ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

SCUOLA DI SCIENZE

Corso di Laurea in Informatica

TECNICHE DI DECIFRAZIONE E MODELLI MATEMATICI DELLA MACCHINA ENIGMA

Relatore:
Prof. GIORGIO CASADEI

Correlatore:
Prof. ANTONIO TEOLIS

Presentata da:

LORENZO ZEFFIRO

II Sessione

Anno Accademico 2018-2019

Alla mia famiglia e tutti coloro che mi hanno supportato

Indice

Introduzione

La scelta di trattare come argometo di tesi la macchina Enigma, utilizzata dall'esercito tedesco, è scaturita dalla curiosità suscitatami dal tema affrontato nel corso di Storia dell'Informatica. In particolare mi ha incuriosito il fatto che in diversi articoli divulgativi riguardanti Turing, non si sia fatto riferimento alla macchina oggetto delle sue ricerche ed alla relativa complessità, per cui egli ha dovuto realizzare congegni e metodi che hanno condotto alla sua decifrazione. Inoltre spesso non vi è traccia degli studi effettuati dai polacchi a supporto del suo lavoro. Questo mi ha spinto ad approfondire vari aspetti della macchina Enigma per comprendere a pieno il suo funzionamento.

Nella seguente tesi verrà esaminato brevemente il contesto storico nel quale è stata utilizzata la macchina Enigma e lo scopo del suo utilizzo. In particolare, saranno affrontate le problematiche legate alla decrittazione della macchina, ricercando il più adatto modello matematico a supporto delle tecniche di decifrazione.

Il lavoro è stato aricolato nel modo seguente:

Capitolo 1: Breve descrizione del contesto storico, analisi della macchina Enigma e del suo funzionamento. In particolare viene messa in risalto la sua complessità e la sua importanza strategica durante la seconda guerra mondiale.

Capitolo 2: Istruzioni per l'utilizzo e descrizione del funzionamento e della realizzazione di un emulatore della macchina Enigma

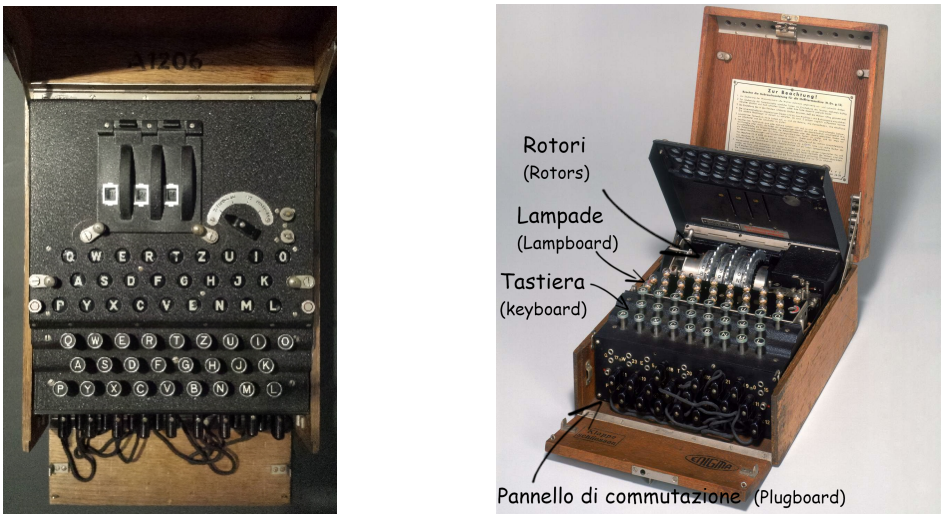
Capitolo 3: Strategie utilizzate dai polacchi e processi deduttivi che hanno portato alla decifrazione di Enigma. Proprietà e definizioni matematiche e descrizione del modello matematico realizzato dai polacchi.

Capitolo 4: Studi ed approfondimenti effettuati dagli inglesi per migliorare le tecniche di decifrazione polacche, superando alcune problematiche precedentemente non risolte. Analisi di alcune componenti della macchina di decrittazione da loro realizzata.

Capitolo 1

Crittografia con il metodo Enigma

Il termine crittografia deriva dal greco κρυπτός(nascosto) e γραφ΄ια(scrittura) e con esso si intende la capacità di scrivere messaggi segreti attraverso una tecnica che li rende "offuscati", in modo che non siano comprensibili a persone non autorizzate e permettano, esclusivamente al destinatario, di leggere e comprendere il contenuto del messaggio. La crittografia è stata usata principalmente per scopi militari e diplomatici; infatti, ha avuto un ruolo fondamentale durante la seconda guerra mondiale. Questo conflitto fu una vera e propria "guerra di codici", combattuta a distanza fra crittografi e crittanalisti con l'ausilio di macchine cifranti.
Durante la guerra si capì l'importanza della crittografia, che si sviluppò enormemente.
Il 23 Febbraio del 1918, l'ingegnere tedesco Arthur Scherbius brevettò una macchina elettro-meccanica cifrante che utilizzava rotori; così nacque la versione commerciale della macchina Enigma che era contenuta in una scatola di dimensioni 34 x 28 x 15 e pesava 12 Kg, messa in vendita a partire dal 1923.
Diverse macchine Enigma vennero acquistate dai tedeschi, che utilizzavano la versione M3, dotata di 3 rotori, per le conversazioni con l'esercito e la M4, che ne possedeva 4, per le conversazioni con la Marina. La macchina Enigma non includeva la trasmissione diretta dei messaggi, il cui invio, inizialmente, era affidato ai corrieri. Successivamente, l'utilizzo delle trasmissioni radio ha agevolato l'invio dei messaggi, ma ne ha anche permesso l'intercettazione da parte dei nemici, dato che si utilizzavano altre apparecchiature facilmente violabili, come il telegrafo, il telefono o la telescrivente. La semplicità d'uso e la presunta indecifrabilità della macchina illusero i tedeschi di poter comunicare in modo sicuro e inviolabile.
La macchina Enigma aveva l'aspetto di una macchina per scrivere ed era dotata di 5 componenti fondamentali: la tastiera (keyboard), le lampade (lampboard), il pannello di commutazione (plugboard), i rotori (rotors) e il riflettore (reflector) (*vedi* Figura 1.1).



(a) Macchina Enigma **(b)** Macchina Enigma aperta

Figura 1.1: Vista della macchina Enigma (a) e delle sue componenti (b)

Per quanto riguarda la tastiera, a differenza di quelle moderne, il tasto andava premuto con forza e tenuto schiacciato, a quel punto si accendeva la lampada della lettera codificata corrispondente. I tasti erano solo 26 e non c'erano tasti per lo spazio, le cifre e i segni di interpunzione.
Infatti, in un testo lo spazio è il carattere più importante, perché viene ripetuto più frequentemente; quindi, con opportuni algoritmi, può dare adito ad una maniera per decifrare il messaggio. Pertanto, l'assenza dello spazio era voluta, mentre l'assenza di cifre, segni di interpunzione e segni diacritici serviva per rendere la macchina più semplice e meno soggetta a rotture.
Le lampade erano 26 ed erano disposte al di sotto di una tastiera, in corrispondenza delle lettere trasparenti. Il pannello di commutazione differenziava il modello militare da quello commerciale, che ne era privo, e permetteva di associare una lettera ad un'altra, tramite un filo; in totale si avevano a disposizione 6 fili, che permettevano di scambiare le lettere a coppie (ad esempio A diventa B e B diventa A). La componente più importante della macchina è il rotore (*vedi* Figura 1.2); nelle sue prime versioni se ne avevano a disposizione 3 e successivamente 5, dei quali ne venivano scelti ed inseriti 3.
Il rotore era formato da una ruota dentata con 26 denti e 26 contatti di ottone, che avevano una piccola molla che gli permetteva di essere spinti in dentro di poco; il corpo del rotore era fatto di bachelite e i 26 pin di entrata venivano connessi in maniera opportuna (realizzando una permutazione) con i 26 pin in uscita che erano fissi e non rientranti (*vedi* Figura 1.2 (a)).

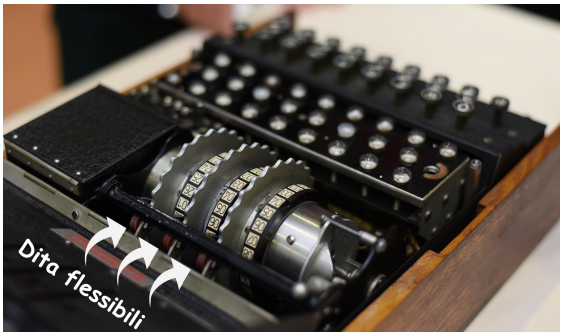
Il rotore era dotato di una tacca e di un anello sul quale erano impresse le 26 lettere maiuscole dell'alfabeto (*vedi* Figura 1.2 (b)).
Il riflettore era simile al rotore, con la differenza che non ruotava e i contatti di ingresso erano collegati a contatti presenti sul medesimo lato.

(a) struttura interna del rotore

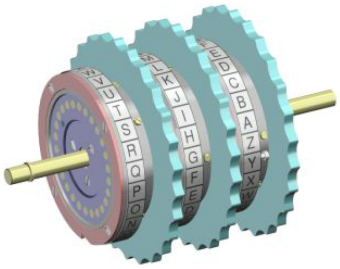
(b) vista laterale del rotore

Figura 1.2: Vista del rotore e dei 26 collegamenti tra i pin di ingresso e i pin di uscita (a) e della tacca (b)

Alzando un coperchio della macchina, era possibile inserire i rotori nell'ordine scelto.
I rotori erano sistemati sullo stesso asse (*vedi* Figura 1.3 (b)) e venivano fatti ruotare da "dita flessibili" (*vedi* Figura 1.3 (a)).
Ogni rotore aveva una tacca, che, quando incotrava il "dito flessibile", faceva ruotare il rotore alla sua sinistra.
Mentre il rotore di destra ruotava ogni volta che veniva digitata una lettera, quello centrale ruotava solo quando veniva a contatto con la tacca del rotore destro e il rotore di sinistra ruotava solo quando incontrava la tacca del rotore centrale. Al verificarsi di questo caso, ovvero che avevano compiuto una rotazione tutti e 3 i rotori, alla successiva digitazione di una lettera ruotavano sia il rotore di destra sia quello centrale.
Successivamente riprendeva la normale rotazione, ovvero ruotava solo il rotore destro fino a quando non avveniva nuovamente l'incontro con la tacca.



(a) dita flessibili

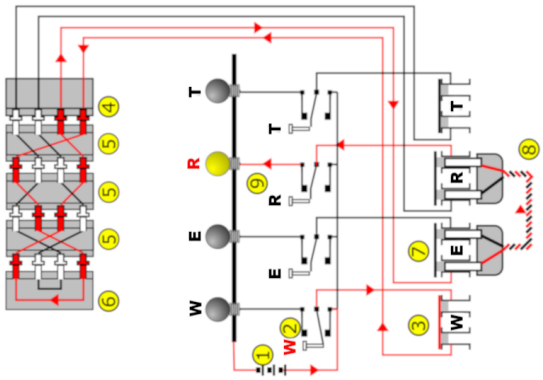


(b) asse dei rotori

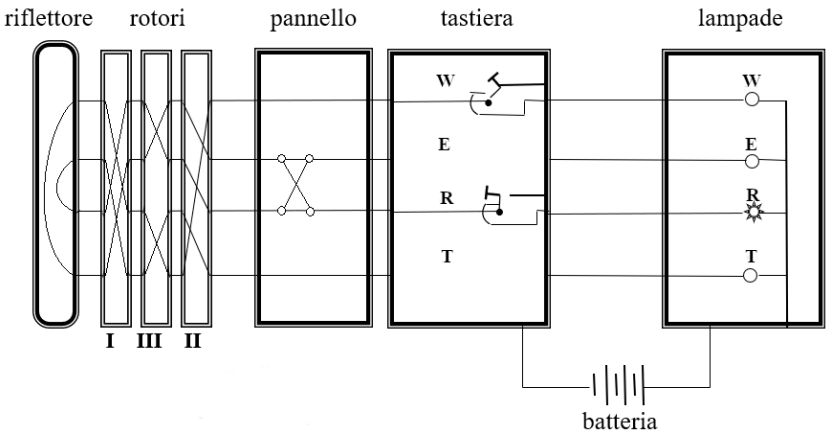
Figura 1.3: Alcune componenti di Enigma, dita flessibili (a) e rappresentazione tridimensionale dei rotori sullo stesso asse (b)

Nel momento in cui veniva premuto un tasto sulla tastiera, veniva mandato un impulso elettrico (*vedi* Figura 1.4 (b)), che arrivava ad uno dei 26 contatti di ottone (*vedi* Figura 1.2 (a)) presenti sulla superficie destra del rotore destro. Il contatto veniva leggermente spinto in dentro, permettendo all'impulso di attraversare il corrispondente pin di ingresso e di continuare il suo percorso lungo il filo che lo collegava al corrispondente pin di uscita. L'impulso, dunque, giungeva all'adiacente contatto di ottone del rotore centrale e proseguiva come già visto per il rotore di destra, attraversando con lo stesso meccanismo anche il rotore di sinistra ed arrivando al riflettore. A questo punto l'impulso veniva deviato dal riflettore, attraverso un filo che collegava il contatto di ingresso ad un altro sulla stessa superficie. Infine il segnale riattraversava i tre rotori da sinistra a destra con lo stesso meccanismo già descritto, fino ad arrivare ad uno dei 26 pin della superficie destra del rotore destro, che faceva accendere la corrispondente luce della lampada, mostrando la lettera codificata (*vedi* Figura 1.4 (a)).

(a) digitazione di un tasto



(b) percorso della corrente da W a R



(c) struttura logica di codifica da W a R

Figura 1.4: un esempio in cui viene mostrato, alla digitazione del tasto W (a), il diagramma interno del percorso della corrente (b) nel dispositivo e le fasi di codifica (c) che avvengono prima dell'accensione della lettera codificata R (a)

L'esempio, rappresentato in Figura 1.4 (c), mostra il processo di codifica che consisteva nel battere un tasto e annotare la lettera della lampadina che si accendeva. Grazie al riflettore la macchina poteva così funzionare anche come decodificatore, purché, avesse la stessa configurazione iniziale. Come si vede dalla figura se da A vado in C allora da C vado in A (involuzione).
Per codificare e decodificare i messaggi si aveva a disposizione un "modulo" composto da varie coppie di righe. Nella prima riga di ogni coppia del modulo veniva scritto dall'operatore il testo in chiaro che doveva essere codificato, mentre nella seconda riga il testo cifrato lettera per lettera e poi trasmesso dal marconista (operatore addetto alle comunicazioni radio) con i vari mezzi di comunicazione a disposizione.

Il funzionamento della macchina, quindi, consisteva nell'applicare ripetutamente sostituzioni e permutazioni di tutte le lettere del messaggio.
Al sito `http://mistic.web.cs.unibo.it/files/enigma/enigma.html` è consultabile l'emulatore della macchina Enigma, realizzato da me, con il quale è possibile provare il funzionamento della macchina.

Capitolo 2

Implementazione di un simulatore

Ho cercato di realizzare un emulatore della macchina Enigma quanto più possibile corrispondente alla macchina originale, utilizzando HTML, Javascript e CSS.

2.1 Interfaccia

Per poter utilizzare l'emulatore, prima di digitare il testo, è necessario eseguire le istruzioni poste sulla sinistra, in particolare è offerta la possibilità di scegliere 3 tra i 5 rotori, uno come rotore destro, uno come rotore centrale e uno come rotore sinistro. Direttamente nella raffigurazione della macchina è possibile selezionare le lettere iniziali dei rotori scelti, denominati rispettivamente "r_dx", "r_c", "r_sx" (in Figura 2.1). Sempre nella raffigurazione della macchina, nella parte sottostante, denominata pannello, vi sono 6 coppie di caselle denominate da una scritta (*label*), costituita da un numero romano che va da uno a sei, seguito dalla dicitura "cavo" (*vedi* Figura 2.2 (b)).

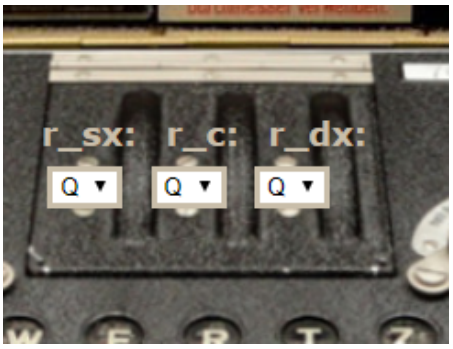


Figura 2.1: Mostra dove si possono selezionare le lettere iniziali dei rotori

Figura 2.2: Viene mostrato dove poter effetuare eventuali scambi delle lettere tramite il pannello (b)

Per ogni coppia è possibile scegliere una lettera da invertire con un'altra mediante le coppie di caselle (*select*). In caso di lettere ripetute nelle diverse coppie di *select*, viene segnalato un errore e viene chiesto di modificare le selezioni che usano le stesse lettere. Una volta terminate o modificate queste scelte è necessario confermarle tramite l'apposito bottone "Macchina Pronta", situato nelle istruzioni sulla sinistra, per poter rendere effettive tutte le scelte effettuate fin'ora.
Terminata la configurazione è possibile digitare il testo, premendo i tasti della tastiera in figura, con il mouse o con le dita in caso di dispositivi touchscreen. Nel riquadro in alto compaiono le lettere digitate, mentre nel riguadro in basso, sottostante la rappresentazione della macchina, compaiono le lettere cifrate.
Ogni qualvolta viene digitata una lettera, sulla destra compare una tabella che mostra il percorso di cifratura della lettera e la rotazione dei rotori.

2.2 Implementazione

Ho ideato ogni rotore come una matrice di 2 righe e 26 colonne, ciascuna riga indica una superfcie del rotore, mentre le colonne indicando il numero di lettere dell'alfabeto (pin di ingresso) per ogni superficie. Per quanto riguarda il riflettore anch'esso è stato realizzato come una matrice a 2 righe e 26 colonne, con la differenza che gli elementi di una qualunque colonna corrispondono agli stessi di un'altra colonna, posti in ordine inverso; si è scelta tale implementazione per emulare il fatto che i pin sono collegati tra loro sulla stessa superficie. Per ciascun vettore ho simulato la rotazione dei rotori, memorizzando in una variabile il primo valore di ogni vettore e realizzando un ciclo che ad ogni elemento del vettore (partendo dal primo) assegna il valore del successivo, fino all'ultimo elemento del vettore al quale, poi, viene assegnato il valore precedentemente salvato.
Alla digitazione di un tasto, viene controllato nell'area del pannello se compare in uno dei *select* la lettera digitata, in caso affermativo si considera quella adiacente come lettera digitata. Dunque, tramite un algoritmo viene ricercato l'indice della lettera digitata (lettera O *in* Figura 2.3), nel vettore "TASTIERA" e la lettera digitata corrisponde alla lettera (lettera A *in* Figura 2.3) avente lo stesso indice, nella prima riga del "ROTORE DESTRO". Con lo stesso algoritmo quest'ultima

lettera (A) e il suo indice vengono individuati nella seconda riga del "ROTORE DESTRO". Di conseguenza tale lettera viene fatta corrispondere alla lettera nella medesima posizione (lettera L *in* Figura 2.3) nel "ROTORE CENTRALE". Con la stessa tecnica viene ricercata la lettera nella seconda riga del "ROTORE CENTRALE" e viene ripetuto il procedimento appena descritto per la corrispondente lettera nel "ROTORE SINISTRO" (lettera K *in* Figura 2.3). Per cui l'algoritmo verrà eseguito nel percorso inverso individuando le corrispondenti lettere dal "RIFLETTORE", al "ROTORE SINISTRO", al "ROTORE CENTRALE" al "ROTORE DESTRO" e infine alla "TASTIERA", eseguendo un controllo sul pannelo per verificare se la lettera è presente; in caso affermativo si considera quella adiacente, determinando, così, la lettera criptata (lettera E *in* Figura 2.3), illuminando tale lettera nella raffigurazione delle lampboard, per circa un secondo.

Figura 2.3: Viene mostrato un esempio del percorso di codifica della lettera digitata evidenziando in arancione la simulazione dell'impulso di andata e in azzurro la simulazione dell'impulso di ritorno fino alla lettera cifrata $O \longrightarrow A \longrightarrow L \longrightarrow K \longrightarrow H \longrightarrow R \longrightarrow O \longrightarrow J \longrightarrow R \longrightarrow E$

A questo punto il rotore destro, come descritto in precedenza, "compie una rotazione" e viene selezionato nel *select* del rotore destro il valore dell' *option* successivo, cioè la lettera che occupa la prima posizione nella prima riga del "ROTORE DESTRO", a rotazione avvenuta. Tale valore viene memorizzato per effetuare dei controlli, cioè per verificare se debbano ruotare anche gli altri rotori. Infatti, se questo valore corrisponde alla variabile tacca per il rotore destro, viene fatto ruotare il rotore centrale di una posizione, poiché questo implicherebbe che nella macchina reale il rotore centrale abbia incontrato la tacca. In caso di rotazione del rotore centrale viene selezionato nel *select* del rotore centrale il valore dell' *option* successivo (cioè la lettera che occupa la prima posizione nella prima riga del "ROTORE DESTRO", a rotazione avvenuta) e viene memorizzato. Se il valore corrisponde alla variabile tacca del rotore centrale, viene fatto ruotare il terzo rotore. A questo punto viene assegnato *true* alla variabile *ruotano_tutti*, per poter far compiere una rotazione al rotore destro e al centrale alla successiva digitazione di una lettera.

Capitolo 3

Tecniche di decifrazione polacche

Dal 1930 la Polonia sapeva di essere il primo obiettivo della Germania (per via di Danzica) e, quindi, cominciò ad intercettare i messaggi scambiati tra i tedeschi. L'intelligenza dei polacchi è stata quella di conservare tutti i messaggi intercettati, anche se non capiti. Nel 1931 una spia tedesca, Hans-Thilo Schmidt, fornì ai francesi il manuale d'uso della macchina Enigma per i mesi di settembre e ottobre dell'anno successivo. Il manuale era costituito da due documenti, chiamati *Gebrauchsanweisung für die Chiffriermaschine Enigma* e *Schlüsselanleitung für die Chiffriermaschine Enigma*. Queste informazioni una volta acquisite dai francesi vennero condivise con l'Ufficio Cifra polacco (Biuro Szyfrów), che decise di interpellare gli accademici della vicina Università Poznań, sottoponendoli a un test per trovare le persone più adatte a decrittare Enigma.
Nel 1932, la macchina Enigma fu forzata nel giro di tre mesi, un po' per l'incredibile leggerezza delle procedure di cifra tedesche, un po' per merito di tre matematici polacchi Marian Rejewski, Henryk Zygalski e Jerzy Rozickii. Questi tre matematici furono assunti dal controspionaggio, in quanto risultarono i migliori nel test del corso di matematica discreta, istituito preventivamente dall'Università di Poznań per potenziare le capacità di decifrazione dei matematici polacchi.
La decifrazione dei messaggi avveniva attraverso metodi manuali, ricostruendo via via la struttura della macchina Enigma, fino a realizzare, nel 1933, una copia polacca della macchina tedesca, chiamata Bomba. Di conseguenza, i polacchi, riuscirono ad intuire che i 3 rotori della macchina potevano essere sistemati negli alloggiamenti in 3! modi diversi. L'anello del rotore poteva essere ruotato manualmente, in modo da ottenere la comparsa di una determinata lettera all'interno della casella. Questo, in termini matematici, significava che la posizione iniziale dei 3 rotori, lettera visibile nella casella (*vedi* Figura 2.1), era una disposizione con ripetizione, quindi $26^3 = 17576$ (cioè 26 possibili posizioni per ciascun rotore). Per il pannello di commutazione si avevano 10^{11} possibilità di associare le lettere, avendo a disposizione 6 cavetti, calcolate moltiplicando le diverse combinazioni

delle lettere scelte a due a due, tenendo conto delle residue, diviso il numero delle permutazioni dei sei cavetti, secondo la seguente formula:

$$\frac{\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}}{6!} \sim 10^{11}$$

Quindi in totale, combinando i possibili alloggiamenti dei 3 rotori con le possibilità di scelta della lettera iniziale di ogni rotore e le possibili associazioni dei cavetti delle lettere nel pannello, otteniamo: $3! \cdot 26^3 \cdot 10^{11} \sim 10^{16}$.
Tra il 1930 e il 1937 i protocolli d'uso erano quelli riportati nel manuale trafugato dalla spia tedesca, che conteneva la chiave del mese, la chiave del giorno e la chiave di messaggio.
La chiave del mese era la posizione dei rotori (quindi per tutto il mese i rotori restavano fissi).
La chiave del giorno (cambiava giorno per giorno) consisteva: nello scegliere come ruotare l'anello per ciascun rotore, in modo tale che una certa lettera corrispondesse alla tacca; nel selezionare, una volta sistemati i rotori, la lettera iniziale(visibile) indicata nel manuale ed infine nel sistemare i 6 cavetti del pannello di commutazione, come indicato nel manuale. I crittanalisti, pertanto, potevano sfruttare questo aspetto per un'intero giorno, dato che i tedeschi usavano sempre la stessa chiave per cifrare una gran quantità di messaggi.
La chiave di messaggio prevedeva la scelta, da parte dell'operatore, di 3 lettere.
Per codificare il messaggio, quindi, occorreva impostare la macchina con la chiave del mese, la chiave del giorno e la chiave di messaggio, la quale veniva ripetuta due volte (duplicata) all'inizio del messaggio. Tale ripetizione garantiva che il messaggio non era stato corrotto, in quanto chi riceveva il messaggio vedeva le prime tre lettere ripetute e questo dava una ragionevole certezza dell'autenticità del messaggio.
Dal 1939 i tedeschi assunsero maggiore confidenza con la struttura di trasmissione dei messaggi e non duplicarono più la chiave di messaggio, anche perché, probabilmente, capirono che alcuni messaggi intercettati erano stati decifrati a causa della duplicazione della chiave.
Per decodificare il messaggio occorreva settare la macchina con le stesse impostazioni (chiave del mese, chiave del giorno, chiave del messaggio) utilizzate dal mittente; questo era possibile perché il procedimento di codifica era involutorio (se $A \longrightarrow B$, $B \longrightarrow A$, cioè dal testo in chiaro ottengo il testo cifrato e dal testo cifrato ottengo quello in chiaro).
La matematica necessaria per la decifrazione fu sviluppata da Gauss, da Galois, da Frobenius e Hermann Weyl.

3.1 Definizioni matematiche introduttive

Definizione 3.1.1. Un gruppo è un insieme G munito di una operazione binaria $*$, che ad ogni coppia di elementi a, b di G associa un elemento, che indichiamo con $a * b$, appartenente a G, rispettando le seguenti proprietà:

- *associativa*: dati a, b, c appartenenti a G, vale $(a * b) * c = a * (b * c)$.
- *esistenza dell'elemento neutro*: esiste in G un elemento neutro e rispetto all'operazione $*$, cioè tale che $a * e = e * a = a$ per ogni a appartenente a G.
- *esistenza dell'inverso*: ad ogni elemento a di G è associato un elemento a', detto inverso di a , tale che $a * a' = a' * a = e$.

Definizione 3.1.2. Siano $f : A \to B$ e $g : C \to D$, due applicazioni, si definisce *prodotto operatorio* di f e g, con l'insieme delle immagini di f incluso in C, denotato $g \circ f$, l'applicazione di dominio A e codominio D, che associa all'elemento x di A l'immagine tramite g dell'elemento $f(x)$.

Definizione 3.1.3. Fissato un insieme finito X, si definisce permutazione una biiezione dell'insieme in sé.

Definizione 3.1.4. Fissato un insieme finito X di n elementi, si definisce S_n il *gruppo simmetrico*, o delle permutazioni σ di un insieme di n elementi, $\sigma \in S_n$, il gruppo con l'operzione di prodotto operatorio di funzioni, indicato con $(S_n, \circ)$.

Tale gruppo ha *ordine*, ossia numero di elementi, pari a $n!$ e per $n \geq 3$, non è commutativo. Sappiamo che il prodotto operatorio è un'operazione associativa e l'applicazione identica è essa stessa una biiezione e gode della proprietà che per ogni funzione $f \in S_n$, $f \circ id_X = id_X \circ f = f$. Inoltre esiste la biiezione inversa f^{-1} tale che $f \circ f^{-1} = f^{-1} \circ f = id_X$. La natura dell'insieme X è irrilevante ai fini dello studio della struttura del gruppo $(S_n, \circ)$. Nel seguito supporremo sempre $X = \{1, 2, \ldots, n\}$ e indicheremo con id l'applicazione identica. Per semplicità di notazione si userà la giustapposizione $\sigma\tau$ per indicare il prodotto operatorio $\sigma \circ \tau$; si ricordi che essendo σ e τ due applicazioni il prodotto operatorio $\sigma \circ \tau$ è l'applicazione che si ottiene eseguendo prima τ e poi σ.
Nel seguito useremo, per brevità, il termine *prodotto*, per intendere il termine *prodotto operatorio*, ove non vi siano situazioni ambigue.

3.2 Presentazione di una permutazione

Sia $\sigma : \{1,2,\ldots,n\} \longrightarrow \{1,2,\ldots,n\}$ una permutazione in S_n.

La presentazione su due righe, anche detta a colonna, di σ è

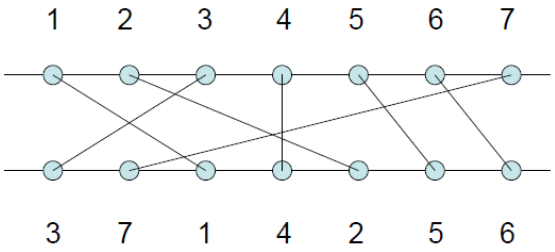
$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Esempio:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 1 & 4 & 2 & 5 & 6 \end{pmatrix}$$

La prima riga è detta permutazione standard e viene scritta ponendo, comunemente, i numeri in ordine crescente.
La seconda riga è una scrittura di tipo funzionale, che rappresenta l'immagine dell'elemento del dominio posto tra parentesi e corrispondente all'elemento soprastante, appartenente alla prima riga.
Una variante di questa presentazione consiste nell' aggiungere dei segmenti che collegano ogni simbolo sulla prima riga con lo stesso simbolo sulla seconda.

Esempio:



In questo modo si possono visualizzare le inversioni della permutazione, cioè le coppie di interi (i,j) tali che

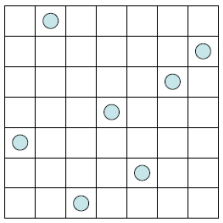
$$i < j \text{ e } \sigma(i) > \sigma(j)$$

Le inversioni, infatti, corrispondono a due segmenti che si intersecano.
Il vantaggio della notazione a colonna è la visualizzazione del collegamento degli elementi della prima riga con gli elementi della seconda. Da notare che lo scambio

di colonne, in tale notazione, lascia la permutazione invariata.
La presentazione su una riga (o presentazione lineare) di σ consiste nello scrivere solamente la sequenza

$$\sigma(1)\,\sigma(2)\ldots\sigma(n)$$

La presentazione grafica, invece, consiste nel considerare una griglia quadrata $n \times n$, nella quale sono inseriti n punti, che rappresentano gli elementi della permutazione, che occupano le caselle $(i, \sigma(i))$ per ogni $i = 1, 2, \ldots, n$.



$$\sigma = 3\ 7\ 1\ 4\ 2\ 5\ 6$$

3.3 Presentazione ciclica

Infine, la presentazione di una permutazione come prodotto di cicli disgiunti. Un ciclo è una lista di interi tra parentesi e definisce la permutazione che associa ad ogni intero quello successivo:

$$(1\ \sigma(1)\ \sigma^2(1)\ \ldots\ \sigma^k(1))\,(\ldots)\,(\ldots)$$

in cui l'ordine con il quale sono elencati i cicli può essere scelto arbitrariamente. Ad esempio la permutazione $\sigma = 3\ 7\ 1\ 4\ 2\ 5\ 6$ ha la seguente scrittura in cicli:

$$\sigma = (1\ 3)\,(2\ 7\ 6\ 5)\,(4)$$

Definizione 3.3.1. Un ciclo $(c_1, c_2, c_3, \ldots, c_p)$, lungo p è la permutazione σ tale che:
$\sigma(c_1) = c_2;\ \sigma(c_2) = c_3;\ \ldots;\ \sigma(c_p) = c_1;\ \sigma(h) = h$, per $h \neq c_j$.

$$(c_1, c_2, c_3, \ldots, c_p) = (c_2, c_3, \ldots, c_p, c_1) = (c_3, \ldots, c_p, c_1, c_2)$$

Due cicli si dicono disgiunti quando non hanno elementi in comune e, se questo accade, essi godono della proprietà commutativa: infatti (1 4 2) (3 5) e (3 5) (1 4 2) definiscono la stessa permutazione.

Definizione 3.3.2. L'*ordine* (o *grado*) k di un ciclo corrisponde alla sua lunghezza, ovvero al numero dei k elementi di cui è costituito.

Definizione 3.3.3. Un ciclo di ordine 2 è detto trasposizione.

Ogni permutazione si può scrivere come composizione di cicli disgiunti in modo unico, a meno dell'ordine secondo cui gli stessi cicli sono stati scritti.
Ogni ciclo, a sua volta, è un prodotto di trasposizioni; ad esempio, il ciclo (1 4 2) può essere riscritto come (1 4) (1 2). Ne segue quindi che anche ogni permutazione è prodotto di trasposizioni: (1 4 2) (3 5) equivale a (1 4) (1 2) (3 5).

Esempio:

$$\sigma = 4\ 1\ 5\ 2\ 3 = (1\ 4\ 2)\ (3\ 5)$$

La notazione ciclica di σ implica che:

$$\begin{array}{ll} \sigma(1) = 4, \sigma(4) = 2, \sigma(2) = 1 & \text{primo ciclo} \\ \sigma(3) = 5, \sigma(5) = 3 & \text{secondo ciclo} \end{array}$$

Esistono vari modi di scrivere una singola permutazione come prodotto di trasposizioni e queste ultime non sono necessariamente disgiunte. Il numero di fattori di questo prodotto non è infatti univocamente determinato dalla permutazione, al contrario però della sua parità. Se una permutazione infatti è pari, essa potrà essere scritta solo e soltanto come prodotto di un numero pari di trasposizioni (e viceversa per quelle dispari):

$$\begin{array}{ll} 4\ 1\ 5\ 2\ 3 = (1\ 4)\ (1\ 2)\ (3\ 5) = (1\ 4)\ (1\ 2)\ (1\ 3)\ (1\ 5)\ (1\ 3) & \text{dispari} \\ 4\ 1\ 5\ 3\ 2 = (1\ 4)\ (1\ 3)\ (1\ 5)\ (1\ 2) & \text{pari} \end{array}$$

Le permutazioni pari di lunghezza n sono la metà di quelle totali, il che equivale a dire che ne esistono tante quante quelle dispari.

3.4 Le involuzioni

Una permutazione σ è un'involuzione se e solo se risulta uguale all'inversa di se stessa:

$$\sigma = \sigma^{-1}$$

Più formalmente le involuzioni di un insieme X sono le funzioni biiettive $i : X \longrightarrow X$ tali che, $\forall x \in X, i(i(x)) = x$ Le permutazioni che soddisfano questa proprietà sono soltanto quelle scomponibili in cicli di lunghezza massima uguale a 2. Infatti applicando 2 volte una stessa trasposizione il risultato è l'identità:

$$2\ 1\ 3 = (1\ 2)\ (3)$$
$$(1\ 2)^2(3)^2 = 1\ 2\ 3$$

L'involuzione è tale che il quadrato della trasformazione risulta l'identità, cioè la trasformazione coincide con la sua inversa.
In altre parole le involuzioni sono sempre riscrivibili come prodotto di trasposizioni disgiunte ed eventuali *punti fissi* o *uniti*, ossia elementi che vengono associati a se stessi.

3.5 Ribaltamento e complemento di una permutazione

Sia $\sigma = x_1\ x_2\ \ldots\ x_n$ una permutazione in S_n. Definiamo il ribaltamento (reverse) di σ come la permutazione:

$$\sigma^r = x_n\ x_{n-1}\ \ldots\ x_2\ x_1$$

ed il complemento (complement) di σ come:

$$\sigma^c = (n+1-x_1)(n+1-x_2)\ldots(n+1-x_n)$$

Esempio:

$$\sigma\ = 3\ 5\ 7\ 1\ 8\ 4\ 2\ 6$$
$$\sigma^r = 6\ 2\ 4\ 8\ 1\ 7\ 5\ 3$$
$$\sigma^c = 6\ 4\ 2\ 8\ 1\ 5\ 7\ 3$$

Notiamo che, indicando con ψ la permutazione

$$\psi = n\ n-1\ \ \ldots\ 2\ 1$$

risulta

$$\sigma^c = \psi\ \sigma$$

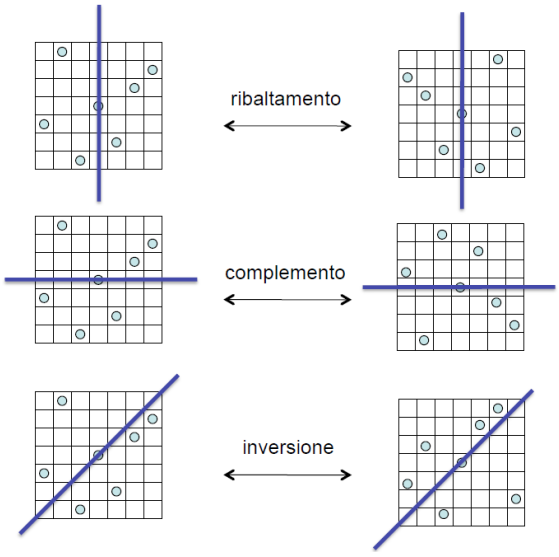
e

$$\sigma^r = \sigma\ \psi$$

inoltre,

$$\sigma^{cr} = \sigma^{rc}$$
$$(\sigma^c)^{-1} = (\sigma^{-1})^r$$
$$(\sigma^r)^{-1} = (\sigma^{-1})^c$$

Osserviamo anche che le operazioni di ribaltamento, complemento ed inversione di una permutazione corrispondono, nella presentazione grafica, alle simmetrie del quadrato:



3.6 Presentazione matematica della macchina Enigma

La struttura delle permutazioni serve a descrivere un rotore, in particolare come mostrato in Figura 3.1, σ è la permutazione di entrata abbinata al rotore, mentre σ^{-1} è la permutazione inversa.

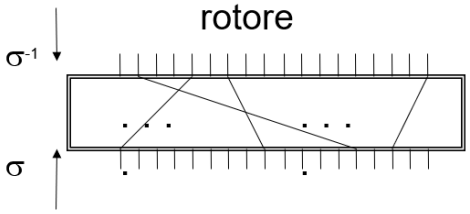


Figura 3.1: Schema logico rotore e relative permutazioni

Come indicato in Figura 3.2, $\varphi\ \lambda\ \mu\ \nu\ \rho$ indicano le singole permutazioni, rispettivamente abbinate, al pannello di commutazione, al rotore di destra, al rotore centrale, al rotore di sinistra, al riflettore.

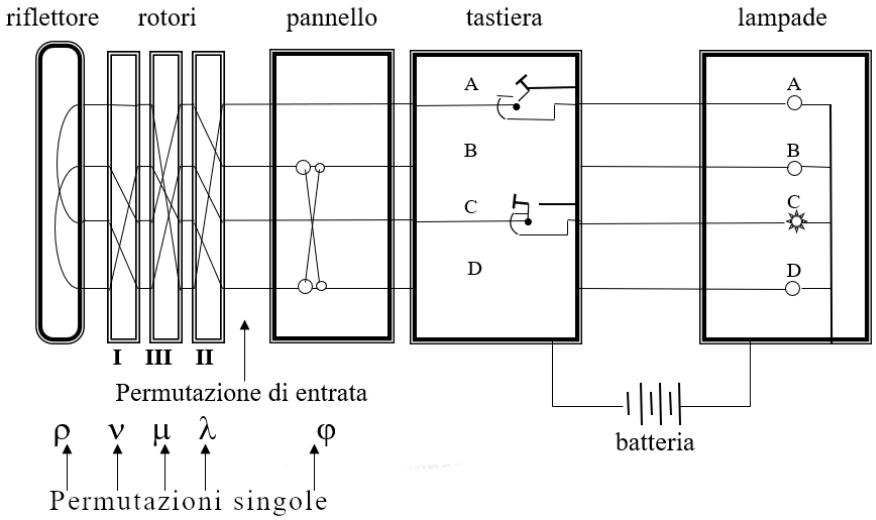


Figura 3.2: Schema logico della macchina Enigma e relative permutazioni

Considerando le relative inverse $\varphi^{-1}, \lambda^{-1}, \mu^{-1}, \nu^{-1}$ e eseguendo il *prodotto* si ottiene:

$$\eta = \varphi^{-1}\ \lambda^{-1}\ \mu^{-1}\ \nu^{-1}\ \rho\ \nu\ \mu\ \lambda\ \varphi$$

Si tenga presente che dato che ρ è una involuzione e anche φ è una involuzione, allora anche η è una involuzione, quindi si ha:

$$\eta^2 = (\varphi^{-1}\ \lambda^{-1}\ \mu^{-1}\ \nu^{-1}\ \rho\ \nu\ \mu\ \lambda\ \varphi) \circ (\varphi^{-1}\ \lambda^{-1}\ \mu^{-1}\ \nu^{-1}\ \rho\ \nu\ \mu\ \lambda\ \varphi)$$

$$\eta^2 = I$$

Pertanto la codifica coincide con la sua inversa: la decodifica (se utilizzate le stesse impostazioni per la macchina).
In particolare φ e φ^{-1} godono di questa proprietà.

Teorema 3.6.1. $\forall \sigma \in S_n$ *esiste un numero finito di cicli disgiunti tali che*

$$\sigma = \lambda_1\ \lambda_2\ \ldots\ \lambda_k$$

La scrittura **standard** di una permutazione si definisce con l'uso di cicli disgiunti costruiti in modo che la lunghezza dei cicli sia non decrescente, ogni ciclo inizi con l'elemento minore, i cicli di uguale lunghezza siano ordinati in base al valore dell'elemento iniziale

Definizione 3.6.1. $\forall \sigma \in S_n$ si dice struttura di cicli di σ la k-upla $(p_1, p_2, \ldots, p_k)$ dove p_j è la lunghezza di λ_k; $(p_1, p_2, \ldots, p_k) \vdash n$

Definizione 3.6.2. $\forall \sigma \in S_n$ la coniugata di σ mediante τ è la permutazione $\tau^{-1}\sigma\tau$ o, data la struttura di gruppo, $\tau\sigma\tau^{-1}$

Teorema 3.6.2. $\forall \sigma \in S_n$ *la coniugata di* σ *mediante una qualunque* τ *ha la stessa struttura di cicli.*

Dalla definizione di trasposizione si ha che detta τ una trasposizione, $\tau^2 = I$
Se $\sigma = \tau_1\ \tau_2\ \ldots\ \tau_p$ e le τ_j sono trasposizioni disgiunte allora $\sigma^2 = I$.
Si tenga conto che il riflettore è il prodotto di 13 trasposizioni disgiunte (fisse); il pannello di commutazione è il prodotto di 6 trasposizioni disgiunte(variabili)

Teorema 3.6.3. *Sia n pari;* $\forall \sigma \in S_n$, $\sigma \neq I$ *involuzione* $(\sigma^2 = I)$ *allora* $\exists\ \tau_1,\ \tau_2,\ \ldots,\ \tau_p$ *trasposizioni disgiunte tali che* $\sigma = \tau_1\ \tau_2\ \ldots\ \tau_p$, $p \leq \frac{n}{2}$

Definizione 3.6.3. Un prodotto di trasposizioni disgiunte si dice trasposizione generalizzata

La permutazione η è una trasposizione generalizzata senza punti uniti

Teorema 3.6.4. *Il prodotto di due trasposizioni generalizzate non è una trasposizione generalizzata, ma è una permutazione la cui struttura in cicli ha le lunghezze dei cicli ripetute*

Esempio:

$(6,6,4,4,3,3) \vdash 26$
$(6,6,4,4,2,2,1,1) \vdash 26$

Consideriamo a questo punto il modello dinamico dei rotori.
Rejewski ha intuito che i rotori potevano essere rappresentati come una permutazione ciclica, in particolare indichiamo $\pi = (A,B,C,D,\ldots,Z)$ tale permutazione; $\pi \equiv (1,2,3,4,\ldots,26)$

Inizialmente denominiamo:

- λ permutazione associata al primo rotore da destra; tale permutazione è considerata statica nel momento in cui viene digitata una lettera sulla tastiera, successivamente avviene una rotazione del rotore che genera una nuova permutazione.

- $\pi = (ABCDEFGHIJKLMNOPQRSTUVWXYZ)$ permutazione ciclica delle 26 lettere in ordine alfabetico
- $\pi^{-1} = (ZYXWVUTSRQPONMLKJIHGFEDCBA)$
  $= (AZYXWVUTSRQPONMLKJIHGFEDCB)$

Il seguente prodotto di permutazioni:

$$\pi^{-0}\ \lambda\ \pi^{0} = \lambda$$

descrive lo stato iniziale del rotore di destra.

Alla digitazione di un carattere si ha:

$$\pi^{-1}\ \lambda\ \pi^{1}$$

alla successiva digitazione di un carattere si ha:

$$\pi^{-2}\ \lambda\ \pi^{2}$$

e cosi via fino all'n-esimo carattere:

$$\eta_n = \varphi^{-1}\ \pi^{n}\ \lambda^{-1}\ \pi^{-n}\ \mu^{-1}\ \nu^{-1}\ \rho\ \nu\ \mu\ \pi^{-n}\ \lambda\ \pi^{n}\ \varphi$$

Pertanto η_n è la permutazione associata ai primi n caratteri del messaggio fin quando non ruota il secondo rotore (cioè fino a quando la tacca dell'anello del primo rotore occupa la posizione in cui il secondo dito flessibile impegna la ruota dentata del secondo rotore).
I problemi riscontrati dai polacchi, fino al 1937, erano sostanzialmente due:

- determinare le permutazioni fisse ρ, ν, μ, λ associate al riflettore e ai tre rotori, cioè di determinare la struttura della macchina
- una volta compresa la struttura della macchina, decifrare i messaggi, quando non era nota la chiave.

3.7 Primo problema

I dati in loro possesso erano le chiavi per i mesi di settembre e ottobre del 1932, qualche migliaio di messaggi cifrati dello stesso periodo e decine di migliaia accumulati dal 1928. Inoltre, inizialmente, i messaggi cifrati dai tedeschi avevano una debolezza fondamentale, data dalla ripetizione della chiave di messaggio.
Un'ulteriore debolezza di tipo strutturale era data dal pannello di commutazione, che come indicato nella chiave del giorno riportata nel manuale, informava sulla disposizione dei cavetti, ma ciò non alterava la struttura in cicli.
Consideriamo il messaggio SPOSTARELETRUPPE... a tale messaggio veniva anteposta per due volte una stessa sequenza di tre lettere, ottendo ad esempio XYZXYZSPOSTARELETRUPPE... al cui messaggio corrispondeva la possibile codifica OTUNSD..., quindi $\eta_1(X) = O$; $\eta_4(X) = N$, da cui $\eta_4\eta_1(O) = N$ considerando che le η sono involuzioni.
Pertanto con numerosi messaggi si poteva determinare completamente $\eta_4\eta_1$.
Utilizzando i messaggi di un giorno erano note le permutazioni:

$\alpha_1 = \eta_4\eta_1$, considerando le lettere 1 e 4 dei messaggi cifrati
$\alpha_2 = \eta_5\eta_2$, considerando le lettere 2 e 5 dei messaggi cifrati
$\alpha_3 = \eta_6\eta_3$, considerando le lettere 3 e 6 dei messaggi cifrati

e se ne poteva determinare la struttura di cicli. Si constata che le lunghezze dei cicli comparivano sempre in coppie, quindi le η sono trasposizioni generalizzate.
Rejewski dimostra un teorema semicostruttivo che permette di fattorizzare le α_j.
Inoltre dall'espressione generale delle η è possibile vedere che i cicli delle α_j non dipendono da ρ e φ, rispettivamente riflettore e pannello. Avendo a disposizione un numero sufficiente di messaggi, circa 80, dello stesso giorno comparivano nella posizione iniziale del rotore tutte le lettere dell'alfabeto. Al crittoanalista non erano note le permutazioni intermedie, che permettevano di passare dalla prima lettera del messaggio alla quarta, ugualmente dalla seconda alla quinta e dalla

terza alla sesta. Ma sapevano che vi era una corrispondenza, dopo due rotazioni, tra le prime sei lettere, ovvero, la prima e la terza lettera del messaggio cifrato corrispondevano alla stessa lettera nel messaggio in chiaro, così come la seconda e la quinta ad una stessa lettera e la terza e la sesta ad una stessa lettera

Secondo il funzionamento della macchina Enigma si deduceva che le permutazioni sconosciute al crittoanalista erano formate solo da trasposizioni. Considerando più messaggi supponiamo di conoscere un frammento della permutazione AD che è un prodotto di permutazioni sconosciute, ad esempio $dmq\ vbn$, $von\ puy$, $puc\ fmq$ denotano le chiavi iniziali di 3 messaggi, per cui, dopo 2 rotazioni del rotore, d è sostituito da v, v da p, p da f, da cui otteniamo il frammento per la permutazione AD, $dvpf$. Allo stesso modo per la seconda e la quinta lettera notiamo che o è sostituito da u, u è sostituito da m e m è sostituito da b, ottenendo un frammento BE, cioè $oumb$. Infine per la terza e la sesta lettera c viene sostituito da q, q da n, n da y. Ottenendo CF, ovvero $cqny$. L'inizio di altri messaggi consente di conoscere completamente le permutazioni AD, BE, CF.

Esempio:

$$\begin{aligned} AD &= (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s) \\ BE &= (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k) \\ CF &= (abviktjgfcqny)(duzrehlxwpsmo) \end{aligned}$$

Questo insieme di uguaglianze, per la sua forma e importanza primaria, sarà chiamato *insieme caratteristico* o, direttamente, le *caratteristiche* di un dato giorno.
Denotando con φ la permutazione associata al pannello, ν, μ, λ le permutazioni associate ai rotori (*vedi* Figura 3.2) e da ρ la permutazione associata al riflettore, premendo un tasto, si ottiene, considerando la proprietà di coniugazione come definito precedentemente, la seguente formula:

$$\eta = \varphi\ \lambda\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \lambda^{-1}\ \varphi^{-1}$$

Considerando la permutazione π si ha che le permutazioni da AF sconosciute possono essere rappresentate nella seguente forma:

$$\begin{aligned} A &= \varphi\ \pi\ \lambda\ \pi^{-1}\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \pi\ \lambda^{-1}\ \pi^{-1}\ \varphi^{-1} \\ B &= \varphi\ \pi^2\ \lambda\ \pi^{-2}\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \pi^2\ \lambda^{-1}\ \pi^{-2}\ \varphi^{-1} \\ &\cdots \\ E &= \varphi\ \pi^5\ \lambda\ \pi^{-5}\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \pi^5\ \lambda^{-1}\ \pi^{-5}\ \varphi^{-1} \\ F &= \varphi\ \pi^6\ \lambda\ \pi^{-6}\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \pi^6\ \lambda^{-1}\ \pi^{-6}\ \varphi^{-1} \end{aligned}$$

Mentre i prodotti noti AD, BE, CF sono dati dalle seguenti formule:

$$AD = \varphi\ \pi\ \lambda\ \pi^{-1}\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \pi\ \lambda^{-1}\ \pi^3\lambda\ \pi^{-4}\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \pi^4\ \lambda^{-1}\ \pi^{-4}\ \varphi^{-1}$$
$$BE = \varphi\ \pi^2\ \lambda\ \pi^{-2}\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \pi^2\ \lambda^{-1}\ \pi^3\lambda\ \pi^{-5}\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \pi^5\ \lambda^{-1}\ \pi^{-5}\ \varphi^{-1}$$
$$CF = \varphi\ \pi^3\ \lambda\ \pi^{-3}\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \pi^3\ \lambda^{-1}\ \pi^3\lambda\ \pi^{-6}\ \mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}\ \pi^6\ \lambda^{-1}\ \pi^{-6}\ \varphi^{-1}$$

Di questo insieme di equazioni conosciamo i membri di sinistra, la permutazione π e le sue potenze riportate a destra, mentre le permutazioni $\varphi, \nu, \mu, \lambda, \rho$ sono sconosciute. Poiché in questa forma l'insieme è certamente irrisolvibile, dobbiamo semplificarlo. Il primo passaggio in questa direzione è puramente formale e consiste nella sostituzione di una lettera Q al posto di $\mu\ \nu\ \rho\ \nu^{-1}\ \mu^{-1}$ in modo da approssimare, i due rotori che girano più raramente insieme al riflettore, come un unico blocco, quindi il numero delle incognite si riduce a 3 φ, λ, Q. Pertanto abbiamo:

$$AD = \varphi\ \pi\ \lambda\ \pi^{-1}\ Q\ \pi\ \lambda^{-1}\ \pi^3\lambda\ \pi^{-4}\ Q\ \pi^4\ \lambda^{-1}\ \pi^{-4}\ \varphi^{-1}$$
$$BE = \varphi\ \pi^2\ \lambda\ \pi^{-2}\ Q\ \pi^2\ \lambda^{-1}\ \pi^3\lambda\ \pi^{-5}\ Q\ \pi^5\ \lambda^{-1}\ \pi^{-5}\ \varphi^{-1}$$
$$CF = \varphi\ \pi^3\ \lambda\ \pi^{-3}\ Q\ \pi^3\ \lambda^{-1}\ \pi^3\lambda\ \pi^{-6}\ Q\ \pi^6\ \lambda^{-1}\ \pi^{-6}\ \varphi^{-1}$$

3.7.1 Teorema sul prodotto delle trasposizioni

Il prossimo passo è il più importante. L'obiettivo è ottenere le permutazioni disgiunte non note dalla A alla F dai prodotti noti AD, BE, CF. Come spiegato in precedenza, le permutazioni sconosciute sono formate solo da trasposizioni e le espressioni AD, BE, CF sono i loro prodotti. Possiamo applicare il seguente:

Teorema 3.7.1. *Se due permutazioni dello stesso grado sono formate solo da trasposizioni disgiunte, il loro prodotto contiene un numero pari di cicli disgiunti della stessa lunghezza*

Dimostrazione. Consideriamo che X ed Y rappresentino il prodotto delle permutazioni e si consideri essere il grado $2n$. Se nella permutazione X compare una trasposizione identica ad una trasposizione in Y, ad esempio (ab) si presenta nel prodotto XY con la presenza di una coppia di cicli a lettera singola $(a)(b)$, quindi in tale caso il teorema risulta dimostrato per le trasposizioni identiche. Dopo aver analizzato il caso particolare, possiamo assumere senza perdita di generalità che si presentano le seguenti trasposizioni:

nella permutazione X	nella permutazione Y
(a_1a_2)	(a_2a_3)
(a_3a_4)	(a_4a_5)
$\dots$	$\dots$
$(a_{2k-3}a_{2k-2})$	$(a_{2k-2}a_{2k-1})$
$(a_{2k-1}a_{2k})$	$(a_{2k}a_1)$

Infatti la lettera iniziale a_1 deve apparire nella permutazione finale della Y. Se facciamo il prodotto XY otteniamo sempre due cicli della stessa lunghezza $k \leq n$

$$(a_1\, a_3\, \ldots\, a_{2k-3}\, a_{2k-1})\,(a_{2k}\, a_{2k-2}\, \ldots\, a_4\, a_2)$$

Se con questa procedura non sono state esaminate tutte le lettere della permutazione, continuiamo la procedura fino a quando non sono state esaminate tutte. Allo stesso tempo si può notare che

1. le lettere di una determinata trasposizione sono sempre osservate in due cicli differenti della stessa lunghezza della permutazione XY
2. se due lettere compaiono in due diversi cicli della stessa lunghezza, nella permutazione XY, appartengono alla stessa trasposizione, quindi le lettere vicine di destra e di sinistra appartengono alla stessa trasposizione.

□

Il teorema inverso è particolarmente importante

Teorema 3.7.2 (teorema inverso)**.** *Se in una qualsiasi permutazione di grado pari appare un numero pari di cicli disgiunti della stessa lunghezza, allora la permutazione può essere considerata come un prodotto di due permutazioni ciascuna delle quali consiste solo di trasposizioni disgiunte.*

Tralasciando la dimostrazione di tale teorema ed applicandolo ai prodotti AD, BE, CF, esso prevede per ciascuna delle espressioni di A, B, C, a seconda della forma dei prodotti, diverse decine di migliaia di possibili soluzioni e scegliere quella corretta sarebbe un compito difficile. Il teorema non ci porta alla completa soluzione del problema, ma in prossimità di essa. Supponendo di conoscere le preferenze di scelta delle tre lettere iniziali, da parte dei vari crittografi, e utilizzando il teorema sul prodotto delle trasposizioni si ha la possibilità di trovare l'unica soluzione reale.
Supponiamo, per esempio, che i crittografi, come chiave, preferiscano le stesse tre lettere. In particolare considerando jjj, se xqr e gve sono le chiavi cifrate, allora facendo uso dell'insieme caratteristico considerato nell'esempio precedente e assumendo che queste lettere corispondano a jjj nel testo in chiaro, concludiamo, ad esempio, che $nfaqqb$ e $eugimf$ siano rispettivamente ppp e zzz le lettere iniziali del messaggio in chiaro.

In conclusione i membri di sinistra dell'insieme di equazioni:

$$\begin{gathered} A = \varphi\ \pi\ \lambda\ \pi^{-1}\ Q\ \pi\ \lambda^{-1}\ \pi^{-1}\ \varphi^{-1} \\ B = \varphi\ \pi^2\ \lambda\ \pi^{-2}\ Q\ \pi^2\ \lambda^{-1}\ \pi^{-2}\ \varphi^{-1} \\ \cdots \\ F = \varphi\ \pi^6\ \lambda\ \pi^{-6}\ Q\ \pi^6\ \lambda^{-1}\ \pi^{-6}\ \varphi^{-1} \end{gathered}$$

possono essere considerati noti. Quindi genralmente il crittoanalista non conosce queste preferenze, ma compensa questa mancanza con lunghe prove e immaginazione. Nel dicembre 1932 l'Ufficio Cifra francese fornì all'Ufficio Cifra polacco il manuale segreto contenente le tabelle delle chiavi tedesche di Enigma, comprese le connessioni del pannello. Quindi fu possibile considerare come nota la permutazione φ nell'insieme delle equazioni, per cui si ha:

$$\begin{gathered} \varphi^{-1}\ A\ \varphi = \pi\ \lambda\ \pi^{-1}\ Q\ \pi\ \lambda^{-1}\ \pi^{-1} \\ \varphi^{-1}\ B\ \varphi = \pi^2\ \lambda\ \pi^{-2}\ Q\ \pi^2\ \lambda^{-1}\ \pi^{-2} \\ \cdots \\ \varphi^{-1}\ F\ \varphi = \pi^6\ \lambda\ \pi^{-6}\ Q\ \pi^6\ \lambda^{-1}\ \pi^{-6} \end{gathered}$$

In questo modo si ottiene l'insieme di sei equazioni con solo due incognite, le permutazioni di λ e Q. Questo insieme è risolvibile ma bisogna fare prima ulteriori trasformazioni. Prima di effettuare tali trasformazioni, analizziamo un problema della teoria delle permutazioni:
Date tre permutazioni G, H, T e

$$G = T^{-1}\ H\ T$$

Allora diremo che la permutazione G è trasformata dalla permutazione H attraverso la permutazione T.
Come è dimostrato nella teoria delle permutazioni, non c'è bisogno di moltiplicare la permutazione H per T^{-1} a sinistra e per T a destra per ottenere la permutazione G. È sufficiente eseguire sugli elementi della permutazione H i cambiamenti descritti nella permutazione T.

Definizione 3.7.1. Due permutazioni si dicono *simili* se hanno la stessa struttura ciclica.

Teorema 3.7.3. *Siano $\sigma_1, \sigma_2 \in S_n$; sono equivalenti:*

(i) *σ_1 e σ_2 sono simili,*

(ii) $\exists \epsilon \in S_n \qquad \epsilon^{-1}\ \sigma_1\ \epsilon = \sigma_2$

Pertanto, le permutazioni G e H sono simili. Ne consegue che se T è considerato non noto, allora l'equazione $G = T^{-1}\ H\ T$ è risolvibile se solo se le permutazioni G e H sono simili e otteniamo tante soluzioni per T quanti sono i modi di scrivere la permutazione G attraverso H, senza cambiare il valore della permutazione G. In tutti i casi, tuttavia, in cui G (o H) è costituito solo da trasposizioni, il numero di soluzioni è molto grande.
Ad esempio per 13 trasposizioni ci sono $2^{13}\cdot 13! = 51011754393600$ soluzioni. Quindi, per eliminare le trasposizioni, dobbiamo effettuare dei cambiamenti. Per prima cosa trasformiamo entrambi i membri delle equazioni consecutive per mezzo di $\pi, \pi^2, \ldots, \pi^6$ rispettivamente, denotiamo per brevità il membro di sinistra delle corrispondenti equazioni con $U, V, \ldots, Z$ si ha:

$$\begin{gathered} U = \pi^{-1}\ \varphi^{-1}\ A\ \varphi\ \pi = \lambda\ \pi^{-1}\ Q\ \pi\ \lambda^{-1} \\ V = \pi^{-2}\ \varphi^{-1}\ A\ \varphi\ \pi^2 = \lambda\ \pi^{-2}\ Q\ \pi^2\ \lambda^{-1} \\ \cdots \\ Z = \pi^{-6}\ \varphi^{-1}\ A\ \varphi\ \pi^6 = \lambda\ \pi^{-6}\ Q\ \pi^6\ \lambda^{-1} \end{gathered}$$

Da cui i prodotti:

$$\begin{gathered} UV = \lambda\ \pi^{-1}\ (Q\ \pi^{-1}\ Q\ \pi)\ \pi\ \lambda^{-1} \\ VW = \lambda\ \pi^{-2}\ (Q\ \pi^{-1}\ Q\ \pi)\ \pi^2\ \lambda^{-1} \\ WX = \lambda\ \pi^{-3}\ (Q\ \pi^{-1}\ Q\ \pi)\ \pi^3\ \lambda^{-1} \\ XY = \lambda\ \pi^{-4}\ (Q\ \pi^{-1}\ Q\ \pi)\ \pi^4\ \lambda^{-1} \\ YZ = \lambda\ \pi^{-5}\ (Q\ \pi^{-1}\ Q\ \pi)\ \pi^5\ \lambda^{-1} \end{gathered}$$

Sostituendo le espressioni in comune $Q\ \pi^{-1}\ Q\ \pi$ si ottiene un insieme di quattro equazioni con solo un'incognita $\lambda\ \pi\ \lambda^{-1}$:

$$\begin{gathered} VW = \lambda\ \pi^{-1}\ \lambda^{-1}\ (UV)\ \lambda\ \pi\ \lambda^{-1} \\ WX = \lambda\ \pi^{-1}\ \lambda^{-1}\ (VW)\ \lambda\ \pi\ \lambda^{-1} \\ XY = \lambda\ \pi^{-1}\ \lambda^{-1}\ (WX)\ \lambda\ \pi\ \lambda^{-1} \\ YZ = \lambda\ \pi^{-1}\ \lambda^{-1}\ (XY)\ \lambda\ \pi\ \lambda^{-1} \end{gathered}$$

Procedendo secondo il metodo considerato in precedenza otteniamo per la prima equazione diverse decine di possibili espressioni per $\lambda\ \pi\ \lambda^{-1}$ a seconda della forma della permutazione UV (o di VW, WX, XY, YZ, poiché tutte queste permutazioni devono avere la stessa forma, altrimenti si è verificato un errore nei calcoli o il rotore centrale ha compiuto una rotazione). Otteniamo lo stesso numero di soluzioni per $\lambda\ \pi\ \lambda^{-1}$ dalla seconda equazione e una delle soluzioni deve essere identica a quella determinata dalla prima equazione. Ora le ultime due equazioni non sono necessarie. Confrontiamo il risultato ottenuto come soluzione per $\lambda\ \pi\ \lambda^{-1}$ con la permutazione π. In questo modo otteniamo 26 possibili soluzioni per λ^{-1} che non differiscono notevolmente tra loro e dopo aver scelto una di queste possiamo facilmente ottenere λ stesso, cioè le connessioni interne del rotore destro.

3.8 Secondo problema

Analizziamo la situazione conoscendo la struttura della macchina, ma non avendo le chiavi. Esaminando i messaggi di ogni giorno o almeno le prime decine si determinano le strutture dei cicli:

$$\alpha_1 = \eta_1\eta_3$$
$$\alpha_2 = \eta_2\eta_5$$
$$\alpha_3 = \eta_3\eta_6$$

Come ampiamente analizzato precedentemente, le α hanno una struttura di cicli ciascuno ripetuto due volte; Rejewsky denomina la struttura in cicli non ripetuti *insieme caratteristico*, che non dipende da φ e ρ per il teorema sulla coniugazione. Inizialmente si compilava a mano un catalogo dell'*insieme caratteristico* delle α_j in corrispondenza delle circa 100000 posizioni iniziali dei tre rotori, successivamente si utilizzerà uno strumento denominato ciclometro. Una possibile voce del catalogo, ad esempio, avrebbe potuto essere:

posizione iniziale dei rotori		insieme caratteristico
$\nu\ \mu\ \lambda$	$\longrightarrow$	(6 4 3) (7 5 1) (7 6)

L'*insieme caratteristico* ha una struttura dimezzata definita in cicli delle α.

λ permutazione associata al rotore destro
μ permutazione associata al rotore centrale
ν permutazione associata al rotore sinistro

I possibili insiemi caratteristici di un'α sono le partizioni di 13: cioè 101. Per il rotore destro sono possibili 101^3 = 1.030.301 configurazioni. Per il rotore sinistro le differenti configurazioni sono $6 \cdot 26^3$ = 105.456, quindi ad ogni insieme caratteristico corrisponde una configurazione o un numero molto piccolo.
Con un centinaio di configurazioni per facciata, il catalogo poteva avere tra i 500 e i 600 fogli e doveva essere consultabile per caratteristica, quindi si aveva un problema costruttivo.
In particolare ci si chiedeva come ordinare il catalogo, costruito inizialmente posizionando gli elementi del dominio in modo crescente, in ordine crescente rispetto agli elementi del codominio.
Molte delle tabelle utilizzate nel corso della storia del calcolo sono di funzioni monotone, ad esempio logaritmiche, o periodiche, di cui è tabulata la parte *monotona*.
Dato un insieme di messaggi di un giorno, si determinava l'*insieme caratteristico*, delle tavole e le relative configurazioni dei rotori venivano provate manualmente sulla replica della macchina (Bomba).

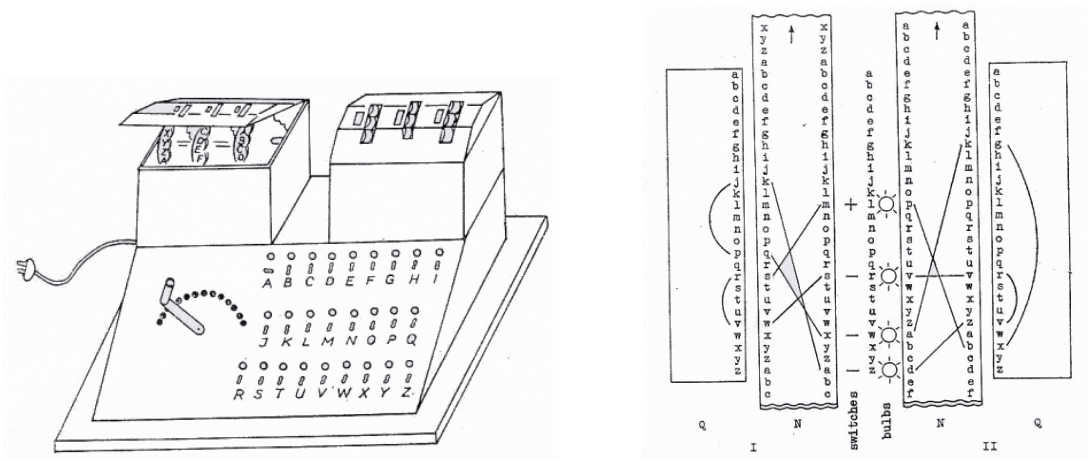
Utilizzando pochi messaggi, si determinava per tentativi:

la φ (dal significato di qualche parola),
la posizione della prima tacca (entro le prime 25 lettere del messaggio)
la seconda tacca (cioè la posizione degli anelli).

Il procedimento spesso veniva terminato in meno di mezz'ora per messaggio. In media un messaggio ogni quattro non poteva essere decifrato così facilmente, perché il rotore centrale poteva ruotare.

3.8.1 Il ciclometro

In seguito, come affermato, per la compilazione di un catalogo, si utilizzò lo strumento, riportato in Figura 3.3, denominato ciclometro.



(a) ciclometro **(b)** schema del rotori del ciclometro

Figura 3.3: Rappresentzione dello strumento, chiamato ciclometro (a) e digramma schematico dei suoi rotori (b)

Non esiste una documentazione precisa e completa (Marian Rejewski, An Application of the Theory of Permutations in Breaking the Enigma Cipher Applicaciones Mathematicae. 16, No. 4, Warsaw 1980. Received on 13.5.1977). Dalle fonti si sa che era composto da 2 gruppi di 3 rotori connessi elettricamente. Il rotore di destra del secondo gruppo era ruotato di 3 posizioni rispetto a quello di destra del primo gruppo, gli altri rotori erano in fase. Con i 2 gruppi di rotori si potevano confrontare le codifiche delle prime 3 lettere di un messaggio con le 3 successive.

Un sistema di connessioni faceva accendere delle lampadine: la lunghezza dei cicli era scandita dalla posizione del reostato. Il sistema era lento e macchinoso, ma efficace per la costruzione del catalogo.

Riassumendo, fino al 1937 la ripetizione della chiave di messaggio consentiva di determinare l'*insieme caratteristico*, mentre i 3 rotori davano la possibilità di scegliere tra circa 100.000 configurazioni e l'associazione caratteristica-configurazione poteva essere costruita e invertita manualmente una volta per tutte.
Dal 1937 al 1939 ci furono vari cambiamenti; nello specifico, nel 1938 i crittoanalisti tedeschi incrementarono la sicurezza di Enigma, aggiungendo alle macchine ulteriori livelli di complessità, i rotori non erano più solo 3, ma venivano scelti da un raggruppamento di 5 e vi fu un cambiamento del riflettore. Tali cambiamenti vennero individuati e la ricostruzione delle permutazioni, associate al riflettore e ai due nuovi rotori, venne fatta manualmente e in maniera relativamente rapida.
Vi erano le seguenti differenze: con 3 rotori si avevano 6 possibilità di disporli nei 3 alloggiamenti, mentre con 5, si avevano 60 possibilità di disporli nei 3 alloggiamenti, quindi circa 1.000.000 di configurazioni; pertanto non era più possibile costruire e, soprattutto, invertire manualmente la corrispondenza.
Si cercò di porre rimedio al problema di ricostruire la configurazione dell'*insieme caratteristico* in vari modi, o manuali (i fogli di Zygalski) o semi-manuali (le bombe di Rejevski), metodi sostanzialmente insoddisfacenti.
Verso la metà del 1939, prima dell'inizio della guerra, ci fu l'evento decisivo: la chiave di messaggio non fu più duplicata. Dunque, diventò inapplicabile il metodo della caratteristica e fallirono i metodi manuali. Si decifravano solo pochissimi messaggi.
Per continuare la decifrazione, da parte dei polacchi, sarebbe stato necessario costruire altre 54 bombe: un costo enorme, insostenibile, che interruppe ogni progresso.
Il 1 settembre 1939 iniziò la guerra e la Polonia fu invasa dalla Germania; astutamente, però, qualche mese prima, i crittoanalisti polacchi contattarono i colleghi francesi e inglesi, offrendo loro le proprie ricerche.
Gli inglesi sfruttarono i progressi raggiunti fino a quel punto dai polacchi nella decifrazione dei messaggi nazisti e assunsero un ruolo di primo piano nello studio dei metodi di decodificazione di tali messaggi, migliorando le procedure di decifrazione. Erano in uso da parte dei tedeschi circa 40.000 macchine Enigma, entro la fine della guerra divennero circa 100.000.

Capitolo 4

Tecniche di decifrazione inglesi

Alla vigilia dell'invasione della Polonia, nel 1939, il progetto venne trasferito agli inglesi, i quali organizzarono un'attività di intercettazione e decifrazione su vasta scala delle comunicazioni radio tedesche, presso un grande edificio vittoriano, detto Bletchley Park, situato in Gran Bretagna. Gli inglesi, con l'aiuto di grandi matematici come Alan Turing e Gordon Welchman, riprogettarono la Bomba e idearono diversi metodi per forzare le chiavi di codifica tedesche, che davano come prodotto il testo in chiaro, noto con il nome in codice Ultra.
Nel maggio del 1941 la marina inglese riuscì a mettere le mani su un apparato Enigma intatto e sui documenti di cifratura, catturando un sommergibile tedesco durante un attacco da parte di quest'ultimo a un convoglio alleato. Questa operazione è conosciuta col nome di Primrose.
Turing fece ricorso ai cosiddetti "crib" (testo in chiaro) e a dei frammenti di testo che egli sapeva sarebbero apparsi nei crittogrammi tedeschi. Per esempio, nei bollettini atmosferici era certo di trovare la parola "tempo", spesso anche nella stessa posizione all'interno del testo cifrato. Un altro metodo era quello di indurre i nazisti a produrre messaggi identici, questa tecnica fu chiamata gardening (planting a crib). Ad esempio, se i tedeschi avevano recentemente bonificato una particolare area dalle mine, l'esercito inglese poteva far credere di aver riminato la stessa zona, in modo che i messaggi nemici contenessero la parola minen (tedesco per mine) ed il nome della località. Sfruttando queste intuizioni, insieme alle concatenazioni matematiche sviluppate da Rajewski, egli riuscì a immaginare un nuovo modello di Bomba, costituita da un gruppo di sessanta macchine Enigma che lavoravano in parallelo. Ciascuna macchina avrebbe controllato 17.576 orientamenti dei meccanismi interni e, alla fine, avrebbe dato un risultato positivo soltanto nel caso in cui la chiave analizzata fosse stata quella esatta.
La bomba di Turing venne effettivamente costruita, ma nelle fasi iniziali si rivelò una delusione, poiché funzionava molto più lentamente del previsto, impiegando una settimana per ciascuna decrittazione.

I tedeschi, nel frattempo, si erano accorti dell'errore nell'uso delle chiavi e avevano rimediato al problema. Lo stratagemma di Turing restava l'ultima speranza per continuare a decifrare i codici nemici.
L'8 agosto 1940, dopo mesi di lavori frenetici, entrò in funzione una versione migliorata della bomba: Agnus Dei, che fu un successo clamoroso. Infatti, in sessanta minuti riusciva a rendere leggibili codici indecifrabili. Date le sue potenzialità, ne furono costruite 15, per poi arrivare a 49 nel 1942. Lo stesso Churchill fu uno dei più grandi sostenitori del progetto, e fino alla fine della guerra gli alleati furono in grado di programmare le loro strategie come fossero stati presenti agli incontri degli alti ufficiali tedeschi.
Il vantaggio strategico derivato dalle intuizioni dei crittoanalisti polacchi prima, e inglesi poi, diede un contributo fondamentale allo sforzo bellico alleato. Sicuramente, senza il loro contributo l'esito del conflitto sarebbe potuto essere molto differente.
Nel 1943 entrò in uso per le comunicazioni tra gli alti comandi tedeschi, una nuova macchina cifrante chiamata macchina di Lorenz SZ40. Successivamente, nel 1944, con lo scopo di decifrare tale macchina, si ebbe un'ulteriore evoluzione della bomba che portò all'introduzione dell'elaboratore Colossus.
Per la marina tedesca venne messa a punto una versione particolare di Enigma, che impiegava 4 rotori cifranti presi da un set di 8 e poteva usare 2 diversi riflettori a scelta, per aumentare ancora il numero di combinazioni disponibili.

4.1 Una nuova analisi del testo cifrato e i crib

Si può assumere che le permutazioni associate ai 5 rotori erano note per merito dei polacchi e la chiave di messaggio non era più ripetuta, per cui rimaneva solo la debolezza strutturale del pannello che era fattorizzabile. L'unico attacco possibile, già realizzato con relativo successo dai polacchi negli ultimi tempi, rimane il plain text attack (crib). L'obbiettivo è quello di individuare la chiave di messaggio (non essendoci più ripetizioni). Poiché gli inglesi avevano un modello funzionante della macchina Enigma, fornito dai polacchi, concentrarono i loro sforzi sul trovare giornalmente la corretta configurazione iniziale; grazie a questa, effettuando delle prove, potevano ottenere porzioni di testo in chiaro, chiamate crib. Avendo i crib e una porzione di testo cifrato, contenente il crib, cercavano di posizionare il crib sul testo cifrato, sfruttando il fatto che la macchina Enigma non cifrava mai un carattere con se stesso.
Consideriamo il seguente esempio:

Testo cifrato:	QFZWRWIVTYRESXBFOGKUHQBAISEZ…
Crib:	WETTERVORHERSAGEBISKAYA

I due frammenti venivano sovrapposti, facendo scorrere il crib di una posizione, finchè nessuna lettera era accoppiata con se stessa.
Di seguito la tabella mostra alcune configurazioni fino ad una accettabile.

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	27	28
Q	F	Z	W	R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B	A	I	S	E	Z
W	E	T	T	E	R	V	O	R	H	E	R	**S**	A	G	E	B	I	S	K	A	Y	A					
	W	E	T	T	E	R	**V**	O	R	H	**E**	R	S	A	G	E	B	I	S	K	A	Y	A				
				W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A	

Poniamo

$$\eta_n = \varphi\, \theta_n\, \varphi$$

ciò è possibile, poiché il pannello è tale che

$$\varphi = \varphi^{-1}$$

ricordando che le η sono trasposizioni generalizzate, quindi, nessuna lettera può essere codificata in se stessa.

5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B	A	I	S	E
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A

$A \xrightarrow{18} G \xrightarrow{19} K \xrightarrow{24} A$
$A = \varphi\, \theta_{18}\, \varphi \bullet G$
$G = \varphi\, \theta_{19}\, \varphi \bullet K$
$K = \varphi\, \theta_{24}\, \varphi \bullet A$
$A = \varphi\, \theta_{18}\, \theta_{19}\, \theta_{24}\, \varphi \bullet A \;\Rightarrow\; \varphi \bullet A = \theta_{18}\, \theta_{19}\, \theta_{24}\, \varphi \bullet A$
$E \xrightarrow{27} A \xrightarrow{25} I \xrightarrow{7} T \xrightarrow{9} E \;\Rightarrow\; \varphi \bullet E = \theta_{27}\, \theta_{25}\, \theta_7\, \theta_9\, \varphi \bullet E$

Si costruisce il *grafo completo*, che ha per nodi le lettere del crib e del corrispondente testo cifrato e per archi le θ; da questo si evidenziano un certo numero di

equazioni al *punto unito* (cioè di cicli).
Il problema analizzato dai polacchi era formulato nelle 3 equazioni relative a tutti i messaggi di un giorno

$$\text{le } \alpha \text{ note} \begin{cases} \theta_4\theta_1 = \alpha_1 \\ \theta_5\theta_2 = \alpha_2 \\ \theta_6\theta_3 = \alpha_3 \end{cases}$$

con gli indici delle θ fissati e i secondi membri dati, poteva essere risolto per tabulazione, partendo dalla chiave del giorno e determinando la caratteristica, funzione di $\alpha_1\ \alpha_2\ \alpha_3$
Il problema impostato dagli inglesi consisteva in un numero variabile di equazioni al *punto unito*, ciascuna con numerose soluzioni, con molti indici per le θ, di volta in volta diversi, e riguardava la chiave di messaggio; pertanto non poteva essere risolto per tabulazione.

$$\begin{gathered} X_1 = \theta_{j_{11}}\ \theta_{j_{12}}\ \ldots\ \theta_{j_{1p}}\ X_1 \\ \ldots \\ X_h = \theta_{j_{h1}}\ \theta_{j_{h2}}\ \ldots\ \theta_{j_{hg}}\ X_h \end{gathered}$$

Viene costruito un sistema elettromeccanico: la Bomba, perfezionamento di quella ideata dai polacchi. Ognuna consisteva in numerose repliche dei 3 rotori di Enigma, 36 nel modello definitivo, che potevano essere variamente collegate mediante un "menù": sostanzialmente un grafo dedotto dal crib.

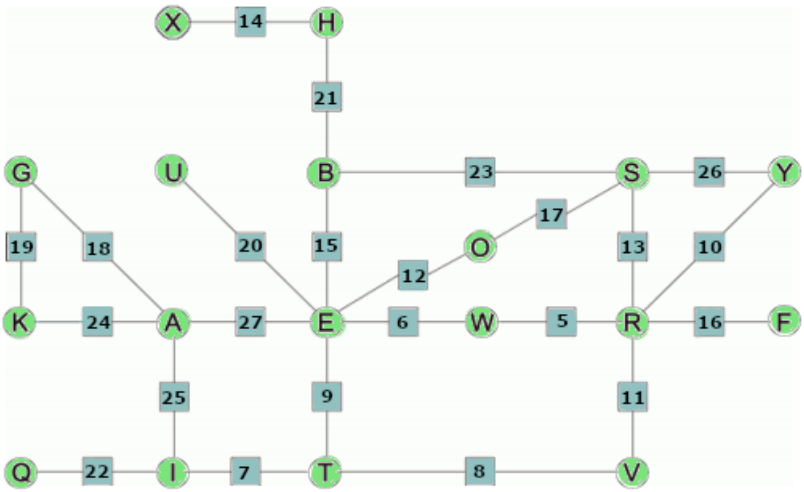


Figura 4.1: Nel menù rappresentato in figura è possibile notare che AGK così come AEIT formano un ciclo, questo ciclo è alla base del lavoro degli inglesi.

Ricordando che la crittazione della macchina Enigma era basata su i seguenti tre passi fondamentali:

- scambio del pannello (φ)
- crittazione dei rotori e del riflettore (θ_n)
- scambio del pannello (φ)

Prendiamo in esame il loop E-A-I-T, come rappresentato in Figura 4.2.
Ipotizziamo che la E sia scambiata dal pannello in K, K cifrata dai rotori in v1 e v1, successivamente, scambiata in A. La A è scambiata dal pannello in v1, v1 cifrata in v2, quindi, scambiata in I. Dunque I viene scambiata in v2, cifrata in v3, scambiata in T. Infine la T è scambiata in v3 che è cifrata in v4 e nel caso in cui v4 non corrisponda a K (che sarebbe scambiata dal pannello in E) la nostra ipotesi iniziale sarebbe errata; di conseguenza l'attuale configurazione dei rotori sarebbe da scartare.
Se escludiamo il lavoro del pannello, sappiamo che K è cifrato in v1, v1 è cifrato in v2, v2 è cifrato in v3 e v3 è cifrato in K, sempre che la nostra ipotesi iniziale sia corretta.

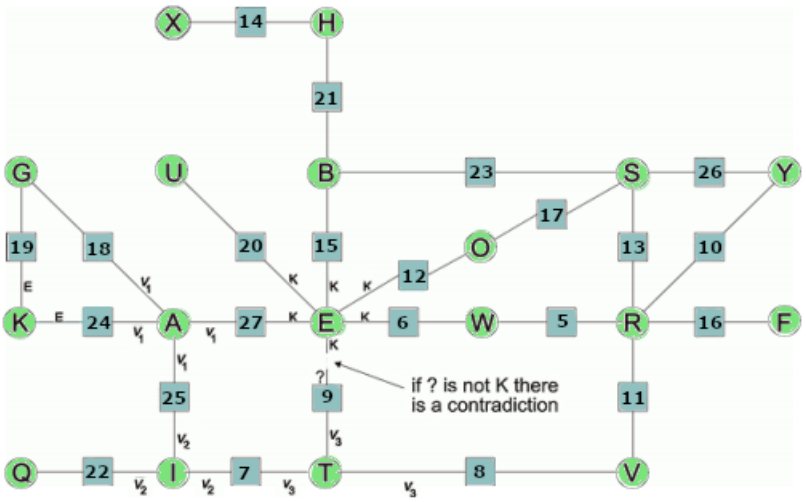


Figura 4.2: Ipotesi in cui la E viene scambiata dal pannello in K, con relativi passaggi

4.2 La Bomba di Turing

La Bomba era una macchina capace di cercare la combinazione corretta dei rotori tra tutte le combinazioni possibili. Era un armadio di una tonnellata di peso, alto oltre due metri, diviso in 3 batterie, ciascuna contenente 12 colonne, di 3 tamburi ciascuna.

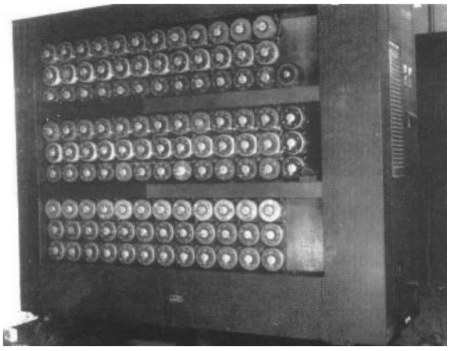


Figura 4.3: Foto della Bomba di Turing

Ogni tamburo rappresentava un rotore, quindi ogni tripletta una intera macchina Enigma. I tamburi ruotavano ad alta velocità, inizialmente 50 giri al minuto (con un "ticchettio", da cui probabilmente deriva l'origine del nome polacco "bomby"). Successivamente la fila superiore di tamburi, di ciascuna batteria, ruotava ad una velocità di 120 giri al minuto (fila corrispondente ai rotori veloci); la fila media ruotava ad ogni rivoluzione completa della prima fila e la fila inferiore ad ogni rivoluzione completa della seconda fila. In pratica 26 fili, ciascuno corrispondente ad una lettera dell'alfabeto, entravano nella fila veloce di tamburi e veniva eseguita la permutazione del primo rotore. La prima fila era collegata con la seconda che eseguiva la permutazione del secondo rotore, la seconda fila era collegata con la terza che eseguiva la permutazione del terzo rotore, quindi lo scambio del riflettore e nuovamente la permutazione del terzo rotore. Dal terzo rotore il segnale elettrico risaliva e subiva nuovamente le permutazioni del secondo e del primo rotore; infine usciva dal primo tamburo.
Turing notò che occasionalmente la stessa coppia chiaro/cifrato di caratteri occorreva più volte in differenti punti del medesimo messaggio. Tale caratteristica venne chiamata "clicks". Ciò era dovuto al fatto che Enigma era reversibile, ovvero la coppia chiaro/cifrato di R,C era la stessa C,R e M,E ed E,M, come riportato in Figura 4.4 (a).

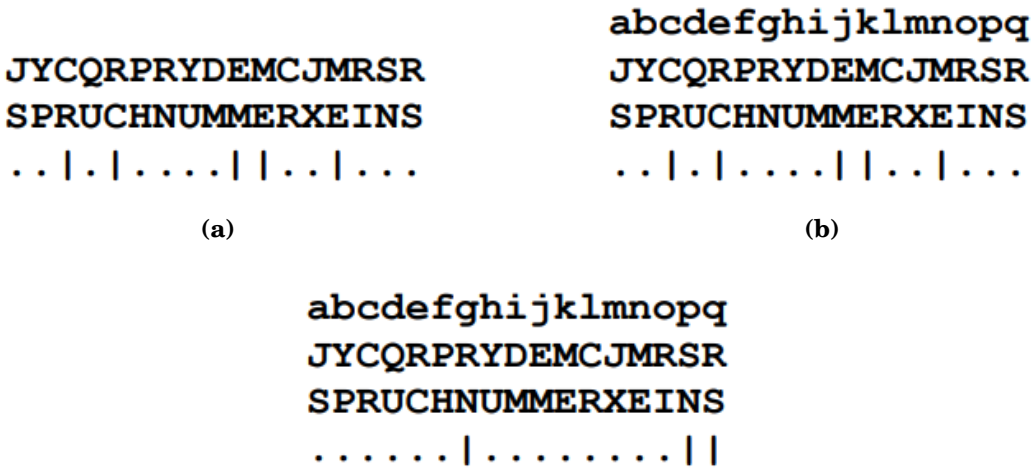


Figura 4.4

L'occorrenza di una coppia è determinata dall'ordine del rotore e dalla posizione iniziale di esso.
Inoltre capì che, l'ordine attuale dei rotori e la loro posizione di partenza, potevano essere trovati provando tutte le configurazioni che soddisfavano la coppia esaminata. Di fatto provare tutte le combinazioni possibili su una sola macchina Enigma una alla volta avrebbe richiesto troppo tempo. Dunque, il passo seguente, fu quello di considerare come il test potesse essere eseguito simultaneamente per una particolare configurazione iniziale della macchina. Il test di ogni coppia di lettere richiedeva un metodo per determinare rapidamente quale configurazione fosse esatta o errata. Ciò si riconduceva al concetto di collegare insieme più macchine Enigma per velocizzare le operazioni di decrittazione. Il risultato fu quello di usare una macchina Enigma "aperta". Questo non era possibile per i tedeschi, a causa della configurazione elettrica di Enigma da loro usata, perché gli ingressi e le uscite che coducevano corrente erano fissati sul rotore. A differenza di tale configurazione, che precludeva ogni possibilità di connessione, nella configurazione aperta ideata da Turing il riflettore aveva due lati. In particolare, quello di uscita era connesso a tre rotori che rappresentavano i percorsi inversi effettuati dalla corrente nella configurazione originale della macchina. Questo metodo dava la possibilità di avere delle connessioni in input/output separate, permettendo, così, di avere più macchine Enigma in serie.
Nella Letchworth Enigma (chiamata così perché la fabbrica British Tabulating Machine, che l'ha costruita, si trovava a Letchworth) l'idea innovativa fu quella di includere entrambi i cablaggi, anteriore e posteriore, dei rotori di Enigma in

un unico tamburo. Le connessioni tra ogni tamburo e il suo successivo avvenivano tramite 4 cerchi, composti da 26 contatti fissati. I 3 set di contatti erano cablati insieme, permanentemente, ai connettori di input/output. I 3 tamburi, rappresentanti i 3 rotori presenti sull'Enigma originale, potevano essere posizionati sull'albero, formando una macchina Enigma in configurazione aperta, con i connettori di input/output separati dagli altri.
Turing decise di indicare con le lettere dell'alfabeto minuscolo ogni coppia di caratteri chiaro/cifrato. In questo modo per la coppia C, R si poteva considerare l'offset da c ad e, mentre per la coppia M, E da j a k e da k a n, come mostrato in Figura 4.4 (b). Il funzionamento era interattivo; infatti, ogni volta che una possibile chiave di messaggio rendeva soddisfatte più equazioni, ciò veniva segnalato per poter effettuare un esame manuale. Ad esempio, alla connessione relativa alla lettera C, dell'Enigma a configurazione aperta veniva applicata una tensione; in questo modo, le 26 lampadine collegate ad essa indicavano se la possibile cifratura fosse esatta. In questo caso si sarebbe dovuta accendere la lampadina relativa alla lettera R. Con una singola macchina Enigma questa operazione avrebbe richiesto un incredibile numero di settaggi. Le macchine Enigma in configurazione aperta erano tutte impostate con lo stesso ordine di tamburi. Tutti i tamburi erano settati nel medesimo modo, tranne l'ultimo che era settato con l'offset della lettera del crib da testare. In questo modo, attraverso un gruppo di relè era possibile fornire un diverso voltaggio in ingresso all'ultimo tamburo di tutte le macchine, così facendo era possibile verificare se l'impostazione dei tamburi soddisfava il crib. Se il risultato era negativo si procedeva a cambiare l'ordine dei tamburi attraverso un motore elettrico.
Un estensione del concetto delle coppie di lettere è il loop di lettere.
In Figura 4.4 (c), si nota che il ciclo RN è in posizione g, NS è in posizione p, SR è in posizione q. Escludendo il pannello, abbiamo R cifrato dalla prima tripletta di tamburi in N, N cifrato dalla seconda tripletta in S e S cifrato nuovamente in R. Se avviene ciò, il ciclo è permanente, cioè l'uscita è connessa all'ingresso, allora la nostra configurazione è corretta.

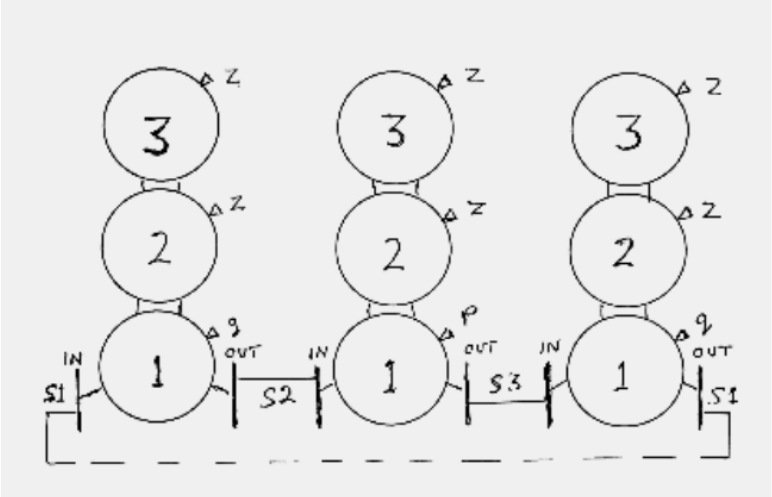


Figura 4.5: Ipotesi in cui la E viene scambiata dal pannello in K, con relativi passaggi

Da notare nel disegno di Turing (Figura 4.5), nella disposizione dei tamburi, la fila superiore (lenta) e la fila intermedia sono sempre impostate a Z, mentre la prima fila (veloce) è impostata, prima a g, poi a p, quindi a q, in accordo alla numerazione (in lettere) assegnata all'accoppiamento crib-cifrato. Le prime due file non cambiano lettera, poiché il secondo rotore gira una volta ogni 26, mentre il terzo rotore una volta ogni 26^2, quindi erano considerati totalmente statici.
Dalla figura si può notare che lo schema rappresenta tre macchine Enigma in configurazione aperta, in cui i tamburi numero 1 sono settati in corrispondenza degli offset S1, S2 e S3, invece i tamburi numero 2 e 3 corrispondono alla configurazione standard dell'Enigma. A questo punto le posizioni dei rotori corrispondono alla posizione originale presente nella macchina Enigma al momento della crittazione. In questo modo il voltaggio di S1 sarà lo stesso in ingresso di S2, mentre il voltaggio di S2 sarà uguale a quello in ingresso di S3, ottenendo la configurazione originale. L'idea sta nel connettere i terminali di uscita dall'ultima macchina in input alla prima. Quest'ultima operazione porterà ad avere un loop tra le macchine, isolando, però, le connessioni S1, S2 e S3. Turing pensò che se S1 era sconosciuto e se gli si fosse applicato un voltaggio casuale, questo avrebbe raggiunto tutte le macchine senza influenzare gli ingressi S1, S2 e S3 dato che essi non erano connessi a nessun terminale. Il test finale consisteva nello spostare i rotori, in modo da vedere se una o 25 lampadine si accendevano; se tutte le lampadine erano accese la posizione era errata. Questo test avveniva in pochissimo tempo, l'unico accorgimento era quello di non surriscaldare i motori che muovevano i tamburi. L'altra idea che ha permesso di perfezionare la Bomba di Turing venne da Gordon Welchman. Egli pensò di costruire dei registri, che opportuna-

mente modificati, potessero riassumere le connessioni tra le macchine Enigma in configurazione aperta. Attraverso un procedimento "diagonale" si poteva risalire in modo agevole alla corrispondenza tra le lettere, in particolare risultava quasi immediata la soluzione nei casi di loop di cifre.
Questo metodo permette di sfruttare anche i "rami" lineari, cioè non ciclici del menù (Figura 4.2).

4.3 La tavola diagonale

La tavola diagonale forniva una schematizzazione del pannello e si basava sul principio di reciprocità di quest'ultimo, se A è scambiato con B, B sarà sempre scambiato con A (Figura 4.6).

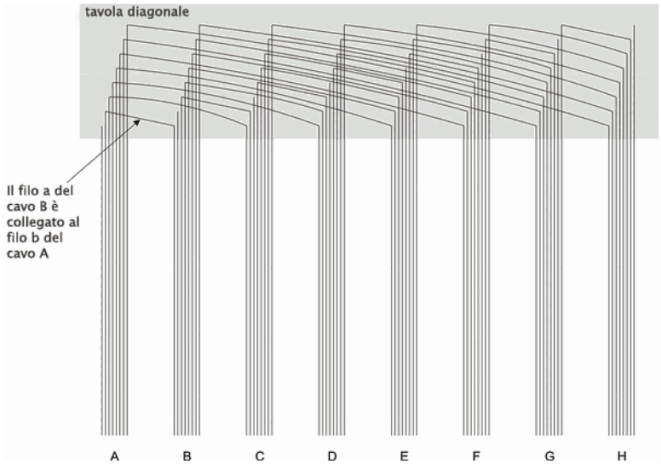


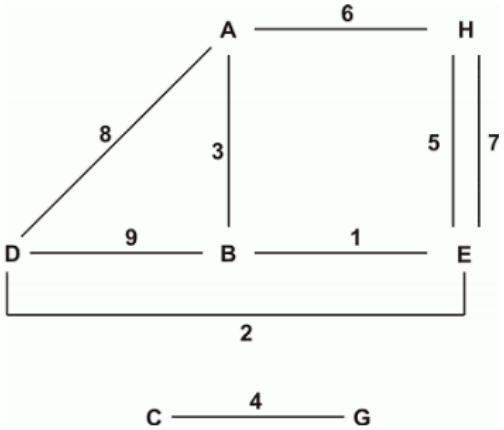
Figura 4.6: Tavola Diagonale

Questa tavola aveva in ingresso 26 cavi, uno per ogni lettera dell'alfabeto, ciascun cavo contenente 26 fili anch'essi corrispondenti ad una lettera dell'alfabeto.
Come si vede nella Figura 4.6 se il filo b del cavo A è collegato con il filo a del cavo B vuol dire che la A è scambiata dal pannello con B e viceversa. Facendo fluire corrente nel filo b del cavo A, questa fluisce anche nel filo a del cavo B.
Per impostare la bomba con la tavola diagonale abbiamo bisogno semplicemente di una coppia crib-cifrato, come visto in precedenza.

Utilizziamo un alfabeto di 8 lettere (A. . . H), per rendere leggibili gli schemi, e le coppie:

1	2	3	4	5	6	7	8	9
B	E	A	C	H	H	E	A	D
E	D	B	G	E	A	H	D	B

il menù corrispondente è:



ora calcoliamo la lettera iniziale di ciascun tamburo

TAMBURO	CAVI CONNESSI DAI TAMBURI	POSIZIONE DELLA COPPIA	LETTERA INIZIALE DEL TAMBURO
veloce	B – E	1	A
veloce	E – D	2	B
veloce	A – B	3	C
veloce	C – G	4	D
veloce	H – E	5	E
veloce	H – A	6	F
veloce	E – H	7	G
veloce	A – D	8	H
veloce	D – B	9	A
medio	D – B	9	B

Ogni riga si riferisce ad una tripletta di tamburi diversa, escluse le ultime due che si riferiscono alla stessa tripletta, infatti hanno la stessa posizione dell'altra coppia.

Nella prima colonna (TAMBURO) è riportato il tipo di tamburo che deve essere posizionato come indicato nella quarta colonna (LETTERA INIZIALE).
Nella seconda colonna (CAVI CONNESSI) sono indicati quali cavi della tavola diagonale la tripletta deve collegare.
Nella terza colonna (POSIZIONE) è riportato l'indice corrispondente nel crib-cifrato alla coppia dei due cavi collegati.
A questo punto si hanno tutte le informazioni per configurare la Bomba:

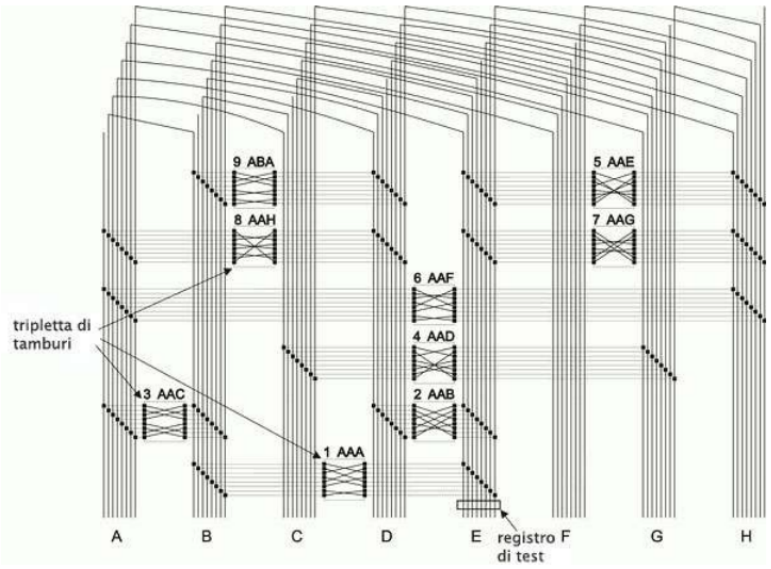


Figura 4.7: Tavola Diagonale configurata

Sul cavo corrispondente alla lettera più frequente era posto un registro di test, in grado di contare il numero di fili in cui c'era corrente (fili vivi). Dopo la configurazione, la Bomba era messa in funzione, facendo fluire corrente su ciascun filo; se il registro di test contava più fili vivi, allora la configurazione era da scartare. La disposizione dei rotori non andava bene se, ad esempio, fluiva corrente nel filo b del cavo A (di conseguenza nel filo a del cavo B), in quanto ciò indicava che A e B erano scambiate dal pannello. Infatti una lettera poteva essere scambiata solo ed esclusivamente con un'altra, perciò se il registro contava più fili vivi, significava che non si aveva uno scambio univoco, quindi una disposizione dei rotori non valida.

Dunque, la macchina veniva stoppata se si aveva una configurazione corretta, ossia quando:

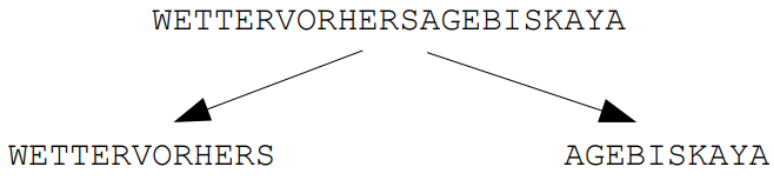
- il registro di test contava un solo filo vivo, configurazione corretta e ipotesi iniziale corretta
- il registro di test contava un solo filo morto, configurazione corretta e ipotesi iniziale errata

4.4 Il problema del secondo rotore

Alla base della bomba c'è la supposizione che il secondo e il terzo rotore siano statici, ma questo effettivamente non è vero.
Con un crib di 23 lettere come:

WETTERVORHERSAGEBISKAYA

abbiamo una probabilità di $\frac{23}{26}$ che il secondo rotore, durante la digitazione del messaggio, giri. Se il secondo rotore cambia posizione tutte le ipotesi cadono e gli attacchi sono del tutto vani. Per sopperire a questo inconveniente, si divide il crib in due, ad esempio:



così il crib è diviso in due testi da 13 e 10 lettere, riducendo il problema del secondo rotore ad uno solo dei due crib (anche se rimane con una probabilità di $\frac{23}{26}$).
In questo modo si risolve l'inconveniente, però si riduce, dividendo il crib, la complessità del menù, rendendo meno efficiente la bomba stessa.

In conclusione, modello definitivo della Bomba esaminava in 11 minuti le ($17575 = 26^3$) chiavi per una scelta di 3 rotori su 5 e una loro disposizione.
Verso la fine della guerra erano operative circa 200 bombe, dislocate in vari luoghi. Circa un egual numero fu costruito dalla marina USA per decifrare la macchina Enigma utilizzata dalla marina, a 4 rotori.
Sporadicamente si usavano ancora metodi tabellari, come per esempio la tabella per EINS (uno in tedesco) per "tutte" le chiavi e "tutte" le posizioni nel messaggio.

Conclusioni

Dall'approfondimento svolto si comprende come parallelamente ad una guerra combattuta con armi ed eserciti ci sia stata una guerra silenziosa, determinante per la sconfitta dei tedeschi, svolta da menti geniali, le cui armi erano le abilità deduttive, l'immaginazione e la creatività. Senza tali menti, probabilmente, la guerra si sarebbe protratta per più anni e sarebbe stata ancor più logorante.
Inoltre, gli studi svolti per giungere a costruire congegni e tecniche finalizzati alla decrittazione della macchina Enigma, hanno portato al progresso nella realizzazione di tecniche e modelli generali.
È importante sottolineare come la compilazione del manuale, di 180.000 voci realizzato dai polacchi per decifrare la macchina Enigma, rappresenti l'ultimo grande sforzo nel compiere calcoli manuali.
Tutto ciò ha permesso l'avanzamento della tecnologia e delle teorie alla base della moderna informatica.
Infatti si può ritenere che i congegni di decifrazione siano dei precusori dei modelli di calcolatori moderni.
Lo sviluppo della tesi mostra che l'avanzamento dei modelli raggiunti non ha seguito un percorso lineare, ma, nel corso degli anni, si è più volte tornati su problematiche affrontate in precedenza per ricercare nuove soluzioni.
Al giorno d'oggi è difficile pensare di poter vivere senza il computer e le tecniche di criptazione. Basti pensare come le tecniche di cifrazione si sono evolute fino ad essere usate nei sistemi moderni di sicurezza bancaria, alla base di tutte le transazioni finanziarie.
Seppure inconsapevolmente, la crittografia è diventata una componente fondamentale della vita quotidiana; infatti, viene utilizzata quando parliamo al cellulare o accediamo ad una rete wireless, pittusto che, quando utilizziamo il bancomat o facciamo acquisti sul web o guardiamo la pay-tv.
Il merito delle tecniche di decifrazione, nel corso della storia, è stato quello di rendere sicuro ciò che semplici metodi, come porte o buste chiuse, non erano più in grado di proteggere.

RIFERIMENTI BIBLIOGRAFICI E SITOGRAFICI

[1] David Kahn, *Seizing the enigma: The race to break the German U-boat codes, 1939-1943*, Barnes & Noble Books, 1991.

[2] Simon Singh, *Codici & segreti*, Milano, Ed. Rizzoli, 1999.

[3] Tuono Pettinato e Francesca Riccioni, *Enigma-La strana vita di Alan Turing*, Ed. Rizzoli Lizard, 2012.

[4] Rita Procesi Ciampi, *Lezioni di Algebra*.

[5] *Algebra 2*, http://www.dmf.unisalento.it/~scienze/Download/algebra_2new.pdf .

[6] Marilena Barnabei, *Combinatoria delle permutazioni*, https://www.researchgate.net/publication/242451774_Combinatoria_delle_permutazioni .

[7] Marian Rejewski, *An Application of the Theory of Permutations in Breaking the Enigma Cipher*, https://cryptocellar.org/Enigma/rew80.pdf .

[8] Władysław Kozaczuk, *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*, Frederick, MD, University Publications of America, 1984, pag. 243–44.

[9] *La Bomba di Turing*, http://www.dia.uniroma3.it/~dispense/rota/La_bomba.pdf .

[10] *La Bomba di Turing o Colossus*, http://www.apav.it/sitostudenti/sito%20giur/federica/turing.htm .

RINGRAZIAMENTI

Un ringraziamento al mio relatore Prof. Giorgio Casadei ed al correlatore Prof. Antonio Teolis per la disponibilità e il materiale fornito.

Grazie alla mia famiglia che mi ha sempre supportato e sopportato, aspettando da tempo questo traguardo insieme a me.

Ringrazio particolarmente mio fratello per i consigli nella stesura della tesi.

Grazie a mia sorella per non avermi mai fatto arrendere durante il percorso universitario.

Grazie a Luciana che mi ha aiutato in un momento difficile e mi ha fatto capire di potercela fare, facendomi ritrovare l'entusiasmo perso.

Grazie per il supporto ricevuto da Vito, con cui ho condiviso gran parte della mia esperienza a Bologna in questi anni e un'amicizia che dura sin dall'infanzia e, se pur con qualche piccola difficoltà, è rinata e si è rafforzata. Grazie anche per l'ospitalità offertami da lui ed Emanuele.

Grazie per il sostegno ricevuto da David, con il quale ho trascorso la quotidianità e senza il quale alcune giornate sarebbero state sicuramente più pesanti.

Ringrazio Luigi e i miei amici che mi sono stati sempre vicini e che con ironia e umorismo hanno contribuito alla mia serenità, perché anche loro sono sempre stati fiduciosi nei miei confronti.

Grazie a tutti voi di cuore.