

# Enigma

a cura di: Zecca Alfonso

## 1 - Introduzione

- Enigma era una macchina cifratrice utilizzata dal Terzo Reich negli anni precedenti e durante la Seconda Guerra Mondiale
- Lo scopo era quello di rendere il più possibile sicure le comunicazioni segrete
- Utilizzata per "mascherare" un messaggio
- Chiunque intercettava il messaggio non era in grado di sapere che cosa diceva

## 1 - Introduzione

AKRJ  
+  
key(cifrata)



CIAO  
+  
key



Operatore 1



CIAO  
+  
key



Operatore 2

## 1 - Introduzione

- La macchina era costituita da diversi elementi relativamente semplici se presi singolarmente
- Costituivano insieme un potente apparato per la produzione di scritture cifrate

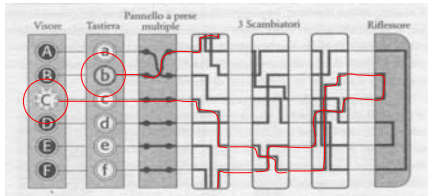
## 1.1 - Funzionamento



## 1.1 - Funzionamento

- Versione base del dispositivo (1918): tre componenti collegati tra loro con fili elettrici
  - tastiera per immettere le lettere del testo in chiaro
  - unità scambiatrice che cifra la lettera trasformandola nel corrispondente elemento del crittogramma
  - visore con varie lampadine: illuminandosi indicano la lettera da inserire nel testo cifrato

## 1.1 - Funzionamento



## 1.1 - Funzionamento

- La parte più importante della macchina è lo scambiatore (o rotore)
- Consiste in uno spesso disco di gomma attraversato da una fitta rete di fili provenienti dalla tastiera

## 1.1 - Funzionamento



## 1.1 - Funzionamento

- I fili entrano nello scambiatore e, dopo un percorso formato da vari gomiti, emergono dalla parte opposta
- Lo schema interno dello scambiatore determina un alfabeto cifrante utilizzabile per una semplice cifratura a sostituzione monoalfabetica

## 1.1 - Funzionamento

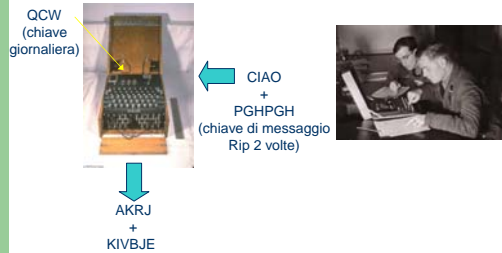
- Il disco del primo scambiatore ruota di un ventiseiesimo di giro dopo la cifratura di ogni lettera
- L'alfabeto cifrante cambia dopo ogni lettera
- Da cifratura monoalfabetica a polialfabetica

## 1.1 - Funzionamento

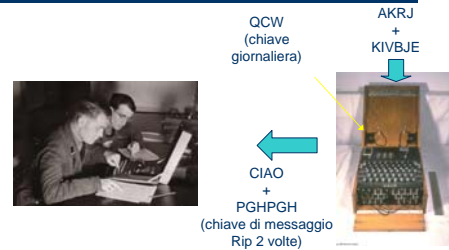
- Il meccanismo presenta il problema della ripetizione
- Comunemente sinonimo di cifratura debole
- Per superarlo vennero introdotti un secondo e un terzo scambiatore



## 1.1 - Funzionamento



## 1.1 - Funzionamento



## 1.1 - Funzionamento

- La sicurezza di Enigma -> elevato numero di combinazioni da controllare per ottenere l'assetto iniziale
- Infatti:
  - controllando una chiave al minuto
  - lavorando giorno e notte
  - circa due settimane per scoprire la chiave di un solo giorno

## 1.1 - Funzionamento

- Due nuove caratteristiche aggiunte in seguito
- Scambiatori rimovibili in modo da poterli scambiare tra loro
- Numero di chiavi aumentato di un fattore pari a 6 (poiché 3 elementi intercambiabili possono essere combinati in 6 modi diversi)

## 1.1 - Funzionamento

- Inserimento di un pannello a prese multiple tra la tastiera e il primo rotore
- Permetteva al mittente di inserire alcuni cavi muniti di spinotti
- Scambiavano due lettere prima della loro immissione nel rotore
- Sei cavi per sei coppie di lettere

## 1.1 - Funzionamento



Pannello a prese multiple

## 1.1 - Funzionamento

Gebiets  
Hilfs für Platten annehmen!

Sonder-Maschinenschlüssel BGT

Datum	Wahrsager	Einrichtung	Stückzahl	Gruppen
21.	I V IIII	06 20 24	0A PF QG RN RI RY RG RL RX ZJ	Jeu nre aqr
22.	V II IIII	01 07 12	OP XV YH ZB CW UX VA 2H	aaa adf bch
23.	IV I V	11 17 22	CT OK PV ZL NX EB AF DJ FE ST	kaf awh lyp

Diagram labels:

- Giorno del mese
- Scambiatori utilizzati
- Assetto degli scambiatori
- Connessioni del pannello a prese multiple

## 1.1 - Funzionamento

- Combinando insieme tutti gli elementi fin qui osservati si può calcolare il numero di chiavi che Enigma poteva impiegare:

- Gli scambiatori (o rotori) potevano orientarsi ognuno in 26 modi nel piano perpendicolare all'asse di rotazione
- generavano  $26 \times 26 \times 26 = 17.576$  combinazioni

## 1.1 - Funzionamento

- Tre scambiatori potevano essere inseriti in diverse posizioni reciproche:
  - 123, 132, 213, 231, 312, 321
- Erano quindi ammesse 6 diverse posizioni reciproche dei rotori

## 1.1 - Funzionamento

- Con il pannello a prese multiple i possibili abbinamenti di 12 (6x2) lettere su 26 sono 100.391.791.500
- Il numero totale di chiavi si ottiene moltiplicando tra loro le suddette possibilità:  $17.576 \times 6 \times 100.391.791.500 = 10.586.916.764.424.000$

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- 1926. Soltanto un ufficio chiamato Biuro Szyfrow - l'ufficio cifre polacco - continuò a funzionare a pieno regime dopo Enigma
- Questo ufficio possedeva una versione commerciale della macchina
- Nessuna utilità per risolvere le comunicazioni militari

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Novembre del 1931: Hans-Thilo Schmidt - un impiegato dell'ufficio amministrativo preposto alle comunicazioni crittate militari - fornì ad una spia francese (nome in codice Rex) le foto di due manuali di istruzioni per la cifratrice
- Questo permise la riproduzione della versione militare della macchina

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- I tedeschi introdussero una nuova chiave per ogni messaggio - chiave di messaggio - oltre alla chiave giornaliera
- Veniva trasmessa usando l'assetto indicato dalla chiave giornaliera
- Ripetuta due volte di seguito
- Usata per regolare il nuovo assetto della macchina per il singolo messaggio

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- A causa della natura elettromeccanica di Enigma i responsabili del Biuro Szyfrow decisero di reclutare dei matematici
- Il più brillante era senza dubbio il giovane Marian Rejewski

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Rejewski si basò sulle ripetizioni
- Chiave di messaggio cifrata due volte di seguito all'inizio di ogni comunicazione
- La prima e la quarta lettera erano legate strettamente alla posizione degli scambiatori così come la seconda e la quinta e la terza e la sesta
- Tabella delle corrispondenze

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Poniamo per esempio che venissero ricevuti i seguenti quattro messaggi (ne consideriamo solo le prime sei lettere):
  - L O K R G M
  - M V T X Z E
  - J K T M P E
  - D V Y P Z X

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Considerando le prime e quarte lettere di ciascun esagramma crittato si poteva costruire una prima tabella:

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

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

Concatenazioni: Numero di collegamenti:

- A -> F -> W -> A 3
- B -> Q -> Z -> K -> V -> E -> L -> R -> I -> B 9
- C -> H -> G -> O -> Y -> D -> P -> C 7
- J -> M -> X -> S -> T -> N -> U -> J 7

- Ovviamente questo lavoro andava ripetuto per le altre coppie di lettere dell'esagramma

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Queste concatenazioni dipendevano in modo complesso:
  - dai collegamenti del pannello a prese multiple
  - dalla collocazione degli scambiatori
  - dall'assetto degli scambiatori
- Possibilità da vagliare non ridotte

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Gli effetti del pannello e quelli degli scambiatori sulle concatenazioni potevano essere separati
- In particolare Rejewski notò che il numero di collegamenti dipende esclusivamente dagli scambiatori

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- S e G scambiate dal pannello a prese multiple. Se usiamo il cavetto di S e G per scambiare ad esempio T e K otteniamo:
- Concatenazioni: 

	Numero di collegamenti:
A -> F -> W -> A	3
B -> Q -> Z -> T -> V -> E -> L -> R -> I -> B	9
C -> H -> S -> O -> Y -> D -> P -> C	7
J -> M -> X -> G -> K -> N -> U -> J	7
- Notiamo che alcune lettere sono cambiate, ma il numero di collegamenti è rimasto invariato

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Ridotte in maniera molto significativa il numero di possibili combinazioni da controllare per trovare la chiave giornaliera
- Non scoprire una chiave tra dieci milioni di miliardi
- Ma quale assetto degli scambiatori avesse generato le concatenazioni osservate

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Numero di assetti da verificare:
  - prodotto delle possibili collocazioni negli alloggiamenti (6) e dei possibili orientamenti (17.576), quindi 105.456
- Si riuscì a compilare un repertorio contenente tutte le possibili lunghezze delle concatenazioni e i relativi assetti degli scambiatori

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Messaggi non totalmente in chiaro a causa degli scambi di lettera effettuati dal pannello a prese multiple
- Escludendo il pannello sulle repliche della macchina una parte del messaggio (quella che conteneva lettere non scambiate dal pannello) era quasi comprensibile
- Perciò non risultava difficile trovare le lettere da collegare con i cavi del pannello a prese multiple

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Rejewski riuscì a progettare un congegno che automatizzava la ricerca della chiave giornaliera
- Controllava rapidamente le 17.576 combinazioni per trovare le posizioni dei rotori

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Questi congegni erano chiamati "bombe"
- Poiché gli scambiatori potevano essere posti in sei posizioni diverse occorrevano sei "bombe" che funzionavano in parallelo
- Enigma = automazione del processo di cifratura
- "bombe" di Rejewski = automatismo della decifrazione

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- 1938: introduzione di nuove misure per aumentare la sicurezza della macchina:
  - due nuovi scambiatori
  - numero di cavetti del pannello a prese multiple passò da sei a dieci

## 2 - Guerra ad Enigma: i crittoanalisti polacchi

- Numero delle possibili collocazioni negli alloggiamenti dei rotori passava da sei a 60
- Le lettere scambiate dal pannello a prese multiple passavano da dodici a venti su ventisei
- Numero di possibili chiavi = 159 miliardi di miliardi!

## 3 - Bletchley Park

- Attorno alla metà del 1939 i polacchi trasferirono il loro materiale in Inghilterra e più precisamente in un palazzo nel Buckinghamshire che si chiamava Bletchley Park ed era la sede della Government Code and Cypher School (GC&CS)

## 3 - Bletchley Park

- "cillies" per scoprire la chiave giornaliera
- Un "cilly" non era una imperfezione di Enigma, ma derivava dal modo in cui veniva usata
- Tre lettere adiacenti sulla tastiera
- Le iniziali di una fidanzata

### 3 - Bletchley Park

- Limitazioni al numero di chiavi stesse
  - Nessuno scambiatore poteva occupare la stessa posizione per due giorni consecutivi

### 3 - Bletchley Park

- Ogni lettera non poteva essere scambiata con quella che la precede e la segue (ad esempio S non andava scambiata con R o T)
- Riduzione del cinquanta per cento del numero di disposizioni degli scambiatori

### 3 - Bletchley Park

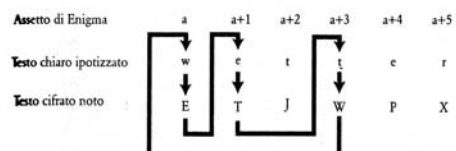
- Alan Turing
- Molti dei messaggi che venivano intercettati avevano una struttura piuttosto rigida
- Messaggi che venivano trasmessi periodicamente (come ad esempio i bollettini meteorologici) avevano le stesse parole nelle stesse posizioni fisse

### 3 - Bletchley Park

- Questo costituiva ciò che in gergo dei crittoanalisti viene definito un "crib"
- Frammento del testo in chiaro che può essere dedotto in base a considerazioni non crittoanalitiche

### 3 - Bletchley Park

- Nella figura è mostrato un possibile crib e la sua concatenazione



### 3 - Bletchley Park

- Analizzando la concatenazione possiamo dire che:
  - Nell'assetto a, Enigma cifra **w** come **E**
  - Nell'assetto a+1, Enigma cifra **e** come **T**
  - Nell'assetto a+3, Enigma cifra **t** come **W**

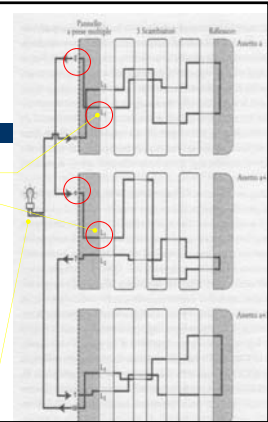
### 3 - Bletchley Park

- Turing progettò un circuito elettrico che collegava tre macchine Enigma con cavi posti tra l'input di una macchina e l'output della successiva
- Procedimento di verifica automatizzato

### 3 - Bletchley Park

- circuito annulla gli effetti del pannello a prese multiple
- collegare l'output del primo gruppo di scambiatori con l'input del secondo gruppo in corrispondenza di L1 (sconosciuto)

Lampadina che evidenzia chiusura circuito



### 3 - Bletchley Park

- Poiché questo valore (L1) non era noto era necessario collegare le 26 uscite del primo gruppo di scambiatori con i 26 ingressi del secondo formando 26 circuiti, ciascuno dotato di una lampadina per evidenziarne la chiusura
- Se scambiatori mutavano orientamento ogni secondo -> operazione completa di controllo di tutti gli orientamenti impiega 5 ore

### 3 - Bletchley Park

- 5 scambiatori
- Le cifratici ne contenevano tre con 60 combinazioni
- Necessari 60 gruppi di tre macchine da far lavorare in parallelo per controllare tutte le disposizioni degli scambiatori

### 4 - La sfida più ardua: Enigma Navale

- Enigma Navale - versione modificata della macchina adottata soltanto dalla Kriegsmarine
- Decisiva per le sorti della battaglia dell'Atlantico
- La difficoltà stava nel sistema di indicatori
  - Due gruppi di 4 lettere di ciascun messaggio
  - Descrive la posizione dei rotori rispetto alla "finestra"
- Unico per la Marina Tedesca
- Basato su sostituzioni di digrammi e trigrammi

### 4.1 - Sommario del funzionamento di Enigma

- "reciprocità": se A -> J allora j -> A nella stessa posizione del rotore
- "non-collisione": A non poteva essere cifrata come A
- Tacche di rotazione sui rotori dell'alfabeto
  - Anelli dell'alfabeto in posizioni differenti rispetto al nucleo del rotore
  - Rotori differivano anche nel punto che trasmetteva il movimento al rotore successivo
  - A seconda del numero del rotore il dentello che trasmetteva il movimento si trovava in corrispondenza di una lettera diversa

## 4.1 - Sommario del funzionamento di Enigma

- Rima usata a Bletchley Park per ricordare la corrispondenza tra numero dei rotori e posizione del dentello (data dalla lettera che appariva nella finestra della macchina):
- **.(R)oyal (F)lags (W)ave (K)ings (A)bove.  
..I.....II.....III.....IV.....V.**
- Questo era un errore. Tutti i rotori avrebbero dovuto avere gli stessi punti di rotazione
- Con punti di rotazione differenti i rotori potevano essere identificati

## 4.1 - Sommario del funzionamento di Enigma

- I rotori 6,7 e 8 furono aggiunti dalla Marina Tedesca. Tutti avevano due punti di rotazione che erano gli stessi per ciascuno di essi
- Sempre la stessa lettera nella finestra

### 4.1.1 - Nascondere la chiave di messaggio

- Due metodi per nascondere la chiave di messaggio ad un eventuale nemico:
- La macchina Enigma stessa
  - Uso di una chiave di messaggio ripetuta due volte, cifrata con la chiave giornaliera e inserita all'inizio del messaggio stesso

### 4.1.1 - Nascondere la chiave di messaggio

- codificare la chiave di messaggio basandosi su sostituzioni di bigrammi
  - Il sistema prevedeva di:
    - selezionare un trigramma da un libro (il Kennbuch, o K Book)
    - cifrare questo trigramma con la chiave Grund (vedi paragrafo successivo)
    - effettuare una sostituzione di bigramma sul trigramma e trasmettere il risultato come intestazione del messaggio
    - Il destinatario compiva la sostituzione inversa del bigramma ottenendo il trigramma originale dal quale poteva ricavare anche la chiave di messaggio decifrandolo con la chiave Grund

## 4.2 - La chiave giornaliera (Tagschlüssel)

- Disposizione degli scambiatori
  - I numeri dei rotori che dovevano essere sistemati nella macchina da sinistra a destra
  - 336 possibilità con 8 rotori, ridotte dalle regole dell'inclusione di almeno uno tra i rotori numerati 6, 7 o 8

## 4.2 - La chiave giornaliera (Tagschlüssel)

- Ringstellung (Assetto delle ruote)
  - per ciascun rotore, da sinistra a destra (17.576 combinazioni)
  - La disposizione degli scambiatori e il Ringstellung cambiavano ogni due giorni
  - L'assetto del pannello a prese multiple e il Grundstellung cambiavano ogni giorno

## 4.2 - La chiave giornaliera (Tagschlüssel)

- Assetto del pannello a prese multiple
  - Di solito si scambiavano dieci paia di lettere
- Grundstellung(Grund)
  - Era costituito dalle tre (o quattro) lettere che mostravano la posizione dei rotori da usare per cifrare la chiave di messaggio

## 4.2.1 - Usare il K Book e le tavole dei bigrammi

- Scegliere un trigramma dal K Book, poniamo YLA
- Cercare nella Zuteilungliste quali colonne del K Book sono allocate a questa chiave particolare ( Acque Territoriali, U-Boat, ecc)
- Selezionare un altro trigramma (il Schlüssel Kennguppe), poniamo YVT

## 4.2.2 - Il foglio di messaggio

- Si scriveva nei rettangoli nella parte superiore del foglio per messaggio:

. Y V T  
Y L A .

- Si sostituiva ai punti lettere qualsiasi, poniamo

Q Y V T  
Y L A G

## 4.2.2 - Il foglio di messaggio

- A questo punto si cercano le coppie verticali di lettere nella tavola dei bigrammi, scrivendo le coppie risultanti

**UB LK RS PW**

- Queste sono trasmesse come due gruppi di quattro lettere all'inizio e alla fine del messaggio cifrato

## 4.3 - Il problema degli intercettatori

- **Risolvere le tavole dei bigrammi**
  - Questa fase doveva cominciare con un "assaggio", cioè il recupero di un gruppo di tavole
- Una volta iniziata la decifrazione dei messaggi, si poteva ricostruire nuove tavole
- Cambiate quasi una volta all'anno

## 4.3 - Il problema degli intercettatori

- **Recuperare la chiave giornaliera**
  - disposizione degli scambiatori
  - Grund (assetto iniziale dei rotori)
  - 336 disposizioni
  - $(26)^3$  o  $(26)^4$  posizioni iniziali diverse
  - totale di 150.000.000 combinazioni da esaminare

#### 4.3.1 - Prove per trovare gli assetti della macchina

- **Cribs**
  - Ipotesi fatta su una parte del testo in chiaro che era cifrato in modo da dare il testo cifrato catturato
  - Messaggi standardizzati
  - Cifrature ripetute dello stesso messaggio con chiavi diverse
  - Lunghezza del messaggio
  - Provenienza del messaggio
  - Tempo di partenza del messaggio

#### 4.3.1 - Prove per trovare gli assetti della macchina

##### **Banburismo (banburismus)**

- Sfruttare l'errore di mettere le tacche di rotazione in posizioni differenti su ogni scambiatore
- La rotazione poteva non verificarsi in certi campi sull'alfabeto input
- Certi rotori non potevano trovarsi sul lato destro

#### 4.3.1 - Prove per trovare gli assetti della macchina

- Disponendo delle tavole dei bigrammi i crittoanalisti avevano il trigramma che rappresentava l'assetto della chiave di messaggio cifrata
- Non conoscevano la chiave di messaggio originale, ma ne conoscevano la cifratura col Grund

#### 4.3.1 - Prove per trovare gli assetti della macchina

- Tutte le cifrature iniziavano col Grund
- La stessa lettera nello stesso posto in una coppia di chiavi di messaggio cifrate => le lettere della chiave di messaggio cercata dovevano essere le stesse

#### 4.3.1 - Prove per trovare gli assetti della macchina

- Se i trigrammi differivano solo nell'ultima lettera - > inizi del messaggio dovevano differire solo nell'ultima lettera
- Se si hanno due lunghezze di testo cifrato

#### 4.3.1 - Prove per trovare gli assetti della macchina

- Dai trigrammi si può pensare che siano state cifrate con lo stesso assetto dei rotori
- Banburismo ci permette di trovare la differenza negli assetti iniziali dei due testi

#### 4.3.1 - Prove per trovare gli assetti della macchina

- Questo funziona perché la distribuzione delle lettere del testo non era completamente casuale
- Se due messaggi iniziano in due punti di cifratura diversi, ad un certo punto nei messaggi si presenterà la stessa lettera
- Tale lettera verrà cifrata da Enigma nello stesso modo

#### 4.3.1 - Prove per trovare gli assetti della macchina

- Buona probabilità di trovare lettere corrispondenti quando i due testi cifrati sono allineati in base alla differenza tra le posizioni dei due rotori più a destra
- Bambury Sheets

#### 4.3.1 - Prove per trovare gli assetti della macchina

- Fissare i due testi cifrati su due fogli diversi
- Far scorrere i fogli uno sull'altro
- Contare i buchi che si sovrapponevano fino ad ottenere le posizioni corrispondenti alla differenza tra gli assetti

#### 4.4 - La procedura del Banburismo

- Il Banburismo dipende dalle tavole di bigrammi ricostruite o catturate
- Vennero raccolte 24 ore di intercettazioni
- Le tavole vennero usate per decodificare le coppie di trigrammi nei due gruppi da quattro lettere dell'inizio dei messaggi

#### 4.4 - La procedura del Banburismo

- Il secondo di questi due, l'indicatore, era quello che l'operatore tedesco destinatario digitava nella sua macchina Enigma, impostata secondo il Grund del giorno, per ricavare l'assetto da usare per il resto del messaggio
- I crittoanalisti non sapevano qual'era il Grund, ma avevano l'indicatore

#### 4.4 - La procedura del Banburismo

- Dimostrazione di come il Banburismo funzionava
- Assetti hanno la stessa lettera iniziale e una limitazione nella lettera intermedia

#### 4.4 - La procedura del Banburismo

- Questo esempio parte da 36 testi cifrati appartenenti alle trasmissioni degli U-boat del 29 luglio 1941
- Isolando solo le coppie di messaggi i cui indicatori davano una corrispondenza massima si ottiene la seguente lista che riporta le coppie di messaggi, gli indicatori e gli offset

#### 4.4 - La procedura del Banburismo

- L'interpretazione che i crittoanalisti usavano seguiva la regola secondo la quale il primo indicatore più l'offset restituisce il secondo indicatore
- 01,14 DXL + 26 = DIL  
01,15 DXL + 28 = DIO  
02,05 DXO + 6 = DXE  
02,06 DXO + 8 = DXW  
02,08 DXO + 12 = DXZ  
02,14 DXO + 24 = DIL  
03,06 DXI + 6 = DXW  
03,14 DXI + 22 = DIL  
03,21 DXI + 36 = DIC  
04,28 DXZ + 48 = DAO  
05,06 DXE + 2 = DXW  
05,14 DXE + 18 = DIL  
05,21 DXE + 32 = DIC  
06,07 DXW + 2 = DXD  
.....
- Ad ogni offset maggiore di 26 si può sottrarre 26

#### 4.4 - La procedura del Banburismo

- Nella seconda coppia, 01,15 , l'offset 28 è interpretato come le lettere centrali dell'indicatore sono cifrate in due lettere adiacenti mentre le terze lettere sono cifrate in due lettere con offset 2
- O<-6->E in 02,05 (che significa che O ed E sono cifrate in lettere con offset 6)  
E<-2->W in 05,14  
O<-8->W in 02,06

#### 4.4 - La procedura del Banburismo

- Questo può essere rappresentato nel modo seguente:  
O<-6->E<-2->W  
O<-.....8.....->W
- In questo modo può essere costruita l'intera rete degli offset per la maggior parte delle profondità, ricordando che la direzione degli offset può essere anche negativa e modulo 26 (ad esempio 26-offset)
- Il risultato, che si potrebbe verificare con un po' di pazienza, è:  
R<-2->K<-4->L<-2->O<-2->I<-2->Z<-2->E<-2->D<-2->W<-2->C

#### 4.4 - La procedura del Banburismo

- Quello che resta da fare a questo punto è trovare le lettere assolute per l'indicatore
- Scrivere le lettere trovate sopra, con la giusta spaziatura, su dei fogli che andrebbero fatti scorrere sotto un alfabeto ripetuto più volte cercando di trovare una posizione del foglio in cui non si rilevano contraddizioni o sovrapposizioni

PQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABC  
.....R.K...L.O.I.Z.E.D.W.C.

#### 4.4 - La procedura del Banburismo

- In questo modo si ricostruisce un alfabeto parziale per il rotore più a destra di Enigma con assetto Grund+2
- Identifichiamo il terzo rotore come il numero 1 poiché è l'unico rotore la cui rotazione ( R ) cade al di fuori del campo compreso tra U e O

#### 4.4 - La procedura del Banburismo

- Così si riusciva a scoprire il numero del terzo rotore con certezza e spesso si poteva trovare anche quello del rotore centrale
- Numero di disposizioni dei rotori ridotto da 336 a soltanto 20

#### 4.5 - L'Enigma con 4 scambiatori

- Febbraio 1942: Shark ( nome in codice della versione navale di Enigma) introdusse una chiave del tutto diversa
- Un nuovo scambiatore, il quarto, era stato inserito nella macchina

#### 4.5 - L'Enigma con 4 scambiatori

- Le caratteristiche principali della nuova versione erano:
  1. due tipi di quarto rotore, Beta e Gamma
  2. due riflessori, Bruno e Ceasar
  3. qualsiasi combinazione poteva essere utilizzata
  4. una combinazione veniva impiegata per un mese
  5. Beta e Gamma erano sempre settati a Z
  6. il quarto rotore poteva essere posto in una qualsiasi delle 26 posizioni, ma non ruotava durante il messaggio
  7. con il quarto scambiatore posto in A, con Beta/Bruno o Gamma/Ceasar, la macchina era equivalente ad una versione con tre rotori
  8. il numero di posizioni iniziali ora è:  $(26)^4 = 456.976$

#### 4.6 - U 559

- Il 30 ottobre 1942 venne intercettato un U-boat nel Mediterraneo dell'est nel quale vennero recuperati degli importanti documenti
- Documenti trovati :
  - Libro Delle Abbreviazioni Meteorologiche (Wetterkurzschlussel)
  - Libro per le Segnalazioni Rapide

#### 4.6 - U 559

- Infatti il Servizio Meteorologico aveva bisogno dei rapporti meteo che gli venivano forniti dai sommergibili
- Dovevano momentaneamente impiegare Enigma con un assetto adatto anche alle macchine con tre rotori

#### 4.6 - U 559

- Codificate e spedite delle abbreviazioni in cui si condensava il contenuto del rapporto richiesto dal Centro Meteo
- Le abbreviazioni erano conservate in un libro
- Wetterkurzschlussel
- Edizione del 1941 catturata con l'U 559

#### 4.6 - U 559

- Centro Meteo trasmetteva una sinottica generale nel loro codice meteo che usava il codice standard internazionale
- Cifrata con le tavole di bigrammi
- Questa sinottica venne decodificata a Bletchley e da essa si conoscevano le condizioni meteo in cui gli U-boat si trovavano
- Si potevano dedurre le osservazioni dei sommergibili

#### 4.6 - U 559

- Dalla cattura del libro dei codici dell'U 559, i crittoanalisti poterono risolvere i codici meteo inseriti dall'operatore Enigma per fornire il segnale intercettato dagli Alleati
- Questo forniva un prezioso crib da usare con le bombe tradizionali a tre rotori e che poteva facilmente fornire una configurazione della macchina

#### 4.7 - I segnali di contatto degli U-boat

- Nel 1943 una nuova battuta d'arresto per Bletchley Park venne dal cambiamento del Libro delle Abbreviazioni Meteo
- Sfruttare i segnali di rapporto degli U-boat

#### 4.7 - I segnali di contatto degli U-boat

- Brevi comunicazioni radio in cui gli equipaggi tedeschi dei sommergibili riportavano i possibili avvistamenti di navi Alleate
- Essi si basavano su un Libro che conteneva le abbreviazioni ed erano lunghi soltanto 22 caratteri

#### 4.7 - I segnali di contatto degli U-boat

- Crib necessario poteva essere ricavato dalla cattura del Libro dal sommergibile U 559
- Segnali dovevano essere mandati velocemente
- Quindi i tedeschi usavano un sistema semplice per l'assetto della chiave di messaggio

#### 4.7 - I segnali di contatto degli U-boat

- La chiave di messaggio era la posizione dei rotori usata per decifrare (e cifrare) il messaggio
- Operatore Enigma cercava una coppia indicatore/chiave nel suo K Book, compreso l'indicatore nell'intestazione del messaggio, e cifrava il segnale partendo con i rotori posti secondo la chiave di messaggio

#### 4.7 - I segnali di contatto degli U-boat

- Bletchley Park aveva in suo possesso un K Book quindi a partire dall'indicatore si poteva direttamente risalire alla chiave di messaggio
- Non si conosceva la configurazione base della macchina Enigma
- Da un numero sufficiente di messaggi si poteva ricavare una disposizione (un Menu) da usare sulle bombe di Turing

#### 5 - Conclusione

- Ultra e Gli uomini di Bletchley Park, pur rimanendo sconosciuti ai più, per tutta la durata del conflitto permisero agli Alleati di avere l'arma in più che risultò essere fondamentale in qualsiasi momento e situazione della guerra: l'informazione
- Dall'Atlantico alla Normandia, passando per gli sbarchi in Sicilia e a Salerno che portarono alla liberazione dell'Italia e di tutta l'Europa, l'intervento dei crittoanalisti salvò numerose vite umane e permise una conclusione anticipata della Seconda Guerra Mondiale

#### 5 - Conclusione

- E tutto questo è rimasto vincolato da un segreto che coinvolgeva tutto il personale della GC&CS e che venne mantenuto ben oltre la fine della guerra. Infatti solo nel 1974 il governo inglese autorizzò la pubblicazione di un libro che finalmente poteva rendere giustizia al lavoro degli uomini di Bletchley Park