprada pels nazis, a través d'una Enigma modificada (sense reflector), immune a la criptoanàlisi a través de les "cribs".

Aquesta màquina, per tant, és factible de fabricar, i podria constituir una bona alternativa mecànica als sistemes de criptografia actuals, que depenen de la transformació digital, ja que posseeix una seguretat molt alta davant els atacs de força bruta, que són, teòricament, els únics que podria patir.

En conclusió, es pot confirmar que aquesta màquina Enigma millorada podria ser vigent en l'actualitat, tenint en compte el poder computacional que posseïm avui dia, que no podria desxifrar-la en un període de temps raonable.

5. Conclusions

A través de la investigació realitzada en aquest Treball de Recerca, tant per la part teòrica com per la part pràctica, s'han pogut complir tots els objectius proposats.

En primer lloc, pel que fa a la primera part del treball, s'ha fet una extensiva recerca sobre els mètodes de xifratge precedents a Enigma, tenint en compte la seva metodologia i la seva connexió amb els esdeveniments bèl·lics més importants de les diverses èpoques.
Finalment, s'ha fet una descripció entenedora i extensiva de la funcionalitat de la màquina Enigma, amb tots els conceptes necessaris per al desenvolupament del Marc Pràctic i la comprensió de tots els factors que participaven en aquest.

Per altra banda, la secció pràctica ha estat tot un èxit, ja que s'ha aconseguit fabricar un simulador d'Enigma a través del llenguatge de programació *Python*. A més, també s'han elaborat mòduls per la criptoanàlisi d'aquesta màquina a través de la força bruta, en dos contexts diferents, amb reflector i sense.
Mitjançant les dades que hem obtingut, hem estat capaços de demostrar experimentalment la hipòtesi inicial que la màquina Enigma sense reflector és menys segura que l'original davant un atac d'aquestes característiques.
Una vegada extretes aquestes conclusions s'ha pogut determinar una possible millora de la màquina Enigma sense reflector, per evitar l'atac de "cribs" d'Alan Turing, afegint-li més rotors, per així fer-la una màquina viable per la seva fabricació actual.

Així i tot, aquest treball podria ser potencialment millorat, ja sigui, per exemple, desenvolupant un codi que pogués desxifrar un missatge d'Enigma mitjançant el mètode de les cribs de manera autònoma o un que ho pogués fer a través de la força bruta parcial sense haver-li de donar el missatge en clar, és a dir, que seleccionés el missatge més coherent per ell mateix.

Malgrat això, pel temps que s'ha tingut disponible per realitzar aquest projecte, penso que els resultats han estat satisfactoris. A més, personalment, m'ha agradat fer un treball sobre una disciplina científica tan desconeguda, i poder, en part, imitar el procés que van patir el grup de brillants científics de l'equip d'Alan Turing davant la tasca de desxifrar els secrets d'Enigma.

6. Bibliografia i bibliografia web

1. ARANA HERNÁNDEZ, Adrián. *Criptoanálisis de las máquinas ENIGMA*. Treball de Fi de Grau a l'Universitat Politècnica de Madrid.
<https://oa.upm.es/75491/1/TFG_ADRIAN_ARANA_HERNANDEZ_2.pdf>

2. BATTISTA BELLASO, Giovan (1553). *La cifra ("The Cypher").* Venècia.

3. CARRIÓN LOSTAL, Óscar (2021). *Criptografia para principiantes: Método de Playfair (Wheatstone)*.
<https://sapm.es/EntornoAbierto/EntornoAbierto-num40/EA40_027-030.pdf>

4. CORCOLES BRIONGOS, Cèsar Pablo (2013). *Bletchley Park (I): las máquinas Enigma y la bombe*. Universitat Oberta de Catalunya. [Data de consulta: 16/06/2024]
<https://blogs.uoc.edu/informatica/es/bletchley-park-i-las-maquinas-enigma-y-la-bombe/>

5. DELGADO MÉNDEZ, Carlos Eduardo (n.d). *Criptografia: "El arte de ocultar y proteger*. [Data de consulta: 31/03/2024]
<https://criptografia20162.wordpress.com>

6. EL HAYANI, Abdelilah, GALÀN, Pablo, GARCÍA, Héctor i PINZÓN, Mateo (n.d). *Criptografia desde su origen hasta la actualidad.* Cartagena: I.E.S Mediterráneo Cartagena. [Data de consulta: 10/03/2024]
<https://www.upct.es/gestionserv/inter/espacios_usuarios/web_servsimip_fich/doc_secciones/355presentacion.pdf>

7. ELLSBURY, Graham (1998). *The Turing Bombe: What it was and how it worked*. [Data de consulta: 12/12/2024]
<http://www.ellsbury.com/bombe1.htm>

8. FERNANDEZ, Tomás i TAMARO, Elena (2004). *Biografía de Al-Kindi.* Biografías y Vidas. [Data de consulta: 27/03/2024]
<https://www.biografiasyvidas.com/biografia/k/kindi.htm>

9. HERN, Alex (2014). *How did the Enigma machine work?* The Guardian. [Data de consulta: 12/06/2024]
<https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game>

10. J. PRIETO, Manuel (2020). *Historia de la criptografia.* Madrid: La Esfera de los Libros.

11. J. SIMMONS, Gustavus (n.d). <<Cryptology>>. Encyclopedia Britannica. [Data de consulta: 18/02/2024]
<https://www.britannica.com/topic/cryptology>

12. KERCKHOFFS, Auguste (1883). *La cryptographie militair*. *Journal des sciences militaires, vol. IX, pp. 5–38.* [Data de consulta: 08/12/2024]
<https://www.petitcolas.net/kerckhoffs/index.html>

13. MARKUSON, Daniel (2023). *The Enigma machine: How cryptography and social engineering helped win WWII*. NordVPN. [Data de consulta: 12/06/2024]
<https://nordvpn.com/es/blog/cracking-the-enigma/>

14. MILLER, A. Ray (2019). *The Cryptographic Mathematics of Enigma.*
<https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/CryptoMathEnigma_Miller.pdf>

15. MOORE, Karleigh, W, Ethan, DEAN, Ejun i WILLIAMS, Cristopher (n.d). *Enigma Machine*. Brilliant. [Data de consulta: 16/06/2024]
<https://brilliant.org/wiki/enigma-machine/>

16. PASCUAL ESTAPÉ, Juan Antonio (2021). *La historia del Código Morse y cómo ha conseguido sobrevivir a la era digital*. ComputerHoy. [Data de consulta: 10/06/2024]
<https://computerhoy.com/reportajes/life/historia-codigo-morse-787075>

17. PARRA, Sergio (2023). *Código Morse: ¿qué es, cómo funciona y qué tiene que ver con el Titanic?* National Geographic. [Data de consulta: 10/06/2024].
<https://www.nationalgeographic.com.es/ciencia/codigo-morse-que-es-como-funciona-que-tiene-que-ver-titanic_19830>

18. RODRÍGUEZ SANTOS, Alberto (n.d). *Criptografia: Métodos Clásicos.* Epsilones. [Data de consulta: 10/03/2024] <https://www.epsilones.com/paginas/historias/historias-015-criptografia-metodosclasicos.html>

19. SATHE, Mihir (2023). *Cracking the Enigma Code Today.* Medium. [Data de consulta: 13/10/2024] <https://medium.com/@mihsathe/cracking-the-enigma-code-today-35c8a97f5e26>

20. SIDHPURWALA, Huzaifa (2023). *Una breve historia de la criptografía.* RedHat. [Data de consulta: 10/03/2024] <https://www.redhat.com/es/blog/brief-history-cryptography>

21. SIMPSON, Ralph (n.d). *Cryptology, the Secret Battlefield of World War I: Dawn of the Crypto Arms Race*. <https://www.worldwar1centennial.org/images/California/pdf/ww1cryptology_paper.pdf>

22. TRITHEMIUS, Johannes (1518). *Polygraphia*. Roma.

23. AA.VV (2024). <<Cryptography>>. Encyclopedia Britannica. [Data de consulta: 18/02/2024] <https://www.britannica.com/topic/cryptography>

24. AA.VV (n.d). <<Data encryption>>. Encyclopedia Britannica. [Data de consulta: 18/02/2024] <https://www.britannica.com/technology/data-encryption>

25. AA.VV (n.d). <<Code>>. Encyclopedia Britannica. [Data de consulta: 18/02/2024] <https://www.britannica.com/technology/data-encryption>

26. Autor desconegut (n.d). *Cifrados contra códigos.* Khan Academy. [Data de consulta: 10/03/2024] <https://es.khanacademy.org/computing/computer-science/cryptography/ciphers/a/ciphers-vs-codes>

27. Autor desconegut (n.d). *Cifrado y privacidad: cifrado en el RGPD.* Agència Espanyola de Protecció de Dades (2019). [Data de consulta: 18/03/2024] <https://www.aepd.es/prensa-y-comunicacion/blog/cifrado-y-privacidad-cifrado-en-el-rgpd>

28. Autor desconegut (n.d). *El mundo del Libro y la criptografía.* TodoLibroAntiguo. [Data de consulta: 18/03/2024] <https://www.todolibroantiguo.es/criptografia-libros-antiguos/index.html>

29. Autor desconegut (n.d). *Al-Kindi, the father of cryptanalysis.* Telsy (2024). [Data de consulta: 27/03/2024] <https://www.telsy.com/en/al-kindi-the-father-of-cryptanalysis/>

30. Autor desconegut (n.d). *Cifrados polialfabéticos*. Criptohistoria. [Data de consulta: 31/03/2024] <https://www.criptohistoria.es/polialfabeticos.html>

31. Autor desconegut (n.d). <<Johannes Trithemius>>. Gran Enciclopèdia Catalana. [Data de consulta: 31/03/2024] <https://www.enciclopedia.cat/gran-enciclopedia-catalana/johannes-trithemius>

32. Autor desconegut (2023). *What does the Kerckhoffs's principle state?* European Information Technologies Certification Academy. [Data de consulta: 10/06/2024] <https://eitca.org/cybersecurity/eitc-is-ccf-classical-cryptography-fundamentals/history-of-cryptography/modular-arithmetic-and-historical-ciphers/the-kerckhoffss-principle-states-that-cryptosystems-should-be-secure-even-when-only-the-decryption-key-is-kept-secret/>

33. Autor desconegut (2021). *The Zimmerman Telegram*. U.S. National Archives and Records Administration. [Data de consulta: 11/06/2024] <https://www.archives.gov/education/lessons/zimmermann>

34. Autor desconegut (n.d). *Vernam cipher*. ADA Computer Science. [Data de consulta: 11/06/2024] <https://adacomputerscience.org/concepts/encrypt_vernam?examBoard=all&stage=all>

35. Autor desconegut (n.d). *Criptografia de clave pública*. IBM. [Data de consulta: 16/06/2024]
<https://www.ibm.com/docs/es/cics-ts/5.6?topic=protection-public-key-encryption>

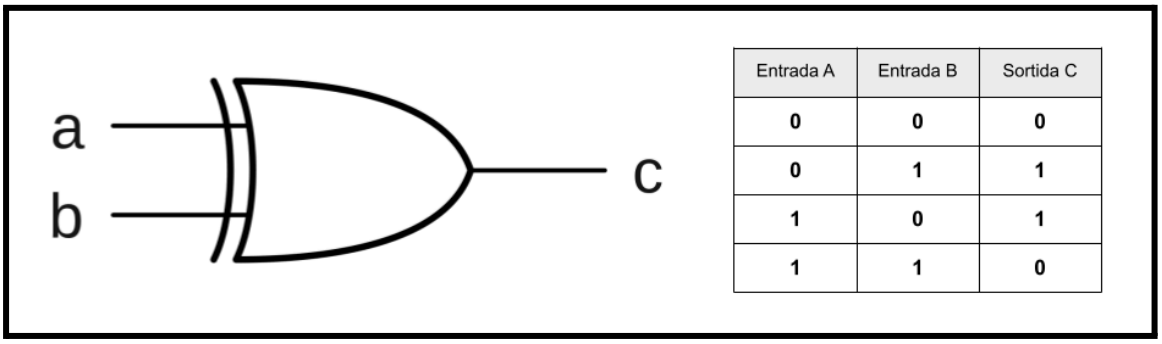
36. Autor desconegut (2021). *Cryptography During World War I.* Probabilistic World. [Data de consulta: 04/04/2024]
<https://www.probabilisticworld.com/cryptography-during-world-war-i/>

37. Autor desconegut (2009). *Enigma M3*. CryptoMuseum. [Data de consulta: 12/12/2024]
<https://www.cryptomuseum.com/crypto/enigma/m3/index.htm>

38. Autor desconegut (2019). *Enigma Crib Analysis*. 101computing.net. [Data de consulta: 12/12/2024]
<https://www.101computing.net/enigma-crib-analysis/>

7. Annex 1: Codi binari

Figura 1: Porta lògica XOR i les seves equivalències



Entrada A	Entrada B	Sortida C
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**0**

Figura 2: Taula de Baudot (equivalències entre caràcters i el seu codi binari)

Nombre	Grup de bits	Grup de lletres
01	00011	A
02	11001	B
03	01110	C
04	01001	D
05	00001	E
06	01101	F
07	11010	G
08	10100	H
09	00110	I
10	01011	J
11	01111	K
12	10010	L
13	11100	M
14	01100	N
15	11000	O
16	10110	P
17	10111	Q
18	01010	R
19	00101	S
20	10000	T
21	00111	U
22	11110	V
23	10011	W
24	11101	X
25	10101	Y
26	10001	Z
27	01000	1
28	00010	2
29	11111	3
30	11011	4
31	00100	5
32	00000	6

8. Annex 2: Codi del simulador d'Enigma en Python

En aquest enllaç es troben ambdós codis simuladors d'Enigma desenvolupats durant el treball: L'Enigma original i l'Enigma sense reflector.

https://drive.google.com/drive/folders/1oCjYxcGH5lZIsuyZaBQRw8Nwh_QOhp_i?usp=sharing

9. Annex 3: Missatges xifrats per la criptoanàlisi

En tots els casos la configuració del wiring i de les posicions del Rotor 3 són les predeterminades de l'Enigma M3, i les dues llistes del panell endollable han d'estar buides:

Rotor 3eq = [2, 4, 6, 8, 10, 12, 3, 16, 18, 20, 24, 22, 26, 14, 25, 5, 9, 23, 7, 1, 11, 13, 21, 19, 17, 15]
Alfabet 3 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
Steckerbrett = [] (buida)
Steckerbrett2 = [] (buida)

En els casos on hi hagi reflector, aquest tindrà també la configuració predeterminada de l'Enigma M3:

Reflector = [25, 18, 21, 8, 17, 19, 12, 4, 16, 24, 14, 7, 15, 11, 13, 9, 5, 2, 6, 26, 3, 23, 22, 10, 1, 20]

Les configuracions predeterminades de les posicions inicials i el wiring dels Rotors 1 i 2 són:

Alfabet 1 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
Alfabet 2 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]
Rotor 1eq = [5, 11, 13, 6, 12, 7, 4, 17, 22, 26, 14, 20, 15, 23, 25, 8, 24, 21, 19, 16, 1, 9, 2, 18, 3, 10]
Rotor 2eq = [1, 10, 4, 11, 19, 9, 18, 21, 24, 2, 12, 8, 23, 20, 13, 3, 17, 7, 26, 14, 16, 25, 6, 22, 15, 5]

- **Text 1**

- Equivalències del wiring dels dos primers rotors:

Rotor 1eq = [15, 23, 25, 8, 24, 21, 19, 16, 1, 9, 2, 18, 3, 10, 5, 11, 13, 6, 12, 7, 4, 17, 22, 26, 14, 20]
Rotor 2eq = [16, 25, 6, 22, 15, 5, 1, 10, 4, 11, 19, 9, 18, 21, 24, 2, 12, 8, 23, 20, 13, 3, 17, 7, 26, 14]

Alfabet 1 = Configuració predeterminada

Alfabet 2 = Configuració predeterminada

- Posicions dels dos primers rotors:

Alfabet 1 = [7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 1, 2, 3, 4, 5, 6]

Alfabet 2 = [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 1, 2, 3, 4, 5, 6, 7, 8, 9]

Rotor 1eq = Configuració predeterminada

Rotor 2eq = Configuració predeterminada

Màquina Enigma amb reflector

Missatge amb el wiring canviat de la configuració predeterminada
“JXFFYPUYZYRUTDJRUNRGAVQQTWXDSUSUFGUXDPEGZWIBUSDRRKJEIZCAPXLBDEWBJCDPBYJOCHPVIVQAIWDCCBGXPFJRVGTDJBFZALUMXPQBUOBLRZCNZOMGCLIPORVHCDJMPDFQUCWCGIAIQBVRDNZBRGBOEWCRRKHVCAJVRFAPCNZJXVLOANNBJOBJXNPUPWAPBIVHYZVYEUCBWNRTFZNQXXDWICJWEKTDRDQ”

Missatge amb les posicions canviades de la configuració predeterminada
“OBGDWXPODSORTWMVTCBKFMZUHDTHXWLKCUWDETVKOATHZMLWCQNHCEAEQBLWQGPUSSQBYLOBEBPGMLFKEJOCDXGCKHSPKZMCMVUHVYVZGUWNNRCAYHQJBXQGLSBSIOCPFGCWYIJXJEFXOSIKTNMVYDXRRLIMXLOSORBAUARHNXTFCPIUXVFJKIJJZOIGGNUYXRUHTLQEVTZBCHABHKLMHNVPUYCHNQTIKJHELCY”

Màquina Enigma sense reflector

Missatge amb el wiring canviat de la configuració predeterminada
“QIUAGLHLIWNRXIMKFNZHQVYBYQYLCVHZQGTMWILJJYTZNPJMBTYWBAVRKYEDRAEWPKFEDDRIUNRGPPUJXVCDWLWRFKGIERYWJXGFNBONLKKIHUGWJWWOEBOJBBNMJJMYDHGISQYBBEQXVUYHLBDYPKGAWXVQFDTOYJEXGTMAUMKQKCEGSYUVIYUOQXGVSPVGUFMWBBPVXXMLGESZUKQRZIZHJHBIFUUXUQVSIYM”

Missatge amb les posicions canviades de la configuració predeterminada
“VTIBOXDJOCPJSXYTCRYTBGNLNPGQOAZTZNQJCLRVFYABKFIATNCWQJD BYUZYNPVBVCBQIMDOOKRMNXLQMPBJETTFDAXRNRZMFFXVQDOVKUGH FITFPJUCINLIVVRUBSEYEZPARBKDQLJLYDVILJOTJKKXJJVOJFVKSMOBRLJ LVQNIVVBUJVDKONZBWYBGDOILRESHMHANRWRBCDQQPCBJNNRNOGGY IFVCLOVPPTV”

- **<u>Text 2</u>**

- <u>Equivalències del wiring dels dos primers rotors:</u>

Rotor 1eq = [12, 7, 4, 17, 22, 26, 14, 20, 15, 23, 25, 8, 24, 21, 19, 16, 1, 9, 2, 18, 3, 10, 5, 11, 13, 6]

Rotor 2eq = [3, 17, 7, 26, 14, 16, 25, 6, 22, 15, 5, 1, 10, 4, 11, 19, 9, 18, 21, 24, 2, 12, 8, 23, 20, 13]

Alfabet 1 = Configuració predeterminada

Alfabet 2 = Configuració predeterminada

- <u>Posicions dels dos primers rotors:</u>

Alfabet 1 = [22, 23, 24, 25, 26, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21]

Alfabet 2 = [12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]

Rotor 1eq = Configuració predeterminada

Rotor 2eq = Configuració predeterminada

<u>Màquina Enigma amb reflector</u>

Missatge amb el wiring canviat de la configuració predeterminada
“WHOGOFONRWBAWRADNDHSLXMWEOACHZQGZMTSJQALMWFOGCPLOP UDDJSPYSHXVDMCJGEXWWZQCSKMFAFQOPONYEEVWUCHVSLZMPXZM WEBZUTQQTVDHTTCFNWXMZOZBRTZMJPMFRLLMMKLSGGDUAFGHNYXV SBBLMJDRKMHWIIMNTBZVDJWIXFDUXSGLVJOENKJIJRPXEZGCLHFROIRZ VDGHJFWHIXNTCMDHYLQPADWLYOCZRFSCBGZWFHKRPWNUKISMWFDG YITGTYPNVPRJESARFTYCIZTJTMUOVHUUEAACCOTLXDGMKTPWPFDXJUM XIUBU”

Missatge amb les posicions canviades de la configuració predeterminada
“YZBSPFKPKRRQTHBWVEAYBVHFLCPZXVDMEFMIZQPDBVQVMOVEJLMKK UPGDGIVVWPIHTNSYJZSSIBSCLXLBNZUSSQPDYPYEXEQTPOUQZFUDMLY SGIJMBVYAGOOYUCOGTDWJFRSLSRLWDYUJDILJWHLFXOMKWGBFSDAIT UJIGMFJYTDPWZCGPJKEODPTDDPVSASIDFWTRBETRKQWXRFZZFEQYFT WDBKHOCBHCRFGYIESRLJHPVUBVLYSQAVNUXYINCYOBNEDSFXNICEBYE VHDILGDIAXKXMOBHBZLCBSGTSBTAVGKQWTUGXZJPUKXVWWVZUJ”

Màquina Enigma sense reflector

Missatge amb el wiring canviat de la configuració predeterminada
“AHQHZPUPUMZRARSPAYCTCUHAYCFRUSAYXJJRYYNYYNPNBIKJIVMLGDY PHYHOBIAYOUWCOCFSVZZCZIQDLGQIBVIVFJTPUKXMZUZDFVLZJUXGVFA FLZJZTSSVVQTXOEFHNUVQAGCDLBNVGRKBILGVRSTYXEWBTDVUSVCPD OBKFLJSLNOLSSLUGOAXHMPRJMUCLEUBUXAWPQFHNOWFHFHWEAPKX XUIRLXZRCYUXCVUNIVDGFDKLVKICHLAAJYVKKJGXEGRHWEMTXHTJSDEZ FEULQBANHAZNJPKRSQRHNUWYFPRVBMTCISMTQQOMEHQJYBPH”

Missatge amb les posicions canviades de la configuració predeterminada
“BBBLQAAHCFUFKYBMEPVUJUDIDKVRBOYKKDCRWGCJRQXNSJAQUJCSV XLDBQIGAKKWSAGZRTUQKIGUMOKQSREDFXZUJKUZZEWPTOBSAGDZYQ TVDVZDAIJSIDCTTPVRVHFLPDOCUMPJCHFRVUUUICPOMNKDWGZJGXNZT CCBPOEIFNEDAGPBCTGTGHLDHASVMFSVJNMPGUFQEYCIIGLZOAIHOXNB JMOWDLXRRUMIITXDWMFBVRSKDQBRMEXRQQYLKUUXUJOJNWQVHQQV XJUXHVPDVIUKDSTGDOCTPTMOWITWTCPMHAFWZEBVEJFQJMFQIEHEA”

10. Annex 4: Codis de criptoanàlisi d'Enigma

En aquest enllaç es troben els quatre codis per la criptoanàlisi d'Enigma desenvolupats durant el treball, separats en dues carpetes: Sense Reflector i Amb Reflector:

https://drive.google.com/drive/folders/1l4QKQnnaXIDGeEjW660DObRertyoSKQ3?usp=sharing