Codis secrets:

Enigma

Fet Per: Josep Adrià Mallafré De Juan,

Iago Mourelo Uroz i Sergi Sànchez Perea.

Tutora: Laura Antón

4t A

28/3/2022

Índex

Introducció:

L'objectiu principal d'aquest projecte és determinar la importància dels codis secrets en els grans esdeveniments històrics. A més de concloure des d'un punt de vista analític i matemàtic, la composició dels codis secrets.

L'estudi de la temàtica és realitzarà mitjançant l'anàlisi de la codificació dels textos de la Segona Guerra Mundial. Per tal de determinar les conclusions dels projecte, estudiarem exemples de textos d'Enigma. Amb aquests mètodes de codificació, s'intentarà cerca patrons en la formació d'aquests codis secrets.

Finalment, a partir del exemples cercats es crearà una codificació del nostre alfabet, per tal de posar en pràctica tots els conceptes extrets d'aquests exemples i donar un sentit pràctic a la recerca.

S'ha escollit aquesta temàtica perquè s'ha cregut que pot arribar a ser molt profitosa i interessant. A més, amb la xerrada d'Enigma, la màquina de codificació que utilitzava Alemanya a la Segona Guerra Mundial, ja ens vam interessar en la seva història. Aquest tema és l'oportunitat perfecta per descobrir més d'Enigma i de més codis secrets al llarg de la història.

Concreció del Tema:

Objectiu: L'objectiu de la recerca consisteix en comprendre el funcionament de la màquina de xifrat Enigma, en un context històric tant assenyalat com és la Segona Guerra Mundial. Fent així un anàlisi del xifrat que permeti saber com les codificacions es duien a terme. Per últim, a partir dels coneixements adquirits es busca realitzar un programa de codificació propi, on s'encriptin textos simulant Enigma.

Imatge 1:Home Amb Dubtes. Extret de: https://us.123rf.com/450wm/asfia/asfia1601/asfia160100610/51197737-3d-illustration-of-doubtful-man-standing-between-question-marks-3d-human-person-character-and-white-.jpg

Metodologia de Treball:

La metodologia de treball per obtenir els resultats de la recerca es basarà en documentació bibliogràfica i de pàgines web, per així obtenir informació suficient per desenvolupar la temàtica a nivell històric. A més, es consultaran estudis previs per tal de poder desxifrar el textos codificats.

També s'empraran eines digitals i programes informàtics com python per dissenyar les aplicacions pràctiques del treball. Per desenvolupar el programa es cercarà informació a xarxes web de programació, a videos on s'expliqui el procés de creació i de funcionament d'Enigma i localitats web on s'enenyi com utilitzar aquestes eines digital per la creació de la part pràctica.

Imatge 2: Treball. Extret de: https://canopylab.com/wp-content/uploads/2021/06/18771.jpg

Desenvolupament de la recerca:

El projecte consta de tres apartats, dividits segons la perspectiva desde que es fa la recerca. El primer apartat que conté un rerefons històric, el segon apartat basada en la recerca analítica dels textos Enigma i una última que busca recrear a partir de l'aplicació Python, un sistema algoritmic semblant a Enigma.

Com ja s'ha citat als objectius del treball, es considera molt important l'entendre en quin moment històric es va desenvolupar aquest tòpic. Aquesta informació permetrà valorar amb major rigor i perspectiva el que va significar Enigma, i com va revolucionar la tecnologia moderna.

1. Recerca Històrica.

1.1 Context històric:

La Segona Guerra mundial va ser un conflicte bèl·lic en el que es van implicar la gran majoria de països del món. La causa coyuntural del conflicte es va donar l'any 1939 amb la invasió de Polònia per part de l'Alemanya Nazi. Tot i que aquesta va ser la causa que va provocar que la guerra es desencadenés, ja existien causes estructurals que feien previsible el desenvolupament del conflicte.

A partir de l'any 1939, el món es va dividir entre els defensors de l'eix: Alemanya, Itàlia, Japó, Romania, Hongria, Bulgària, Finlàndia i Àustria, entre d'altres; i els aliats al eix: Gran Bretanya, Estats Units, França, Xina, Polònia, Bèlgica i Holanda, entre d'altres.

Des de l'inici de la Guerra fins l'any 1941, Alemanya pretenia crear un gran imperi. A partir d'una sèrie de tractats militars i campanyes bel·licistes, van aconseguir fer-se amb el domini de gran part de l'Europa continental. Aquestes avenços territorials per part de l'eix van ser frenats després de que es produïssin diverses derrotes navals per part de l'exèrcit japonès. A més, les derrotes de les tropes europees al nord de l'Àfrica, i la derrota a la batalla de Stalingrado van acabar de frustrar la conquesta.

L'any 1943 va seguir amb aquesta tendència, ja que els fronts de l'eix van debilitar-se i es van veure obligats a retirar-se de la major part dels conflictes, per així reduir el desgast i militar. És a dir, l'eix estava perdent força, cosa que els aliats aprofitarien. França va ser reconquerida per els aliats occidentals i els soviètics van seguir recuperant els territoris perduts.

Finalment, el 8 de maig de 1945 les tropes polaques i soviètiques van fer-se amb el control de Berlín. Després de perdre el control del centre neuràlgic de l'eix, les tropes dels Estats Units van passar a l'ofensiva envaint el Japó. Aquesta invasió de l'altre gran intgrant del eix va derivar en la Guerra d'Àsia, on va haver un bombardeig de Hiroshima i Nagasaki .

Finalment, el conflicte bèl·lic va finalitzar amb victòria dels aliats, tot i que la Guerra Freda entre els Estats Units i la Unió Soviètica va perdurar durant 45 anys. Per últim, com a símbol de reconstrucció i pau es va crear la Organització de les Nacions Unides (ONU), que va constituir una organització de cooperació internacional antibel·licista.

En aquest cas, l'explicació del context històric i del conflicte no té en compte els conflictes socials i les pèrdues humanes, sinó que es basa en els militar. Això es deu a que Enigma va ser clau principalment en les actuacions bel·licistes i estratègiques.

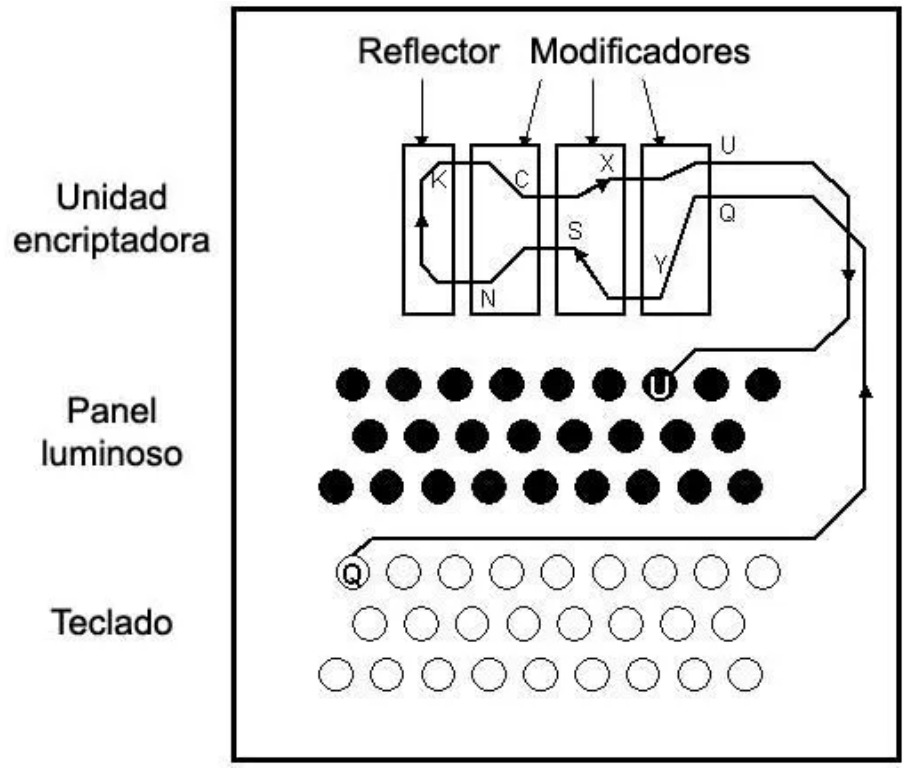
Imatge 3: Il·lustració Segona Guerra Mundial. Extret de:https://www.google.com/url?sa=i&url=http%3A%2F%2Fwww.020mag.com%2Fnoticias%2F10417%2F-cual-es-tu-replica-de-la-2gm-favorita-&psig=AOvVaw3OOpLpts7bQHte3Om-2FMc&ust=1648023589565000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCNDcwbyk2fYCFQAAAAAdAAAAABAD

1.2 Què és Enigma?

Enigma es la màquina de xifrat que va ser utilitzada a la segona guerra mundial, per part dels alemanys. El creador d'aquesta màquina va ser Arthur Scherbius, un enginyer alemany.

L'objectiu d'Enigma era poder enviar missatges a soldats alemanys, és a dir, poder establir comunicacions amb l'exèrcit sense ser descoberts.

La màquina estava formada per cinc rotors diferents, cada instant en el que una tecla era premuda, amb l'ajuda dels rotors, canviava a una lletra diferent, creant moltes possibilitats per lletra. El missatge de la lletra premuda "viatjava" per la màquina fins passar per tots els rotors, canviant en cada un d'ells, la lletra final.



Imatge 4:Funcionament d'Enigma. Extret de: https://i0.wp.com/www.portierramaryaire.com/imagenes/enigma_esq.jpg

1.3 Com va afectar Enigma a la Segona Guerra Mundial?

Tot i que Enigma va ser creada l'any 1918, no va començar a ser utilitzada per l'exèrcit d'alemanys fins 1926. En essència, era utilitzada per encriptar missatges militars, tot i que també va ser utilitzada pels serveis diplomàtics i per el Reichsbahn, el departament de la xarxa de ferrocarrils alemany.

Els anglesos, que eran plenament conscients de l'existència d'Enigma, van conformar un grup d'experts que trobes la clau de xifrat. Tenien una gran avantatge, ja que anys abans els serveis d'intel·ligència polacs havien descobert la seva codificació. Ho van aconseguir a partir de trobar grups de lletres iguals en tots els textos del dia.

Una vegada obtenien aquesta informació ja podien, a partir d'un algoritme, obtenir la clau del dia. El alemanys al adonar-se de la situació van augmentar la seguretat del xifrat. En comptes d'utilitzar grups de tres lletres, s'utilitzaven grups de cinc. Llavors, el polacs van crear màquines que simulaven el funcionament d'Enigma, però novament els alemanys van incrementar l'encriptació del textos. Això va provocar que per als polacs no poguessin simular Enigma, i que es posessin en contacte amb el anglesos perquè ells intentessin solucionar-ho.

Els anglesos que tenien més recursos, i que comptaven amb l'estudi previ dels polacs, van contractar un grup de criptògrafs experts en xifrats de textos. Entre ells es trobaven Alan Turing i Joan Clarke, que van ser els principals investigadors dins del projecte. Ràpidament es van adonar de que tots els textos acabaven amb ''Hi Hitler'', fet que van aprofitar per descartar un gran nombre de combinacions. Finalment, a partir de la creació d'una màquina ''Colossus'', van poder aconseguir desxifrar les combinacions poques hores després i fer-se amb el control de les comunicacions germàniques.

Imatge 5: Treballant en Colossus. Link.

A partir d'aquest punt, el anglesos van pendre la davantera en les estrategia militar i les seves actuacions van ser claus per derrotar l'eix. D'aquesta manera els anglesos sabien amb antelació com els alemanys actuarien, fet que va reduir en gran quantitat el nombre de enfonsaments de tropes americanes i britàniques. Toi i així, no sempre podien utilitzar la informació, ja que sinó els alemanys sospitarien de que havien desxifrat els seus textos.

El desxiframent d'Enigma va ser clau en la victòria dels aliats de l'eix. En primer lloc, per la reducció de les víctimes del seu exèrcit, però principalment en un dels sucesos que va marcar el final de la guerra: el Desembarcament de Normandia.

El Desembarcament de Normandia va ocorrer el dia 6 de juliol de l'any 1944. El principal objectiu era confondre les tropes de Hitler, per tal que pensessin que aquest es produiria en una altra zona. D'aquesta manera les tropes podrien avançar, i envair França des de la costa francesa.

Imatge 6: Platja de Normandia. Link.

I així o van fer, després de deixar pistes falses i de comprovar les comunicacions de l'exèrcit germànic es van adonar de que la seva planificació estava sorgint efecte. Van seguir amb la seva estratègia i van fer creure als alemanys que la invasió es produiria des de Dovers fins Calais. Els anglesos i americans, que sabien que tenien via lliure van poder desembarcar totes les tropes i fer-se amb el control de tot el país, i especialment frenar el desplegament territorial de Hitler.

És per aquest motiu que es diu que la interferència del textos de Enigma va ser essencial en el desenllaç de la Segona Guerra Mundial. Sense el desxiframent de les comunicacions germàniques, el rumb de la guerra podria haver sigut totalment diferent i haver canviat la nostra història per sempre.

2. Anàlisi de la codificació d'Enigma:

A continuació, es treballarà des d'una perspectiva analítica la codificació d'Enigma. Es desenvoluparà la recerca a partir dels textos del Desembarcament de Normandia. Com a suport, es farà servir una pàgina web que simula el desenvolupament que faria una màquina Enigma al rebre o enviar un missatge. A més de la informació que coneixem respecte al funcionament d'Enigma.

2.1 Què és la criptografia?

La criptografia és la tècnica de escriure amb procediments o claus secretes o d'un mode enigmàtic, perquè així només el pugui entendre al destinatari a qui va dirigit.

El xifrat de missatges es porta practicant des de fa més de quatre mil anys, i precisament l'origen de la paraula criptografia el trobem al grec: Krypto, <<Ocult>>, i Graphos, <<Escriure>>, és a dir, escriptura oculta.

Avui dia, la criptografia s'utilitza per mantenir segur en línia material sensible, com poden ser les contrasenyes privades.

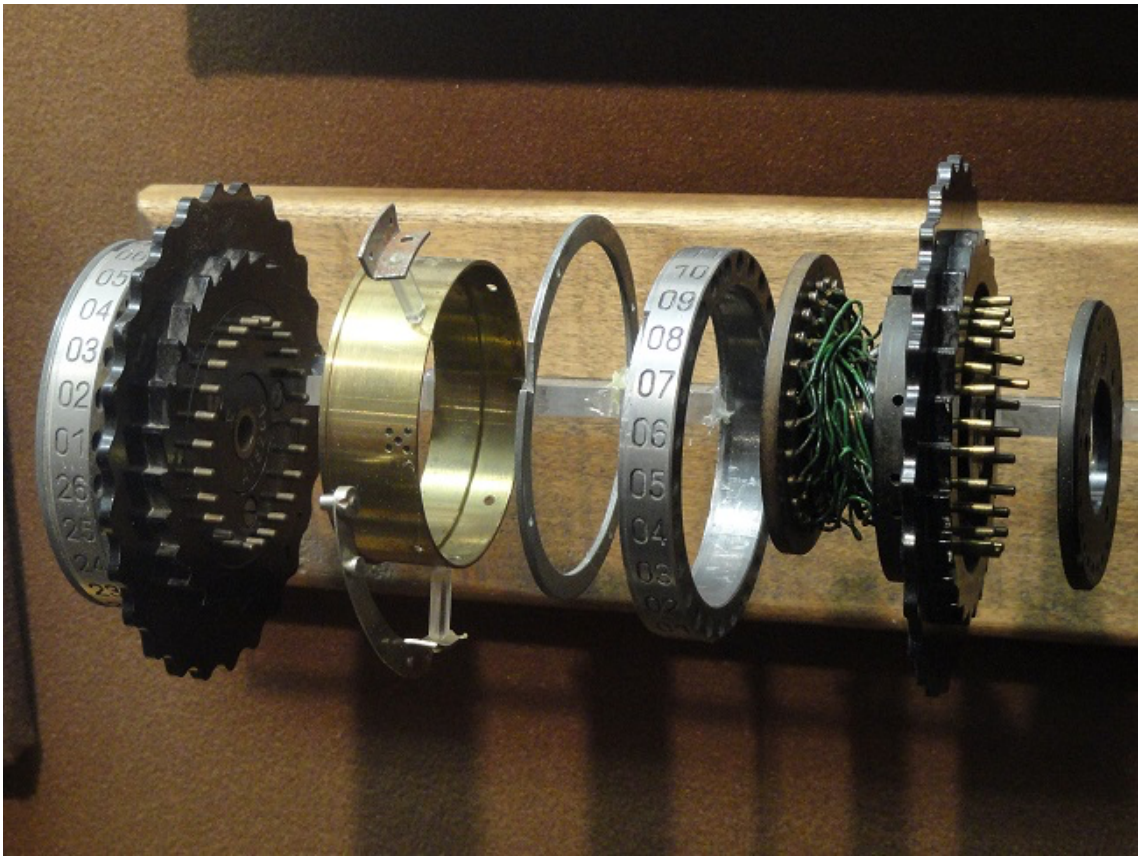
Els experts en ciber-seguretat recorren a la criptografia per dissenyar algoritmes, xifrats i altres mesures de seguretat que codifiquen i protegeixen les dades de empreses i clients.

2.2Funcionament de Enigma:

En el primer apartat, s'ha explicat breument i de manera poc explícita com era el funcionament de la màquina, per tal de poder orientar al lector. En canvi, en aquesta secció es procedirà a detallar tècnicament com Enigma duia a terme el xifrat. El fet de saber com funcionava el procés de codificació, facilitarà la traducció dels textos xifrats.

Per entendre com s'utilitza Enigma, primer s'ha de saber com funciona a nivell intern. L'aparença exterior de la màquina és molt semblant a la d'una màquina d'escriure, però està dotada d'un seguit de components que permeten encriptar el contingut.

Quan es polsa una tecla s'envia un senyal elèctric que viatge fins al rotor. Aquests rotors estan formats per un alfabet extern i un altre intern. Com s'il·lustra a la imatge següent:

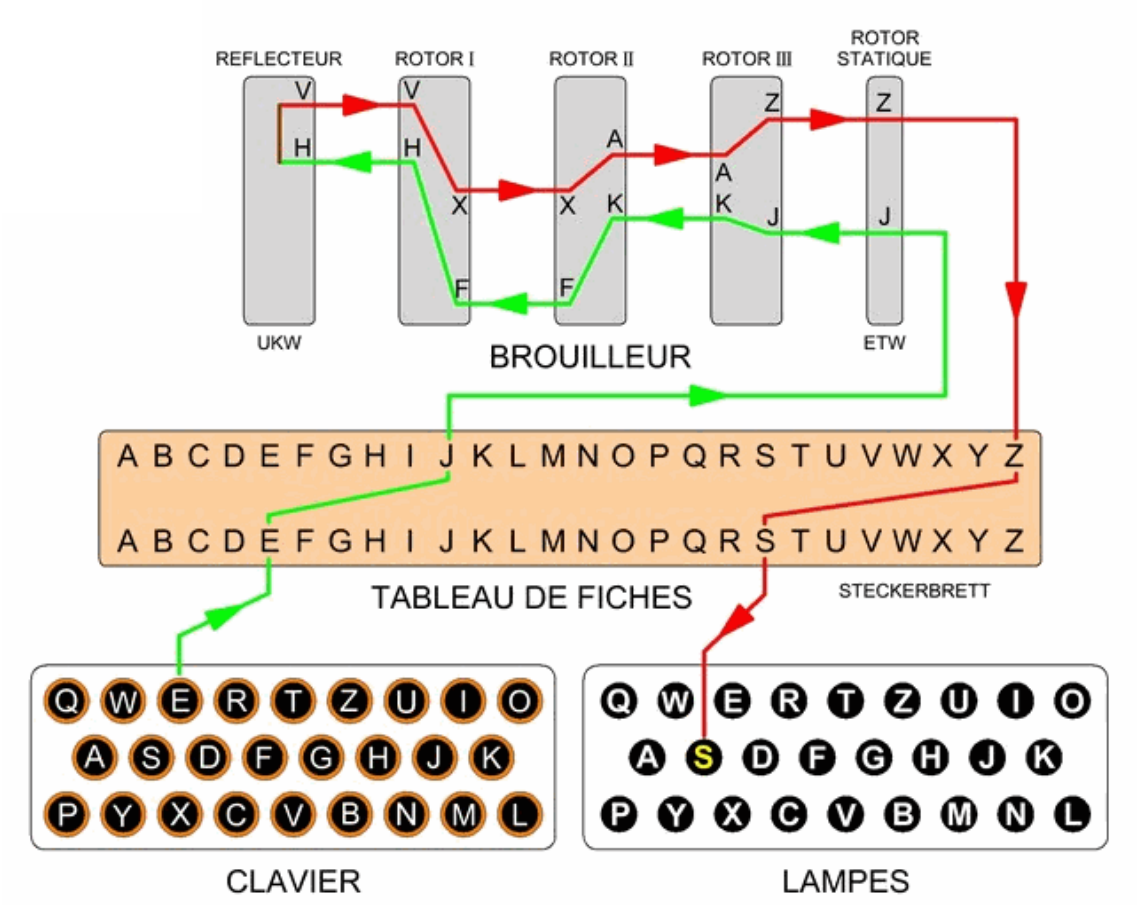


Imatge 7: rotors d'Enigma. Imatxe extreta de: https://proyectoenigma.files.wordpress.com/2015/03/enigma_wired_rotor_-_national_cryptologic_museum_-_dsc07768.jpg

L'imput arriba al rotor a través d'uns pins. Aquests pins connecten amb la primera lletra de l'alfabet del rotor extern. A partir d'un sistema de cablejat, l'impuls passa de l'alfabet extern a un altra lletra de l'alfabet intern. Aquest procés es repeteix dues vegades als dos rotors adjacents.

Finalment, aquest impuls elèctric rebota a un reflector i torna a fer el camí de tornada. Quan aquest surt del primer rotor, novament, mitjançant un sistema de cablejats arriba a un panel, on s'ilumina la lletra resultant. Si es torna a premer la mateixa lletra no es encriptada igual que l'anterior, ja que la posició dels rotors no és igual a la inicial. Per últim, no seria possible que sortis la mateixa lletra que s'introdueix, ja que perquè el circuit es tanqui ha de passar per un altre via d'aquest.

A la imatge següent s'explica quin és el recorregut de l'impuls èlectric a la màquina Enigma, des de que s'introdueix la lletra fins que surt l'encriptació.



Imatge 8: Recorregut de l'imput elèctric a través d'Enigma. Imatge extreta de: https://www.elettroamici.org/wp-content/uploads/2018/11/fig8.png

Ara que ja s'ha explicat el funcionament intern, s'introduiran quins passos d'ha de seguir per utilitzar aquesta màquina criptogràfica. Per fer servir la màquina Enigma son necessàries dues coses, evidentment un exemplar de la màquina i una fulla instructiva.

Aquesta fulla instructiva conté les directrius per poder desxifrar el missatge en concret, ja que la manera de col·locar les diferents peces és essencial per poder traduir el missatge. Tant la persona que xifra el missatge, com la que l'ha de desxifrar han de tenir les mateixes instruccions, ja que si no fos així, el contingut original no correspondria al traduït o xifrat.

Instruccions per utilitzar Enigma:

1. Agafar el full i identificar el nombres romans que hi ha.
2. Treure cuidadosament els rotors de la màquina.
3. Assignar la posició dels rotors segons posi al full.

4. Girar els rotors fins que la combinació de lletres coincideix amb la marca vermella de cada rotor. Exemple: A, L, G.
5. Tornar a introduir els rotors a la màquina.
6. Escriure el missatge desitjat.

D'aquesta manera, cada cop que prenem una tecla, el primer rotor girarà, canviant així la lletra. Quan el primer rotor hagi fet una volta sencera girarà el segon, després el tercer i finalment el quart. Això provocará que el missatge s'encripti sistemàticament quatre vegades, i que per aquelles persones que tinguin la clau de xifrat (instruccions per resoldre l'encriptació) sigui molt senzill de resoldre, però per aquells que no resulti pràcticament impossible.

Desencriptar un missatge xifrat amb una màquina Enigma és relativament senzill, sempre que es segueixin els pasos requerits. Només s'ha d'introduir les mateixes dades: l'ordre dels rotors i les quatre lletres especificades; per últim es deu escriure a la màquina el missatge encriptat. Instantaniament, es transcriurà el missatge desxifrat a un paper, com si d'una màquina d'escriure convencional es tractés.

2.3 Com es resolien els textos a l'època?

A l'apartat anterior, s'ha explicat qui va ser Alan Turing, i com va crear una màquina anomenada Colossus capaç de desencriptar enigma. És per això que en aquest es tractarà de explicar com aquesta funcionava i determinar com de innovadora va ser.

El funcionament de la màquina colossus és gairebé senzill, es tracta dels següents components:

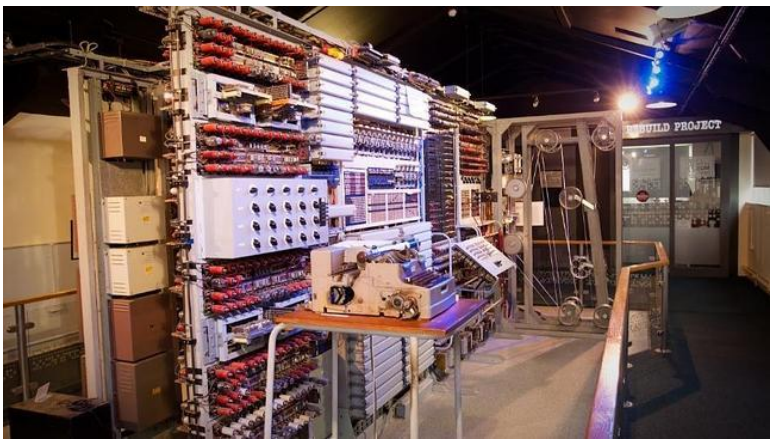
- Una cinta el més llarg possible dividida en casellas, que serà la memòria, i podrem escribir símbols, per exemple ceros i uns.
- Un altre component es un cap que es pugui moure per la cinta d'esquerra a dreta i escriure símbols en cada casella.
- Finalment un programa que li digui que es el que ha de fer, aquest programa pot estar escrit en la cinta, com ara en xifrats de ceros i uns.

Aquesta màquina simulava la funció dels rotors d'Enigma. La qüestió era provar el màxim nombre de convinacions fins trobar la posició de rototrs inicials correcte. El

principal objectiu era cercar la clau d'aquell dia el més abans possible. Per arribar a aquest propòsit es va acabar utilitzant desenes d'aquestes màquines.

Finalment ho van aconseguir. Diariament, poques hores després de l'inici de les comunicacions alemanyes, els anglesos ja havien aconseguit dexsifrar els textos de l'Eix.

Com s'ha explicat en l'apartat tres de la recerca històrica, aquest fet va marcar un punt d'inflexió en el desenllaç del conflicte.



Imatge 9: Màquina de Turing (Colossus). Link

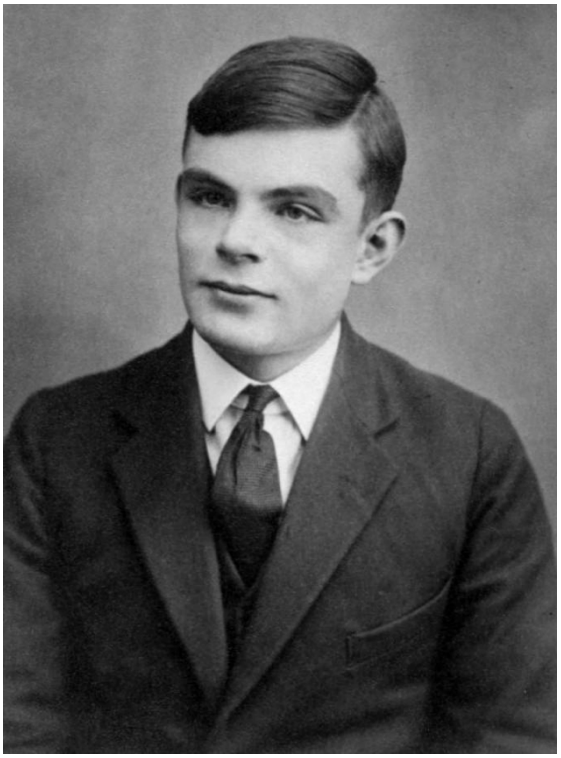
2.4 Biografia d'Alan Turing:

Alan Turing va néixer l'any 1912 a Londres i va morir l'any 1954 a Cheshire (Anglaterra), fou un molt bon matemàtic, va destacar en totes les institucions en les que va ser inscrit. Ja de petit es diu que va destacar pel seu excessiu interès en àmbits peculiars per a l'edat, amb 6 anys es passava moltes hores fent trencaclosques i jugant amb números. Amb 8 anys destacà a la seva escola degut al seu alt nivell en l'àmbit matemàtic i químic, va fer un petit laboratori químic a sa casa. Va finalitzar els seus estudis a Hazel Hurst.

A la vida de Alan va haver-hi una persona especialment important, Christopher Morcom, el millor amic de Turing, compartien els mateixos interessos per els trencaclosques i la física i química, durant classes es passaven notes amb missatges que només ells entenien. Degut a la bona relació que portaven i la confiança que tenia Morcom en ell, Christopher Morcom va convertir-se en el primer amor d'Alan Turing. Per desgràcia per a Turing Christopher va morir poc després de graduar-se. Una tuberculosis originada en la ingestió de llet de vaca infectada va acabar amb la seva vida.

Alan Turing es conegut per ser una peça clau en la resolució de la màquina Nazi Enigma, va desenvolupar una màquina capaç de batre Enigma, aquesta màquina, segons calculen els historiadors, va acurtar la guerra 3 anys, són 3 anys sense milers de morts diàries, sense més bombardeig, amb una relativa pau. La màquina es deia Colossus. Colossus va ser la introducció als ordinadors que ara tenim, Alan Turing va crear altres dues màquines següents, cada qual avançava més la tecnologia del moment.

Finalment, Alan Turing va morir per sobredosi de pastilles, les prenia per recepta del metge, ja que era homosexual i el van categoritzar com a malalt mental.



Imatge 10: Fotografia d'Alan Turing. Extret de:https://upload.wikimedia.org/wikipedia/commons/a/a1/Alan_Turing_Aged_16.jpg

2.5 Frases Xifrades amb Enigma:

Per poder exemplificar i introduir d'una manera més senzilla el funcionament d'una codificació, s'utilitzarà una pàgina que realitza aquesta funció.
Mitjançant la pàgina web: http://www.amenigma.com/ , que és un simulador d'Enigma, és a dir, xifra textos amb el codi Enigma i els desxifra oració al simulador per veure com seria rebre, mitjançant enigma, aquest missatge:

En aquest cas s'ha introduït la oració: "Hola, estem fent el treball de recerca". El resultat que hem obtingut és: "RXZRA DIOYM KJBQA JYGLS UILSN RNRTF K".
Més exemples són:

- "Atac a les dotze zero tres" "WKNOR GNLNP CAUAS WQDXS M".

Possiblement, la sensació d'algú que llegeix aquests textos és semblant a la dels soldats francesos, que rebien diàriament milers de missatges alemanys que contenien estratègies de guerra, però que contenien lletres sense sentit amb les quals no podien fer res.

2.6 Creació d'un sistema de codificació:

Tot i que en un principi l'objectiu era crear i desxifrar textos d'Enigma, no s'ha pogut relitzar. En primer lloc, la dificultat de la pràctica era molt elevada, i els medis i temps dels que es disposava eren limitats. A més, la falta d'informació a llibres i llocs web, ha dificultat encara més la tasca. És per això, que s'ha decidit crear un sistema de codificació propi.

Aquest es basa en la complementarietat entre dues lletres de l'alfabet. S'ha d'establir parelles de lletres, així quan s'escrigui una es traduirà per l'altra, i al inrevés.

Complementarietat de lletres:

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

Exemples d'encriptament de missatges:

Per explicar com funciona aquest codi d'encriptació, s'utilitzarà un seguit d'oracions. Per il·lustrar la diferència entre aquest i Enigma s'utilitzaran les oracions xifrades amb el lloc web.

Oració original	Enigma	Codi xifrat de complementarietat
Hola, estem fent el treball de recerca.	RXZRA DIOYM KJBQA JYGLS UILSN RNRTF K	SLOZ VHGVN UVMG VO GIVYZOO WV IVXVIXZ
Atac a les dotze zero tres	WKNOR GNLNP CAUAS WQDXS M	ZGZX Z OVH WLGA AVIL GIVH
Avui no hi ha notícies	KSYVB ICVFU OHBMM EPI	ZEFR ML SR SZ MLGRXRVH
Més tropes al punt C	ULEZF AURMZ GMVVK K	NVH GILKVH ZO KFMG X
Fronteres atacades	ECNSX NNYKT MSQTP NU	UILMGVIVH ZGZXZWH
Tothom a les trinxeres	LICFP JKJSB ZBKQA RSRY	GLGSLN Z OVH GIRMCVIVH

3. Simulació d'encriptació en clau Cèsar:

Per tal de donar un sentit pràctic a la nostra recerca, s'ha decidit recrear un tipus de cifrat al software de programació Python. Aquest programa permet fet tot tipus de programacions i utilitza un llengüatge propi. És per aquest motiu que no s'ha pogut programar un codi original. Llavors, he utilitzat el codi d'un tutorial de Youtube, que explicava com fer aquets tipus de xifrat.

El xifrat Cèsar és un tipus de codificació que pren el nom d'un dels seus inventors, Julio Cèsar. Aquest consisteix en canviar les lletres d'un text a partir de desplaçar l'abecedari. El nombre de vegades que desplacem el text correspon al nombre de la clau. Per exemple, si la clau de la codificació és 3, el desplaçament de les lletres es farà tres vegades. És a dir la ''A'' es convertirà en la ''D'' i la "B" en la ''E'' i així succesivament.

El codi que s'ha utilitzat en la programació és el següent:

```python
import string
alfabeto = list(string.ascii_lowercase)
def cifrado_cesar(alfabeto,n,texto):
    texto_cifrado = ""
    for letra in texto:
        if letra in alfabeto:
            indice_actual = alfabeto.index(letra)
            indice_cesar = indice_actual + n
            if indice_cesar > 25:
                indice_cesar -= 25
                texto_cifrado += alfabeto[indice_cesar]
            else:
                texto_cifrado += letra
        return texto_cifrado

frase = "bon dia, benvinguts a la nostra presentació d'enigma"
frase_cifrada = cifrado_cesar(alfabeto,3,frase)

```

Imatge 11: Codi enigma.py. Extre de: font propia

(Gonzalez Rico, Javier;, 2020)

Finalment, aquesta part del projecte no s'ha pogut executar, ja que han aparegut diverses complicacions durant la realització del mateix. Algunes falles en el codi de

programació no han permés que el programa no funciones. A més, la mancança de coneixaments respecte a aquest format, han dificultat encara més la tasca.

Com a conseqüència d'això, es dona com a acabada aquesta part del projecte, però no s'interpreta com un fracàs. El principal motiu que permet aquesta interpretació és que hem extret un seguit de coneixaments i conclusion, i per tant, es pot dir que ha sigut una experiència positiva.

Conclusions:

Després de la realització de la recerca, s'han obtingut un seguit de coneixament i aprenentatges que han permés obtenir conclusions profitoses. Aquestes es podrien dividir en dos grups: conclusions que responen als objectius plantejats, i conclusions extretes a partir dels coneixaments adquirits.

Respecte al primer grup de conclusions, destacaríem la importància d'Enigma a nivell històric. No només per com va afectar a la guerra, ni com va condicionar la història, sinó per els avenços que va generar. Es ben sabut, que sense la presència de la màquina Enigma la guerra podria haver succeit d'una manera molt diferent, ja que aquesta va ser la base de les comunicacions de l'Eix, i posteriorment va ser clau en la victòria dels aliats.

A nivell tecnològic, Enigma i Colossus van marcar un abans i un després en la manera de entendre el món. Aquestes dues creacions van ser claus en el desenvolupament de la criptografia, i especialment en la branca de l'enginyeria que anys després va canviar el món: la computació. De fet, a dia d'avui, som capaços de realitzar aquest treball des d'un ordinador gràcies a que fa anys van succeir aquests fets. Per exemple, actualment, la resolució de textos de Enigma no planteja una excesiva dificultat. De fet, existeixen llocs web en el que es resolen aquests tipus de textos, i permeten xifrar d'altres. És a dir, els avenços tecnològics i computacionals han posat a l'abast de tothom resoldre aquest tipus d'enigmes. En gran mesura, les facilitats amb les que avui comptem són el resultat del treball de generacions passades. Per exemple, Colossus va ser un dels primers ordinadors de la història, que va haver de ser creat per poder desencriptar textos de Enigma.

És per això que molt sovint conflictes que són tan devastadors com la Segona Guerra Mundial, provoquen genialitats que fan avançar tant les societats com els ordinadors. Ja que és en els moments més complicats on l'enginy humà s'aguditza, per tal de sobre posar-se a l'adversitat.

A continuació, es detallaran les conclusions extrertes a paritr dels coneixament adquirits a partir de la recerca, i dels objectius plantejats. Tot el que s'ha aprés durant el treball ha fet que ens plantegem paral·lelismes entre aquell moment històric i l'actual. És a dir, si al passat han succeït certs fets, perquè no poden estar passant a l'actualitat. La

censura i la malversació informativa estan a l'ordre del dia, per tant, la situació que es va viure en aquell moment potser no difereix tant de l'actual.

A més se'ns suggereix la següent qüestió: Existeixen actualment codis secrets? És a dir, avui dia estem envoltats de sistemes d'encriptació que tothom veiem, però no ens adonem de la seva presència o dels seu significat real. La resposta a aquesta pregunta segurament sigui afirmativa, i per això aquesta qüestió es mereixedora de reflexió.

La nostra percepció de la realitat va directament relacionada amb els nostres coneixements. Quan més coses sabem sobre el nostre medi, més estem preparats per actuar davant d'una situació difícil. Per tant, sempre s'ha d'intentar analitzar i profunditzar al màxim en la nostra realitat, per així poder anticipar-nos a les traves del sistema.

Agraïments:

De part de tots els integrants del grup voldríem agrair a la nostra tutora del projecte, Laura Antón, ja que considerem que la seva orientació ha sigut de gran ajuda. A més, pensem que la seva visió i experiència ha sigut molt enriquidora, i s'ha vist plasmada al treball.

També ens agradaria donar les gràcies a tots aquells professors que al llarg de la setmana han posat de la seva part i ens han ofert part del seu coneixement i disponibilitat, per tal de fer més fàcil la realització del projecte.

Webgrafia:

Codis secrets:

- Khan Academy. (n.d.). *Codis.* Retrieved from https://es.khanacademy.org/computing/computer-science/cryptography/ciphers/a/shift-cipher

Segona Guerra Mundial (context):

- WordPress.com. (n.d.). *Segona Guerra Mundial(Context).* Retrieved from https://thehistorystyle.wordpress.com/2011/11/07/la-segunda-guerra-mundial-1939-1945-contexto-historico-internacional/

Enigma a la Segona Guerra Mundial

- elDiario.es. (n.d.). *Enigma.* Retrieved from https://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_1_5038272.html

Màquina enigma simulador:

- 101Computing.net. (n.d.). *SimuladorEnigma.* Retrieved from https://www.101computing.net/enigma/enigma-M3.html

Desembarcament de Normandia:

- Militari, M. (2011, junio 6). *Desembarcament Normandia.* Retrieved from http://www.manu-militari.es/2011/06/el-enigma-del-mensaje-verlaine-dia-d.html

Video Funcionament Enigma:

- Burgos, U. d. (n.d.). *Video Funcionament Enigma.* Retrieved from https://www.youtube.com/watch?v=VnsTHAH5yAE

Video Funcionament màquina de Turing (Colossus):

- Derivando (2018, gener 10). *Video Funcionament màquina de Turing (Colossus).* Retrieved from https://youtu.be/iaXLDz_UeYY

Biografia Alan Turing:

- Víctor Moreno, María E. Ramírez, Cristian de la Oliva, Estrella Moreno y otros (n.d.). *Biografía Alan Turing.* Retrieved from https://www.buscabiografias.com/biografia/verDetalle/1886/Alan%20Turing

Python:

- Python. (n.d.). *Tutorial Python.* Retrieved from https://docs.python.org/es/3/tutorial/