

# La macchina Enigma

Angela Bonazza   Lara Maines   Giorgia Marcolini  
Chiara Marcolla   Valentina Pulice

Università degli Studi di Trento

Povo, 20 settembre 2005

# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 Cenni storici
  - La Macchina Enigma
  - Carta d'Identità
- 3 Struttura
  - Versione base
  - Modifiche
  - Combinazioni
- 4 Funzionamento
  - Assetto giornaliero
  - Cifratura e Decifratura
- 5 Guerra ad Enigma
  - I crittoanalisti polacchi
  - La Bomba di Turing
- 6 La crittografia nella WW II
  - I successi dei crittoanalisti

# Perchè la crittografia?

Fin dall'antichità l'uomo ha sentito l'esigenza di creare codici segreti, sistemi di segni in grado di nascondere ad occhi indiscreti un importante messaggio e rivelarlo solo al destinatario.

Ha qui le sue radici la **crittografia** che nei secoli ha trovato applicazioni sia nella sfera privata che in quella pubblica.

# Perchè la crittografia?

Fin dall'antichità l'uomo ha sentito l'esigenza di creare **codici segreti**, sistemi di segni in grado di nascondere ad occhi indiscreti un importante messaggio e rivelarlo solo al destinatario.

Ha qui le sue radici la **crittografia** che nei secoli ha trovato applicazioni sia nella sfera privata che in quella pubblica.

# Perchè la crittografia?

Fin dall'antichità l'uomo ha sentito l'esigenza di creare **codici segreti**, sistemi di segni in grado di nascondere ad occhi indiscreti un importante messaggio e rivelarlo solo al destinatario.

Ha qui le sue radici la **crittografia** che nei secoli ha trovato applicazioni sia nella sfera privata che in quella pubblica.

# Scrittura segreta

Una **scrittura segreta**, o crittosistema, è una scrittura in codice utilizzata per comunicare senza che terzi vengano a conoscenza del messaggio.

Si basa su:

- una chiave  $g$
- un algoritmo  $E$

# Scrittura segreta

Una **scrittura segreta**, o crittosistema, è una scrittura in codice utilizzata per comunicare senza che terzi vengano a conoscenza del messaggio.

Si basa su:

- una **chiave**  $g$
- un **algoritmo**  $E$ : un procedimento per tradurre in linguaggio codice un testo in chiaro  $M$ , ovvero il messaggio che si vuole trasmettere.

# Scrittura segreta

Una **scrittura segreta**, o crittosistema, è una scrittura in codice utilizzata per comunicare senza che terzi vengano a conoscenza del messaggio.

Si basa su:

- una **chiave**  $g$
- un **algoritmo**  $E$ : un procedimento per tradurre in linguaggio codice un testo in chiaro  $M$ , ovvero il messaggio che si vuole trasmettere.



# Scrittura segreta

Una **scrittura segreta**, o crittosistema, è una scrittura in codice utilizzata per comunicare senza che terzi vengano a conoscenza del messaggio.

Si basa su:

- una **chiave**  $g$
- un **algoritmo**  $E$ : un procedimento per tradurre in linguaggio codice un testo in chiaro  $M$ , ovvero il messaggio che si vuole trasmettere.

# Scrittura segreta

Una **scrittura segreta**, o crittosistema, è una scrittura in codice utilizzata per comunicare senza che terzi vengano a conoscenza del messaggio.


Si basa su:

- una **chiave**  $g$
- un **algoritmo**  $E$ : un procedimento per tradurre in linguaggio codice un testo in chiaro  $M$ , ovvero il messaggio che si vuole trasmettere.

# L'Esperto definisce. . .

*"A secrecy system is defined abstractly as a set of transformations of one space (the set of possible messages) into a second space (the set of possible cryptograms). Each particular transformation of the set corresponds to enciphering with a particular key. The transformations are supposed reversible (non-singular) so that unique deciphering is possible when the key is known."*<sup>1</sup>

---

<sup>1</sup>Shannon, C.E., "Communication Theory of Secrecy System" 

## ...la Storia risponde

Alcuni esempi di applicazione pratica della crittografia in un passato lontano sono:

- I secolo a.C, Codice di Cesare
- XV secolo d.C, Disco Cifrante dell'Alberti

## ...la Storia risponde

Alcuni esempi di applicazione pratica della crittografia in un passato lontano sono:

- V secolo a.C, **Scitale Spartana**
- I secolo a.C, **Codice di Cesare**
- XV secolo d.C, **Disco Cifrante dell'Alberti**

## ...la Storia risponde

Alcuni esempi di applicazione pratica della crittografia in un passato lontano sono:

- V secolo a.C, **Scitale Spartana**
- I secolo a.C, **Codice di Cesare**
- XV secolo d.C, **Disco Cifrante dell'Alberti**

## ...la Storia risponde

Alcuni esempi di applicazione pratica della crittografia in un passato lontano sono:

- V secolo a.C, **Scitale Spartana**
- I secolo a.C, **Codice di Cesare**
- XV secolo d.C, **Disco Cifrante dell'Alberti**

## ...la Storia risponde

Alcuni esempi di applicazione pratica della crittografia in un passato lontano sono:

- V secolo a.C, **Scitale Spartana**
- I secolo a.C, **Codice di Cesare**
- XV secolo d.C, **Disco Cifrante dell'Alberti**





# Disco Cifrante dell'Alberti

- Dispositivo costituito da due dischi di rame concentrici di diametro diverso, infilati su un perno, sui cui lati è riportato un alfabeto
- Il disco esterno riproduce l'alfabeto nell'ordine consueto ed è fisso
- Il disco interno riproduce un alfabeto in ordine casuale (**alfabeto cifrante**)
- Per effettuare la cifratura, il disco mobile viene fissato su una data lettera (**chiave di messaggio**): si ottiene così una corrispondenza "lettera in chiaro (disco esterno) - lettera cifrata (disco interno)"

# Disco Cifrante dell'Alberti

- Dispositivo costituito da due dischi di rame concentrici di diametro diverso, infilati su un perno, sui cui lati è riportato un alfabeto
- Il disco esterno riproduce l'alfabeto nell'ordine consueto ed è fisso
- Il disco interno riproduce un alfabeto in ordine casuale (alfabeto cifrante)
- Per effettuare la cifratura, il disco mobile viene fissato su una data lettera (chiave di messaggio): si ottiene così una corrispondenza "lettera in chiaro (disco esterno) - lettera cifrata (disco interno)"

# Disco Cifrante dell'Alberti

- Dispositivo costituito da due dischi di rame concentrici di diametro diverso, infilati su un perno, sui cui lati è riportato un alfabeto
- Il disco esterno riproduce l'alfabeto nell'ordine consueto ed è fisso
- Il disco interno riproduce un alfabeto in ordine casuale (**alfabeto cifrante**)
- Per effettuare la cifratura, il disco mobile viene fissato su una data lettera (**chiave di messaggio**): si ottiene così una corrispondenza "lettera in chiaro (disco esterno) - lettera cifrata (disco interno)"

# Disco Cifrante dell'Alberti

- Dispositivo costituito da due dischi di rame concentrici di diametro diverso, infilati su un perno, sui cui lati è riportato un alfabeto
- Il disco esterno riproduce l'alfabeto nell'ordine consueto ed è fisso
- Il disco interno riproduce un alfabeto in ordine casuale (**alfabeto cifrante**)
- Per effettuare la cifratura, il disco mobile viene fissato su una data lettera (**chiave di messaggio**): si ottiene così una corrispondenza "lettera in chiaro (disco esterno) - lettera cifrata (disco interno)"

# Disco Cifrante dell'Alberti

- Dispositivo costituito da due dischi di rame concentrici di diametro diverso, infilati su un perno, sui cui lati è riportato un alfabeto
- Il disco esterno riproduce l'alfabeto nell'ordine consueto ed è fisso
- Il disco interno riproduce un alfabeto in ordine casuale (**alfabeto cifrante**)
- Per effettuare la cifratura, il disco mobile viene fissato su una data lettera (**chiave di messaggio**): si ottiene così una corrispondenza "lettera in chiaro (disco esterno) - lettera cifrata (disco interno)"

## Più recentemente

Nella storia moderna, la crittografia si sviluppa parallelamente agli eventi bellici, data l'esigenza di comunicare strategie militari, senza che il nemico ne venga a conoscenza.

E' in questo contesto che fanno la loro comparsa le **macchine cifratrici**.

## Più recentemente

Nella storia moderna, la crittografia si sviluppa parallelamente agli eventi bellici, data l'esigenza di comunicare strategie militari, senza che il nemico ne venga a conoscenza. E' in questo contesto che fanno la loro comparsa le **macchine cifratrici**.



# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 **Cenni storici**
  - **La Macchina Enigma**
  - Carta d'Identità
- 3 Struttura
  - Versione base
  - Modifiche
  - Combinazioni
- 4 Funzionamento
  - Assetto giornaliero
  - Cifratura e Decifratura
- 5 Guerra ad Enigma
  - I crittoanalisti polacchi
  - La Bomba di Turing
- 6 La crittografia nella WW II
  - I successi dei crittoanalisti

# La Macchina Enigma



© 1998, Marlow DeMeier



# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 **Cenni storici**
  - La Macchina Enigma
  - **Carta d'Identità**
- 3 Struttura
  - Versione base
  - Modifiche
  - Combinazioni
- 4 Funzionamento
  - Assetto giornaliero
  - Cifratura e Decifratura
- 5 Guerra ad Enigma
  - I crittoanalisti polacchi
  - La Bomba di Turing
- 6 La crittografia nella WW II
  - I successi dei crittoanalisti

# Carta d'identità

COSA?

Una macchina cifratrice

CHI?

Arthur Scherbius

QUANDO?

Inizio XX secolo

PERCHÈ?

Segretezza delle comunicazioni militari

DOVE?

Nella Germania nazista

# Carta d'identità

**COSA?**

Una macchina cifratrice

**CHI?**

Arthur Scherbius

**QUANDO?**

Inizio XX secolo

**PERCHÈ?**

Segretezza delle comunicazioni militari

**DOVE?**

Nella Germania nazista

# Carta d'identità

**COSA?**

Una macchina cifratrice

CHI?

Arthur Scherbius

QUANDO?

Inizio XX secolo

PERCHÈ?

Segretezza delle comunicazioni militari

DOVE?

Nella Germania nazista

# Carta d'identità

**COSA?**

Una macchina cifratrice

**CHI?**

Arthur Scherbius

**QUANDO?**

Inizio XX secolo

**PERCHÈ?**

Segretezza delle comunicazioni militari

**DOVE?**

Nella Germania nazista

# Carta d'identità

**COSA?**

Una macchina cifratrice

**CHI?**

Arthur Scherbius

**QUANDO?**

Inizio XX secolo

**PERCHÈ?**

Segretezza delle comunicazioni militari

**DOVE?**

Nella Germania nazista



# Carta d'identità

**COSA?**

Una macchina cifratrice

**CHI?**

Arthur Scherbius

**QUANDO?**

Inizio XX secolo

**PERCHÈ?**

Segretezza delle comunicazioni militari

**DOVE?**

Nella Germania nazista

# Carta d'identità

COSA?

Una macchina cifratrice

CHI?

Arthur Scherbius

QUANDO?

Inizio XX secolo

PERCHÈ?

Segretezza delle comunicazioni militari

DOVE?

Nella Germania nazista

# Carta d'identità

**COSA?**

Una macchina cifratrice

**CHI?**

Arthur Scherbius

**QUANDO?**

Inizio XX secolo

**PERCHÈ?**

Segretezza delle comunicazioni militari

**DOVE?**

Nella Germania nazista



# Carta d'identità

COSA?

Una macchina cifratrice

CHI?

Arthur Scherbius

QUANDO?

Inizio XX secolo

PERCHÈ?

Segretezza delle comunicazioni militari

DOVE?

Nella Germania nazista

# Carta d'identità

**COSA?**

Una macchina cifratrice

**CHI?**

Arthur Scherbius

**QUANDO?**

Inizio XX secolo

**PERCHÈ?**

Segretezza delle comunicazioni militari

**DOVE?**

Nella Germania nazista

# Carta d'identità

**COSA?**

Una macchina cifratrice

**CHI?**

Arthur Scherbius

**QUANDO?**

Inizio XX secolo

**PERCHÈ?**

Segretezza delle comunicazioni militari

**DOVE?**

Nella Germania nazista

# Come Enigma veniva utilizzata



Quando un operatore utilizzava Enigma, digitava le lettere che costituivano il messaggio sulla tastiera della macchina e i meccanismi interni della stessa trasformavano quel testo in un altro apparentemente incomprensibile

# Come Enigma veniva utilizzata



Quando un operatore utilizzava Enigma, digitava le lettere che costituivano il messaggio sulla tastiera della macchina e i meccanismi interni della stessa trasformavano quel testo in un altro apparentemente incomprensibile



# Come Enigma veniva utilizzata

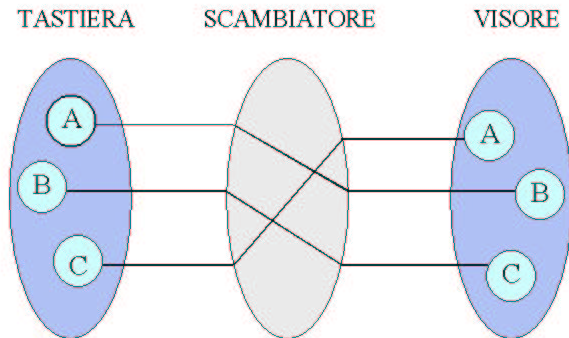


Quando un operatore utilizzava Enigma, digitava le lettere che costituivano il messaggio sulla tastiera della macchina e i meccanismi interni della stessa trasformavano quel testo in un altro apparentemente incomprensibile

# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 Cenni storici
  - La Macchina Enigma
  - Carta d'Identità
- 3 **Struttura**
  - **Versione base**
  - Modifiche
  - Combinazioni
- 4 Funzionamento
  - Assetto giornaliero
  - Cifratura e Decifratura
- 5 Guerra ad Enigma
  - I crittoanalisti polacchi
  - La Bomba di Turing
- 6 La crittografia nella WW II
  - I successi dei crittoanalisti

# Versione base (con 3 lettere)



# Versione base

La complessità della macchina Enigma era ottenuta mediante la combinazione di elementi semplici:

- una **tastiera** per immettere le lettere del testo in chiaro
- un'**unità scambiatrice** che cifra la lettera trasformandola nel corrispondente elemento del crittogramma
- un **visore** con varie lampadine che illuminandosi indicano la lettera da inserire nel testo cifrato

# Versione base

La complessità della macchina Enigma era ottenuta mediante la combinazione di elementi semplici:

- una **tastiera** per immettere le lettere del testo in chiaro
- un'**unità scambiatrice** che cifra la lettera trasformandola nel corrispondente elemento del crittogramma
- un **visore** con varie lampadine che illuminandosi indicano la lettera da inserire nel testo cifrato

# Versione base

La complessità della macchina Enigma era ottenuta mediante la combinazione di elementi semplici:

- una **tastiera** per immettere le lettere del testo in chiaro
- un'**unità scambiatrice** che cifra la lettera trasformandola nel corrispondente elemento del crittogramma
- un **visore** con varie lampadine che illuminandosi indicano la lettera da inserire nel testo cifrato

# Versione base

La complessità della macchina Enigma era ottenuta mediante la combinazione di elementi semplici:

- una **tastiera** per immettere le lettere del testo in chiaro
- un'**unità scambiatrice** che cifra la lettera trasformandola nel corrispondente elemento del crittogramma
- un **visore** con varie lampadine che illuminandosi indicano la lettera da inserire nel testo cifrato

# Versione base

La complessità della macchina Enigma era ottenuta mediante la combinazione di elementi semplici:

- una **tastiera** per immettere le lettere del testo in chiaro
- un'**unità scambiatrice** che cifra la lettera trasformandola nel corrispondente elemento del crittogramma
- un **visore** con varie lampadine che illuminandosi indicano la lettera da inserire nel testo cifrato



# Versione base

La complessità della macchina Enigma era ottenuta mediante la combinazione di elementi semplici:

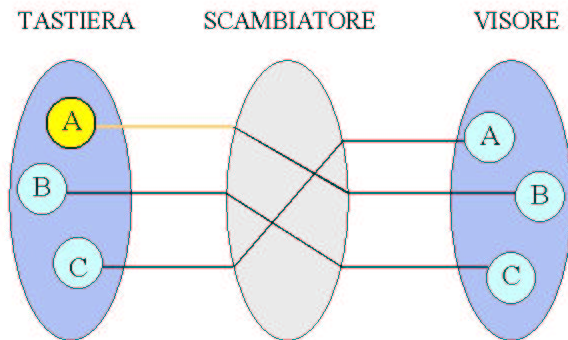
- una **tastiera** per immettere le lettere del testo in chiaro
- un'**unità scambiatrice** che cifra la lettera trasformandola nel corrispondente elemento del crittogramma
- un **visore** con varie lampadine che illuminandosi indicano la lettera da inserire nel testo cifrato

# Versione base

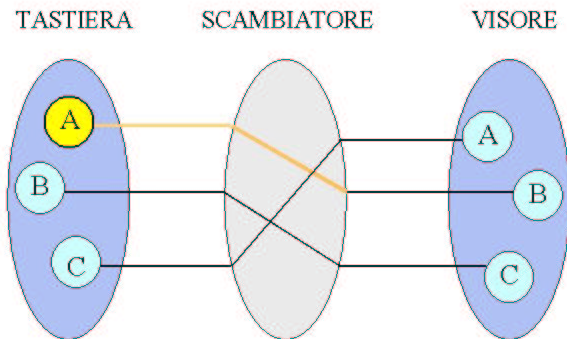
La complessità della macchina Enigma era ottenuta mediante la combinazione di elementi semplici:

- una **tastiera** per immettere le lettere del testo in chiaro
- un'**unità scambiatrice** che cifra la lettera trasformandola nel corrispondente elemento del crittogramma
- un **visore** con varie lampadine che illuminandosi indicano la lettera da inserire nel testo cifrato

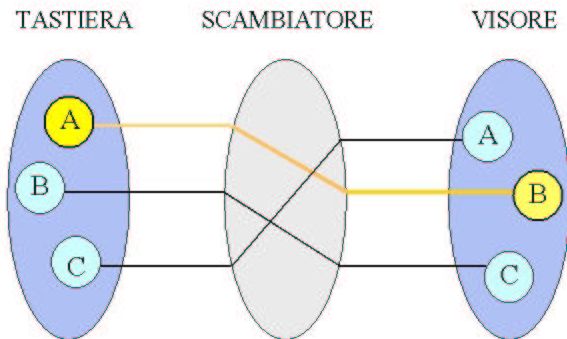
# Versione base (con 3 lettere)



# Versione base (con 3 lettere)



# Versione base (con 3 lettere)



# Lo Scambiatore



- E' l'elemento più importante della macchina Enigma
- Consiste in uno spesso disco di gomma attraversato da una fitta rete di fili provenienti dalla tastiera. Questi fili entrano nello scambiatore e, dopo un percorso formato da vari gomiti, emergono dalla parte opposta
- Lo schema interno del rotore determina un alfabeto cifrante utilizzabile per una semplice cifratura a sostituzione *monoalfabetica*

# Lo Scambiatore



- E' l'elemento più importante della macchina Enigma
- Consiste in uno spesso disco di gomma attraversato da una fitta rete di fili provenienti dalla tastiera. Questi fili entrano nello scambiatore e, dopo un percorso formato da vari gomiti, emergono dalla parte opposta
- Lo schema interno del rotore determina un alfabeto cifrante utilizzabile per una semplice cifratura a sostituzione *monoalfabetica*

# Lo Scambiatore



- E' l'elemento più importante della macchina Enigma
- Consiste in uno spesso disco di gomma attraversato da una fitta rete di fili provenienti dalla tastiera. Questi fili entrano nello scambiatore e, dopo un percorso formato da vari gomiti, emergono dalla parte opposta
- Lo schema interno del rotore determina un alfabeto cifrante utilizzabile per una semplice cifratura a sostituzione *monoalfabetica*



# Lo Scambiatore



- E' l'elemento più importante della macchina Enigma
- Consiste in uno spesso disco di gomma attraversato da una fitta rete di fili provenienti dalla tastiera. Questi fili entrano nello scambiatore e, dopo un percorso formato da vari gomiti, emergono dalla parte opposta
- Lo schema interno del rotore determina un alfabeto cifrante utilizzabile per una semplice cifratura a sostituzione *monoalfabetica*

# Lo Scambiatore



- E' l'elemento più importante della macchina Enigma
- Consiste in uno spesso disco di gomma attraversato da una fitta rete di fili provenienti dalla tastiera. Questi fili entrano nello scambiatore e, dopo un percorso formato da vari gomiti, emergono dalla parte opposta
- Lo schema interno del rotore determina un alfabeto cifrante utilizzabile per una semplice cifratura a sostituzione *monoalfabetica*

# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 Cenni storici
  - La Macchina Enigma
  - Carta d'Identità
- 3 **Struttura**
  - Versione base
  - **Modifiche**
  - Combinazioni
- 4 Funzionamento
  - Assetto giornaliero
  - Cifratura e Decifratura
- 5 Guerra ad Enigma
  - I crittoanalisti polacchi
  - La Bomba di Turing
- 6 La crittografia nella WW II
  - I successi dei crittoanalisti

# Da monoalfabetica a polialfabetica

- Il passo successivo dell'idea di Scherbius prevedeva di far *ruotare* il disco dello scambiatore di un ventiseiesimo di giro dopo la cifratura di ogni lettera
- In questo modo l'alfabeto cifrante cambiava dopo ogni lettera
- Si passò così dalla cifratura monoalfabetica a quella *polialfabetica*

# Da monoalfabetica a polialfabetica

- Il passo successivo dell'idea di Scherbius prevedeva di far *ruotare* il disco dello scambiatore di un ventiseiesimo di giro dopo la cifratura di ogni lettera
- In questo modo l'alfabeto cifrante cambiava dopo ogni lettera
- Si passò così dalla cifratura monoalfabetica a quella *polialfabetica*

# Da monoalfabetica a polialfabetica

- Il passo successivo dell'idea di Scherbius prevedeva di far *ruotare* il disco dello scambiatore di un ventiseiesimo di giro dopo la cifratura di ogni lettera
- In questo modo l'alfabeto cifrante cambiava dopo ogni lettera
- Si passò così dalla cifratura monoalfabetica a quella *polialfabetica*

# Il problema della ripetizione

Così com'è il meccanismo presenta il **problema della ripetizione**, che è comunemente sinonimo di cifratura debole.

Per superarlo vennero introdotti un secondo e un terzo scambiatore. Il secondo compie una rotazione parziale soltanto dopo che il primo ha compiuto un intero giro e allo stesso modo fa il terzo rispetto al secondo.

# Il problema della ripetizione

Così com'è il meccanismo presenta il **problema della ripetizione**, che è comunemente sinonimo di cifratura debole. Per superarlo vennero introdotti un secondo e un terzo scambiatore. Il secondo compie una rotazione parziale soltanto dopo che il primo ha compiuto un intero giro e allo stesso modo fa il terzo rispetto al secondo.



# Il problema della ripetizione

Così com'è il meccanismo presenta il [problema della ripetizione](#), che è comunemente sinonimo di cifratura debole. Per superarlo vennero introdotti un secondo e un terzo scambiatore. Il secondo compie una rotazione parziale soltanto dopo che il primo ha compiuto un intero giro e allo stesso modo fa il terzo rispetto al secondo.



# Scambiatore modificato

- **Diametro di circa 4 pollici (circa 10 cm)**
- Esternamente: lato destro 26 contatti a molla sporgenti (*pin*, maschio), lato sinistro altri 26 rientranti (*pad*, femmina)
- Internamente: corrispondenza biunivoca tra maschi e femmine data da fili elettrici
- Contrassegnato da un numero romano (I II III)
- Anello esterno rotabile in 26 posizioni diverse

# Scambiatore modificato

- Diametro di circa 4 pollici (circa 10 cm)
- Esternamente: lato destro 26 contatti a molla sporgenti (*pin*, maschio), lato sinistro altri 26 rientranti (*pad*, femmina)
- Internamente: corrispondenza biunivoca tra maschi e femmine data da fili elettrici
- Contrassegnato da un numero romano (I II III)
- Anello esterno rotabile in 26 posizioni diverse

# Scambiatore modificato

- Diametro di circa 4 pollici (circa 10 cm)
- Esternamente: lato destro 26 contatti a molla sporgenti (*pin*, maschio), lato sinistro altri 26 rientranti (*pad*, femmina)
- Internamente: corrispondenza biunivoca tra maschi e femmine data da fili elettrici
- Contrassegnato da un numero romano (I II III)
- Anello esterno rotabile in 26 posizioni diverse

# Scambiatore modificato

- Diametro di circa 4 pollici (circa 10 cm)
- Esternamente: lato destro 26 contatti a molla sporgenti (*pin*, maschio), lato sinistro altri 26 rientranti (*pad*, femmina)
- Internamente: corrispondenza biunivoca tra maschi e femmine data da fili elettrici
- Contrassegnato da un numero romano (I II III)
- Anello esterno rotabile in 26 posizioni diverse

# Scambiatore modificato

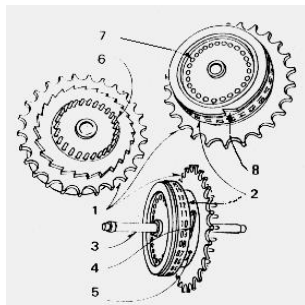
- Diametro di circa 4 pollici (circa 10 cm)
- Esternamente: lato destro 26 contatti a molla sporgenti (*pin*, maschio), lato sinistro altri 26 rientranti (*pad*, femmina)
- Internamente: corrispondenza biunivoca tra maschi e femmine data da fili elettrici
- Contrassegnato da un numero romano (I II III)
- Anello esterno rotabile in 26 posizioni diverse

# Scambiatore modificato

- Diametro di circa 4 pollici (circa 10 cm)
- Esternamente: lato destro 26 contatti a molla sporgenti (*pin*, maschio), lato sinistro altri 26 rientranti (*pad*, femmina)
- Internamente: corrispondenza biunivoca tra maschi e femmine data da fili elettrici
- Contrassegnato da un numero romano (I II III)
- Anello esterno rotabile in 26 posizioni diverse

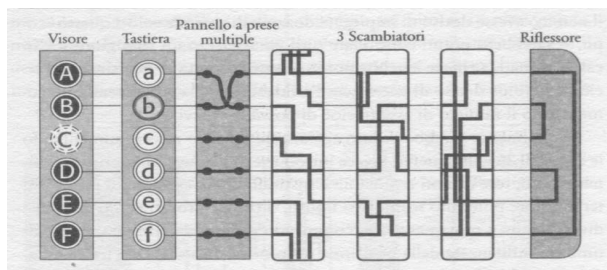


# Dettagli di uno scambiatore



- 1 Dentellature usate per posizionare il rotore
- 2 Anello dell'alfabeto
- 3 Asse di rotazione
- 4 Gancio che blocca l'anello al nucleo (5)
- 5 Nucleo contenente i collegamenti elettrici tra contatti (6) e dischi (7)
- 6 Contatti elettrici
- 7 Dischi di contatto tra rotori successivi
- 8 Gancio per ruotare l'anello dell'alfabeto

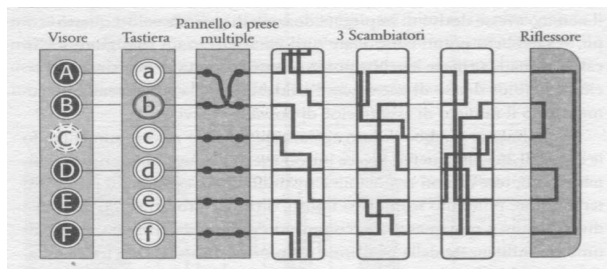
# Il Riflessore



E' un disco fisso simile agli scambiatori, tale che i fili che vi entrano riemergano dallo stesso lato.

Il segnale in ingresso alla macchina attraversa i tre scambiatori, passa al riflessore e viene rimandato indietro passando nuovamente negli scambiatori, ma percorrendo fili diversi.

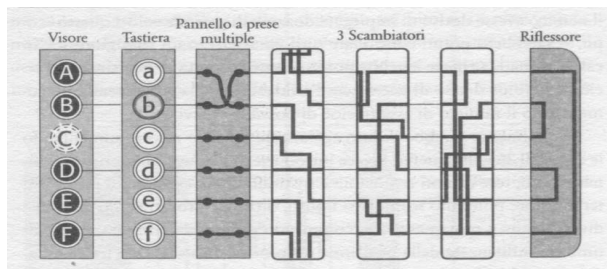
# Il Riflessore



E' un disco fisso simile agli scambiatori, tale che i fili che vi entrano riemergano dallo stesso lato.

Il segnale in ingresso alla macchina attraversa i tre scambiatori, passa al riflettore e viene rimandato indietro passando nuovamente negli scambiatori, ma percorrendo fili diversi.

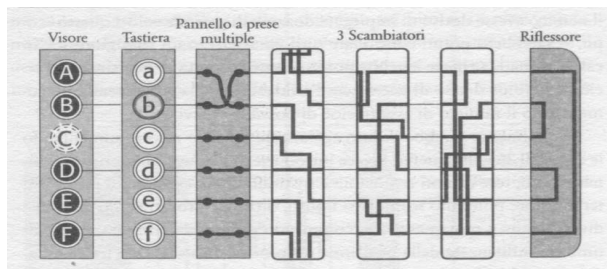
# Il Riflessore



E' un disco fisso simile agli scambiatori, tale che i fili che vi entrano riemergano dallo stesso lato.

Il segnale in ingresso alla macchina attraversa i tre scambiatori, passa al riflessore e viene rimandato indietro passando nuovamente negli scambiatori, ma percorrendo fili diversi.

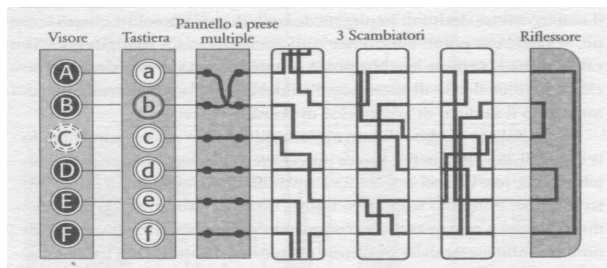
# Il Riflessore



E' un disco fisso simile agli scambiatori, tale che i fili che vi entrano riemergano dallo stesso lato.

Il segnale in ingresso alla macchina attraversa i tre scambiatori, passa al riflettore e viene rimandato indietro passando nuovamente negli scambiatori, ma percorrendo fili diversi.

# Il Riflessore



E' un disco fisso simile agli scambiatori, tale che i fili che vi entrano riemergano dallo stesso lato.

Il segnale in ingresso alla macchina attraversa i tre scambiatori, passa al riflettore e viene rimandato indietro passando nuovamente negli scambiatori, ma percorrendo fili diversi.

## Due nuove caratteristiche: Rotori Removibili..



- Il numero di rotor disponibili passò da 3 a 5
- I rotor potevano essere sostituiti con altri o scambiati tra loro
- Questo accorgimento aumentava il numero delle chiavi

## Due nuove caratteristiche: Rotori Removibili..



- Il numero di rotorì disponibili passò da 3 a 5
- I rotorì potevano essere sostituiti con altri o scambiati tra loro
- Questo accorgimento aumentava il numero delle chiavi



## Due nuove caratteristiche: Rotori Removibili..



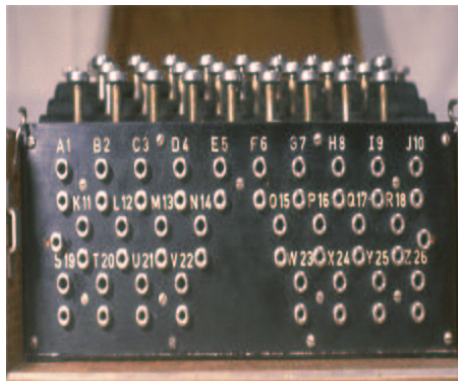
- Il numero di rotor disponibili passò da 3 a 5
- I rotor potevano essere sostituiti con altri o scambiati tra loro
- Questo accorgimento aumentava il numero delle chiavi

## Due nuove caratteristiche: Rotori Removibili..



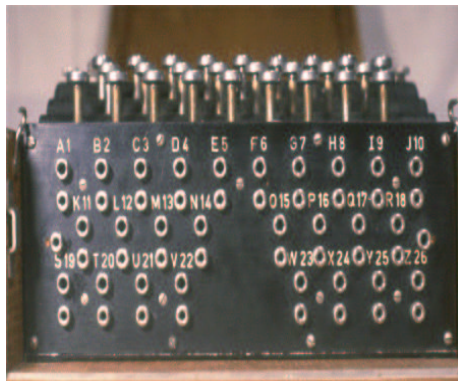
- Il numero di rotor disponibili passò da 3 a 5
- I rotor potevano essere sostituiti con altri o scambiati tra loro
- Questo accorgimento aumentava il numero delle chiavi

# ..e Stecker



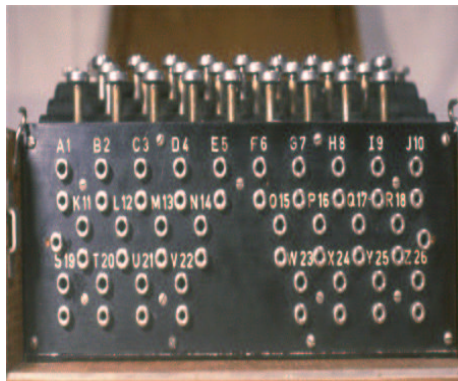
- Pannello a prese multiple posto tra tastiera e primo rotore
- Permetteva di inserire alcuni cavi muniti di spinotti, che avevano l'effetto di scambiare due lettere prima della loro immissione nel rotore

# ..e Stecker



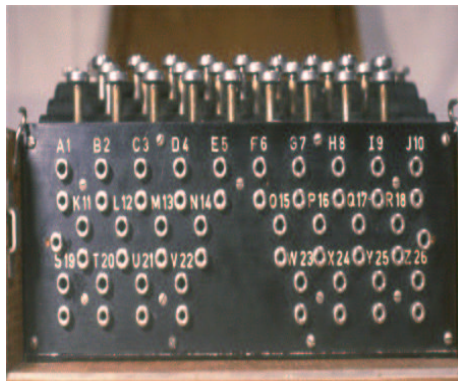
- Pannello a prese multiple posto tra tastiera e primo rotore
- Permetteva di inserire alcuni cavi muniti di spinotti, che avevano l'effetto di scambiare due lettere prima della loro immissione nel rotore

# ..e Stecker



- Pannello a prese multiple posto tra tastiera e primo rotore
- Permetteva di inserire alcuni cavi muniti di spinotti, che avevano l'effetto di scambiare due lettere prima della loro immissione nel rotore

# ..e Stecker



- Pannello a prese multiple posto tra tastiera e primo rotore
- Permetteva di inserire alcuni cavi muniti di spinotti, che avevano l'effetto di scambiare due lettere prima della loro immissione nel rotore

## Il Pannello a prese multiple: un esempio



Collegando attraverso uno **spinotto** la coppia di lettere  $Q$  e  $R$ , la corrente che rappresenta la  $Q$  in entrata rappresenta poi la  $R$  in uscita.

Digitando  $Q$  sulla tastiera, la sua cifratura sarà la cifratura di  $R$ .

Viceversa se una qualsiasi lettera viene cifrata nella  $Q$ , il risultato finale sarà  $R$ .

## Il Pannello a prese multiple: un esempio



Collegando attraverso uno **spinotto** la coppia di lettere  $Q$  e  $R$ , la corrente che rappresenta la  $Q$  in entrata rappresenta poi la  $R$  in uscita.

Digitando  $Q$  sulla tastiera, la sua cifratura sarà la cifratura di  $R$ .

Viceversa se una qualsiasi lettera viene cifrata nella  $Q$ , il risultato finale sarà  $R$ .



## Il Pannello a prese multiple: un esempio



Collegando attraverso uno **spinotto** la coppia di lettere  $Q$  e  $R$ , la corrente che rappresenta la  $Q$  in entrata rappresenta poi la  $R$  in uscita.

Digitando  $Q$  sulla tastiera, la sua cifratura sarà la cifratura di  $R$ .

Viceversa se una qualsiasi lettera viene cifrata nella  $Q$ , il risultato finale sarà  $R$ .

## Il Pannello a prese multiple: un esempio



Collegando attraverso uno **spinotto** la coppia di lettere  $Q$  e  $R$ , la corrente che rappresenta la  $Q$  in entrata rappresenta poi la  $R$  in uscita.

Digitando  $Q$  sulla tastiera, la sua cifratura sarà la cifratura di  $R$ .

Viceversa se una qualsiasi lettera viene cifrata nella  $Q$ , il risultato finale sarà  $R$ .

## Il Pannello a prese multiple: un esempio



Collegando attraverso uno **spinotto** la coppia di lettere  $Q$  e  $R$ , la corrente che rappresenta la  $Q$  in entrata rappresenta poi la  $R$  in uscita.

Digitando  $Q$  sulla tastiera, la sua cifratura sarà la cifratura di  $R$ .

Viceversa se una qualsiasi lettera viene cifrata nella  $Q$ , il risultato finale sarà  $R$ .

## Il Pannello a prese multiple: un esempio



Collegando attraverso uno **spinetto** la coppia di lettere  $Q$  e  $R$ , la corrente che rappresenta la  $Q$  in entrata rappresenta poi la  $R$  in uscita.

Digitando  $Q$  sulla tastiera, la sua cifratura sarà la cifratura di  $R$ .

Viceversa se una qualsiasi lettera viene cifrata nella  $Q$ , il risultato finale sarà  $R$ .

## Il Pannello a prese multiple: un esempio



Collegando attraverso uno **spinotto** la coppia di lettere  $Q$  e  $R$ , la corrente che rappresenta la  $Q$  in entrata rappresenta poi la  $R$  in uscita.

Digitando  $Q$  sulla tastiera, la sua cifratura sarà la cifratura di  $R$ .

Viceversa se una qualsiasi lettera viene cifrata nella  $Q$ , il risultato finale sarà  $R$ .

# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 Cenni storici
  - La Macchina Enigma
  - Carta d'Identità
- 3 **Struttura**
  - Versione base
  - Modifiche
  - **Combinazioni**
- 4 Funzionamento
  - Assetto giornaliero
  - Cifratura e Decifratura
- 5 Guerra ad Enigma
  - I crittoanalisti polacchi
  - La Bomba di Turing
- 6 La crittografia nella WW II
  - I successi dei crittoanalisti

# Calcolo delle combinazioni

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

- posizionamento di 3 rotori scelti su 5
- possibili orientamenti dei rotori
- possibili abbinamenti di 12 lettere su 26 dovuti allo *stecker*



105 869 167 644 240 000

# Calcolo delle combinazioni

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

- posizionamento di 3 rotori scelti su 5: 60
- possibili orientamenti dei rotori:  $26 \times 26 \times 26 = 17\,576$
- possibili abbinamenti di 12 lettere su 26 dovuti allo *stecker*:  
100 391 791 500



105 869 167 644 240 000



# Calcolo delle combinazioni

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

- posizionamento di 3 rotori scelti su 5: 60
- possibili orientamenti dei rotori:  $26 \times 26 \times 26 = 17\,576$
- possibili abbinamenti di 12 lettere su 26 dovuti allo *stecker*:  
100 391 791 500



105 869 167 644 240 000

# Calcolo delle combinazioni

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

- posizionamento di 3 rotori scelti su 5: 60
- possibili orientamenti dei rotori:  $26 \times 26 \times 26 = 17\,576$
- possibili abbinamenti di 12 lettere su 26 dovuti allo *stecker*:  
100 391 791 500



105 869 167 644 240 000

# Calcolo delle combinazioni

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

- posizionamento di 3 rotori scelti su 5: 60
- possibili orientamenti dei rotori:  $26 \times 26 \times 26 = 17\,576$
- possibili abbinamenti di 12 lettere su 26 dovuti allo *stecker*  
100 391 791 500



105 869 167 644 240 000

# Calcolo delle combinazioni

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

- posizionamento di 3 rotori scelti su 5: 60
- possibili orientamenti dei rotori:  $26 \times 26 \times 26 = 17\,576$
- possibili abbinamenti di 12 lettere su 26 dovuti allo *stecker*:  
100 391 791 500



105 869 167 644 240 000

# Calcolo delle combinazioni

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

- posizionamento di 3 rotori scelti su 5: 60
- possibili orientamenti dei rotori:  $26 \times 26 \times 26 = 17\,576$
- possibili abbinamenti di 12 lettere su 26 dovuti allo *stecker*:  
100 391 791 500



105 869 167 644 240 000

# Calcolo delle combinazioni

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

- posizionamento di 3 rotori scelti su 5: 60
- possibili orientamenti dei rotori:  $26 \times 26 \times 26 = 17\,576$
- possibili abbinamenti di 12 lettere su 26 dovuti allo *stecker*:  
100 391 791 500



105 869 167 644 240 000

# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 Cenni storici
  - La Macchina Enigma
  - Carta d'Identità
- 3 Struttura
  - Versione base
  - Modifiche
  - Combinazioni
- 4 **Funzionamento**
  - **Assetto giornaliero**
  - Cifratura e Decifratura
- 5 Guerra ad Enigma
  - I crittoanalisti polacchi
  - La Bomba di Turing
- 6 La crittografia nella WW II
  - I successi dei crittoanalisti

# Il Cifrario

Prima di iniziare la cifratura di un messaggio, gli scambiatori dovevano essere posizionati con un certo assetto e la loro posizione costituiva una vera e propria chiave.

L'insieme di tali chiavi giornaliere era contenuta in un **cifrario** che veniva distribuito mensilmente a tutti gli operatori e che doveva essere, ovviamente, molto ben custodito.

Gli assetti giornalieri del cifrario venivano usati per tutti i messaggi di una giornata.



# Il Cifrario

Prima di iniziare la cifratura di un messaggio, gli scambiatori dovevano essere posizionati con un certo assetto e la loro posizione costituiva una vera e propria chiave.

L'insieme di tali chiavi giornaliere era contenuta in un **cifrario** che veniva distribuito mensilmente a tutti gli operatori e che doveva essere, ovviamente, molto ben custodito.

Gli assetti giornalieri del cifrario venivano usati per tutti i messaggi di una giornata.

# Il Cifrario

Prima di iniziare la cifratura di un messaggio, gli scambiatori dovevano essere posizionati con un certo assetto e la loro posizione costituiva una vera e propria chiave.

L'insieme di tali chiavi giornaliere era contenuta in un **cifrario** che veniva distribuito mensilmente a tutti gli operatori e che doveva essere, ovviamente, molto ben custodito.

Gli assetti giornalieri del cifrario venivano usati per tutti i messaggi di una giornata.

# Il Cifrario

Prima di iniziare la cifratura di un messaggio, gli scambiatori dovevano essere posizionati con un certo assetto e la loro posizione costituiva una vera e propria chiave.

L'insieme di tali chiavi giornaliere era contenuta in un **cifrario** che veniva distribuito mensilmente a tutti gli operatori e che doveva essere, ovviamente, molto ben custodito.

Gli assetti giornalieri del cifrario venivano usati per tutti i messaggi di una giornata.

# Il Cifrario

Prima di iniziare la cifratura di un messaggio, gli scambiatori dovevano essere posizionati con un certo assetto e la loro posizione costituiva una vera e propria chiave.

L'insieme di tali chiavi giornaliere era contenuta in un **cifrario** che veniva distribuito mensilmente a tutti gli operatori e che doveva essere, ovviamente, molto ben custodito.

Gli assetti giornalieri del cifrario venivano usati per tutti i messaggi di una giornata.

# Il Cifrario

Prima di iniziare la cifratura di un messaggio, gli scambiatori dovevano essere posizionati con un certo assetto e la loro posizione costituiva una vera e propria chiave.

L'insieme di tali chiavi giornaliere era contenuta in un **cifrario** che veniva distribuito mensilmente a tutti gli operatori e che doveva essere, ovviamente, molto ben custodito.

Gli assetti giornalieri del cifrario venivano usati per tutti i messaggi di una giornata.

# Il Cifrario

Prima di iniziare la cifratura di un messaggio, gli scambiatori dovevano essere posizionati con un certo assetto e la loro posizione costituiva una vera e propria chiave.

L'insieme di tali chiavi giornaliere era contenuta in un **cifrario** che veniva distribuito mensilmente a tutti gli operatori e che doveva essere, ovviamente, molto ben custodito.

Gli assetti giornalieri del cifrario venivano usati per tutti i messaggi di una giornata.

# Il Cifrario

Passaggi necessari per impostare quotidianamente Enigma:

Geheim! Sonder - Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SN UY DF GV LJ DO MX	vyj
30.	III V II	Y V P	OR KI JV QN ZN NU DP YC DS GP	eqr
29.	V IV I	O H R	UX JC EB DN TA ND ST DS LU PI	vhf

- 1 **Walzenlage:** quali rotori usare e in che ordine [I II III]
- 2 **Ringstellung:** assetto degli anelli [F T R]
- 3 **Steckerverbindungen:** assetto del pannello a prese multiple [HR AT IW SN UY DF GV LJ DO MX]
- 4 **Grundstellung:** le 3 lettere che mostravano la posizione dei rotori da usare per cifrare il messaggio [v y j]

# Il Cifrario

Passaggi necessari per impostare quotidianamente Enigma:

Geheim! Sonder - Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SN UY DF GV LJ DO MX	vyj
30.	III V II	Y V P	OR KI JV QZ EN NU DP YC DS GP	eqr
29.	V IV I	O H R	UX JC EB DK TA ED ST DS LU FI	vhf

- 1 Walzenlage:** quali rotori usare e in che ordine [I II III]
- 2 Ringstellung:** assetto degli anelli [F T R]
- 3 Steckerverbindungen:** assetto del pannello a prese multiple [HR AT IW SN UY DF GV LJ DO MX]
- 4 Grundstellung:** le 3 lettere che mostravano la posizione dei rotori da usare per cifrare il messaggio [v y j]



# Il Cifrario

Passaggi necessari per impostare quotidianamente Enigma:

Geheim! Sonder - Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SN UY DF GV LJ DO MX	vyj
30.	III V II	Y V P	OR KI JV QZ ZK NU DP YC DS GP	eqr
29.	V IV I	O H R	UX JC EB DK TA ED ST DS LU FI	vhf

- 1 Walzenlage:** quali rotori usare e in che ordine [I II III]
- 2 Ringstellung:** assetto degli anelli [F T R]
- 3 Steckerverbindungen:** assetto del pannello a prese multiple [HR AT IW SN UY DF GV LJ DO MX]
- 4 Grundstellung:** le 3 lettere che mostravano la posizione dei rotori da usare per cifrare il messaggio [v y j]

# Il Cifrario

Passaggi necessari per impostare quotidianamente Enigma:

Geheim! Sonder - Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SN UY DF GV LJ DO MX	vyj
30.	III V II	Y V P	OR KI JV QZ EN NU DP YC DS GP	eqr
29.	V IV I	O H R	UX JC FB BK TA ND ST DS LU PI	vhf

- 1 Walzenlage:** quali rotori usare e in che ordine [I II III]
- 2 Ringstellung:** assetto degli anelli [F T R]
- 3 Steckerverbindungen:** assetto del pannello a prese multiple [HR AT IW SN UY DF GV LJ DO MX]
- 4 Grundstellung:** le 3 lettere che mostravano la posizione dei rotori da usare per cifrare il messaggio [v y j]

# Il Cifrario

Passaggi necessari per impostare quotidianamente Enigma:

Geheim! Sonder - Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SN UY DF GV LJ DO MX	vyj
30.	III V II	Y V P	OR KI JV QZ EN NU DP YC DS GP	eqr
29.	V IV I	O H R	UX JC EB LN TA ND ST DS LU XI	vhf

- Walzenlage:** quali rotori usare e in che ordine [I II III]
- Ringstellung:** assetto degli anelli [F T R]
- Steckerverbindungen:** assetto del pannello a prese multiple [HR AT IW SN UY DF GV LJ DO MX]
- Grundstellung:** le 3 lettere che mostravano la posizione dei rotori da usare per cifrare il messaggio [v y j]

# La chiave di messaggio

- Adottata per aumentare la sicurezza
- Trasmessa due volte di seguito all'inizio di ogni messaggio, con l'assetto della chiave giornaliera
- Usata per regolare il nuovo assetto

# La chiave di messaggio

- Adottata per aumentare la sicurezza
- Trasmessa due volte di seguito all'inizio di ogni messaggio, con l'assetto della chiave giornaliera
- Usata per regolare il nuovo assetto

# La chiave di messaggio

- Adottata per aumentare la sicurezza
- Trasmessa due volte di seguito all'inizio di ogni messaggio, con l'assetto della chiave giornaliera
- Usata per regolare il nuovo assetto

# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 Cenni storici
  - La Macchina Enigma
  - Carta d'Identità
- 3 Struttura
  - Versione base
  - Modifiche
  - Combinazioni
- 4 Funzionamento**
  - Assetto giornaliero
  - Cifratura e Decifratura**
- 5 Guerra ad Enigma
  - I crittoanalisti polacchi
  - La Bomba di Turing
- 6 La crittografia nella WW II
  - I successi dei crittoanalisti

# Esempio: cifratura

- Chiave giornaliera: QCW
- Chiave di messaggio: PGH
- Il mittente posiziona i rotori secondo la chiave giornaliera
- Digita PGH PGH sulla tastiera, ottenendo KIV BJE
- Posiziona gli scambiatori secondo la chiave di messaggio
- Scrive il messaggio



# Esempio: cifratura

- Chiave giornaliera: QCW
- Chiave di messaggio: PGH
- Il mittente posiziona i rotori secondo la chiave giornaliera
- Digita PGH PGH sulla tastiera, ottenendo KIV BJE
- Posiziona gli scambiatori secondo la chiave di messaggio
- Scrive il messaggio

# Esempio: cifratura

- Chiave giornaliera: QCW
- Chiave di messaggio: PGH
- Il mittente posiziona i rotori secondo la chiave giornaliera
- Digita PGH PGH sulla tastiera, ottenendo KIV BJE
- Posiziona gli scambiatori secondo la chiave di messaggio
- Scrive il messaggio

# Esempio: cifratura

- Chiave giornaliera: QCW
- Chiave di messaggio: PGH
- Il mittente posiziona i rotori secondo la chiave giornaliera
- Digita PGH PGH sulla tastiera, ottenendo KIV BJE
- Posiziona gli scambiatori secondo la chiave di messaggio
- Scrive il messaggio

# Esempio: cifratura

- Chiave giornaliera: QCW
- Chiave di messaggio: PGH
- Il mittente posiziona i rotori secondo la chiave giornaliera
- Digita PGH PGH sulla tastiera, ottenendo KIV BJE
- Posiziona gli scambiatori secondo la chiave di messaggio
- Scrive il messaggio

# Esempio: cifratura

- Chiave giornaliera: QCW
- Chiave di messaggio: PGH
- Il mittente posiziona i rotori secondo la chiave giornaliera
- Digita PGH PGH sulla tastiera, ottenendo KIV BJE
- Posiziona gli scambiatori secondo la chiave di messaggio
- Scrive il messaggio

# Esempio: decifrazione

- Il destinatario posiziona i rotori sulla chiave giornaliera QCW
- Digita le prime sei lettere del messaggio ricevuto, ottenendo PGH PGH
- Posiziona gli scambiatori secondo la chiave di messaggio
- Digita il resto del testo cifrato sulla tastiera ottenendo il testo in chiaro

# Esempio: decifratura

- Il destinatario posiziona i rotori sulla chiave giornaliera QCW
- Digita le prime sei lettere del messaggio ricevuto, ottenendo PGH PGH
- Posiziona gli scambiatori secondo la chiave di messaggio
- Digita il resto del testo cifrato sulla tastiera ottenendo il testo in chiaro

# Esempio: decifratura

- Il destinatario posiziona i rotori sulla chiave giornaliera QCW
- Digita le prime sei lettere del messaggio ricevuto, ottenendo PGH PGH
- Posiziona gli scambiatori secondo la chiave di messaggio
- Digita il resto del testo cifrato sulla tastiera ottenendo il testo in chiaro



# Esempio: decifratura

- Il destinatario posiziona i rotori sulla chiave giornaliera QCW
- Digita le prime sei lettere del messaggio ricevuto, ottenendo PGH PGH
- Posiziona gli scambiatori secondo la chiave di messaggio
- Digita il resto del testo cifrato sulla tastiera ottenendo il testo in chiaro

# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 Cenni storici
  - La Macchina Enigma
  - Carta d'Identità
- 3 Struttura
  - Versione base
  - Modifiche
  - Combinazioni
- 4 Funzionamento
  - Assetto giornaliero
  - Cifratura e Decifratura
- 5 **Guerra ad Enigma**
  - **I crittoanalisti polacchi**
  - La Bomba di Turing
- 6 La crittografia nella WW II
  - I successi dei crittoanalisti

# I crittoanalisti polacchi

- Poca attenzione da parte degli Inglesi, forti della loro superiorità militare, ai messaggi crittati
- Prime intercettazioni di messaggi crittati di Enigma nella Polonia, minacciata dalla Germania (1926)
- Lavoro di intercettazione e raccolta dei crittogrammi fatta dall'Ufficio Cifre Polacco
- Reclutamento di matematici, anziché linguisti, tra cui Marian Rejewski

# I crittoanalisti polacchi

- Poca attenzione da parte degli Inglesi, forti della loro superiorità militare, ai messaggi crittati
- Prime **intercettazioni** di messaggi crittati di Enigma nella Polonia, minacciata dalla Germania (1926)
- Lavoro di intercettazione e raccolta dei crittogrammi fatta dall'**Ufficio Cifre Polacco**
- Reclutamento di **matematici**, anziché linguisti, tra cui Marian Rejewski

# I crittoanalisti polacchi

- Poca attenzione da parte degli Inglesi, forti della loro superiorità militare, ai messaggi crittati
- Prime **intercettazioni** di messaggi crittati di Enigma nella Polonia, minacciata dalla Germania (1926)
- Lavoro di intercettazione e raccolta dei crittogrammi fatta dall'**Ufficio Cifre Polacco**
- Reclutamento di **matematici**, anziché linguisti, tra cui Marian Rejewski

# I crittoanalisti polacchi

- Poca attenzione da parte degli Inglesi, forti della loro superiorità militare, ai messaggi crittati
- Prime **intercettazioni** di messaggi crittati di Enigma nella Polonia, minacciata dalla Germania (1926)
- Lavoro di intercettazione e raccolta dei crittogrammi fatta dall'**Ufficio Cifre Polacco**
- Reclutamento di **matematici**, anziché linguisti, tra cui Marian Rejewski

# I crittoanalisti polacchi

- Poca attenzione da parte degli Inglesi, forti della loro superiorità militare, ai messaggi crittati
- Prime **intercettazioni** di messaggi crittati di Enigma nella Polonia, minacciata dalla Germania (1926)
- Lavoro di intercettazione e raccolta dei crittogrammi fatta dall'**Ufficio Cifre Polacco**
- Reclutamento di **matematici**, anziché linguisti, tra cui Marian Rejewski

# La tecnica di Rejewski

- Basò la sua strategia sul fatto che la ripetizione è nemica della sicurezza
- La più ovvia ripetizione era quella della chiave di messaggio, cifrata due volte di seguito all'inizio di ogni testo trasmesso



# La tecnica di Rejewski

- Basò la sua strategia sul fatto che la ripetizione è nemica della sicurezza, perché crea degli schemi
- La più ovvia ripetizione era quella della chiave di messaggio, cifrata due volte di seguito all'inizio di ogni testo trasmesso cioè egli sfruttò il legame presente tra la I e la IV lettera, tra la II e la V, tra III e la VI

K I V B J E

# La tecnica di Rejewski

- Basò la sua strategia sul fatto che la ripetizione è nemica della sicurezza, perché crea degli schemi
- La più ovvia ripetizione era quella della chiave di messaggio, cifrata due volte di seguito all'inizio di ogni testo trasmesso cioè egli sfruttò il legame presente tra la I e la IV lettera, tra la II e la V, tra III e la VI

K I V B J E

# La tecnica di Rejewski

- Basò la sua strategia sul fatto che la ripetizione è nemica della sicurezza, perché crea degli schemi
- La più ovvia ripetizione era quella della chiave di messaggio, cifrata due volte di seguito all'inizio di ogni testo trasmesso cioè egli sfruttò il legame presente tra la I e la IV lettera, tra la II e la V, tra III e la VI

K I V B J E

# La tecnica di Rejewski

- Basò la sua strategia sul fatto che la ripetizione è nemica della sicurezza, perché crea degli schemi
- La più ovvia ripetizione era quella della chiave di messaggio, cifrata due volte di seguito all'inizio di ogni testo trasmesso cioè egli sfruttò il legame presente tra la I e la IV lettera, tra la II e la V, tra III e la VI

K I V B J E

# La tecnica di Rejewski

- Basò la sua strategia sul fatto che la ripetizione è nemica della sicurezza, perché crea degli schemi
- La più ovvia ripetizione era quella della chiave di messaggio, cifrata due volte di seguito all'inizio di ogni testo trasmesso cioè egli sfruttò il legame presente tra la I e la IV lettera, tra la II e la V, tra III e la VI

K I V B J E

# La nascita delle bombe

- Intercettando più messaggi, Rejewski riuscì a risalire a delle concatenazioni tra le lettere
- Capì, inoltre, che il numero dei collegamenti dipendeva solo dagli scambiatori e non dal pannello a prese multiple
- Per velocizzare il procedimento, Rejewski progettò congegni meccanici detti **bombe**

# La nascita delle bombe

- Intercettando più messaggi, Rejewski riuscì a risalire a delle concatenazioni tra le lettere
- Capì, inoltre, che il numero dei collegamenti dipendeva solo dagli scambiatori e non dal pannello a prese multiple in questo modo vennero escluse molte combinazioni di chiavi da provare per decrittare il messaggio, bastava cioè controllare le 17 576 posizioni dei rotori
- Per velocizzare il procedimento, Rejewski progettò congegni meccanici detti **bombe**

# La nascita delle bombe

- Intercettando più messaggi, Rejewski riuscì a risalire a delle concatenazioni tra le lettere
- Capì, inoltre, che il numero dei collegamenti dipendeva solo dagli scambiatori e non dal pannello a prese multiple: in questo modo vennero escluse molte combinazioni di chiavi da provare per decrittare il messaggio, bastava cioè controllare le 17 576 posizioni dei rotori
- Per velocizzare il procedimento, Rejewski progettò congegni meccanici detti **bombe**



# La nascita delle bombe

- Intercettando più messaggi, Rejewski riuscì a risalire a delle concatenazioni tra le lettere
- Capì, inoltre, che il numero dei collegamenti dipendeva solo dagli scambiatori e non dal pannello a prese multiple: in questo modo vennero escluse molte combinazioni di chiavi da provare per decrittare il messaggio, bastava cioè controllare le 17 576 posizioni dei rotori
- Per velocizzare il procedimento, Rejewski progettò congegni meccanici detti bombe

# La nascita delle bombe

- Intercettando più messaggi, Rejewski riuscì a risalire a delle concatenazioni tra le lettere
- Capì, inoltre, che il numero dei collegamenti dipendeva solo dagli scambiatori e non dal pannello a prese multiple: in questo modo vennero escluse molte combinazioni di chiavi da provare per decrittare il messaggio, bastava cioè controllare le 17 576 posizioni dei rotori
- Per velocizzare il procedimento, Rejewski progettò congegni meccanici detti **bombe**

# La nascita delle bombe

- Intercettando più messaggi, Rejewski riuscì a risalire a delle concatenazioni tra le lettere
- Capì, inoltre, che il numero dei collegamenti dipendeva solo dagli scambiatori e non dal pannello a prese multiple: in questo modo vennero escluse molte combinazioni di chiavi da provare per decrittare il messaggio, bastava cioè controllare le 17 576 posizioni dei rotori
- Per velocizzare il procedimento, Rejewski progettò congegni meccanici detti **bombe**

# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 Cenni storici
  - La Macchina Enigma
  - Carta d'Identità
- 3 Struttura
  - Versione base
  - Modifiche
  - Combinazioni
- 4 Funzionamento
  - Assetto giornaliero
  - Cifratura e Decifratura
- 5 **Guerra ad Enigma**
  - I crittoanalisti polacchi
  - **La Bomba di Turing**
- 6 La crittografia nella WW II
  - I successi dei crittoanalisti



# Bletchley Park

- Nuove misure per aumentare la sicurezza di Enigma portano all'inapplicabilità del metodo Rejewski
- Nel 1939 **Bletchley Park**, sede della GC&CS, divenne il centro di riferimento per le ricerche crittografiche
- Si reclutarono matematici tramite un concorso

# Bletchley Park

- Nuove misure per aumentare la sicurezza di Enigma portano all'inapplicabilità del metodo Rejewski
- Nel 1939 **Bletchley Park**, sede della GC&CS, divenne il centro di riferimento per le ricerche crittografiche
- Si reclutarono matematici tramite un concorso

# Bletchley Park

- Nuove misure per aumentare la sicurezza di Enigma portano all'inapplicabilità del metodo Rejewski
- Nel 1939 **Bletchley Park**, sede della GC&CS, divenne il centro di riferimento per le ricerche crittografiche
- Si reclutarono matematici tramite un concorso



# Bletchley Park

- Nuove misure per aumentare la sicurezza di Enigma portano all'inapplicabilità del metodo Rejewski
- Nel 1939 **Bletchley Park**, sede della GC&CS, divenne il centro di riferimento per le ricerche crittografiche
- Si reclutarono matematici tramite un concorso



# Cenni sulla tecnica di Alan Turing

- Struttura rigida dei messaggi intercettati
- Metodo intuitivo per l'elaborazione di un'ipotesi detta *crib*
- Confronto *crib*-crittogramma: corrispondenza lettera in chiaro-lettera cifrata

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

# Cenni sulla tecnica di Alan Turing

- **Struttura rigida dei messaggi intercettati**, ad esempio bollettini metereologici
- Metodo intuitivo per l'elaborazione di un'ipotesi detta *crib*
- Confronto *crib*-crittogramma: corrispondenza lettera in chiaro-lettera cifrata

Esempio:

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

# Cenni sulla tecnica di Alan Turing

- Struttura rigida dei messaggi intercettati, ad esempio bollettini metereologici
- Metodo intuitivo per l'elaborazione di un'ipotesi detta *crib*
- Confronto *crib*-crittogramma: corrispondenza lettera in chiaro-lettera cifrata

Esempio:

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

# Cenni sulla tecnica di Alan Turing

- Struttura rigida dei messaggi intercettati, ad esempio bollettini metereologici
- Metodo intuitivo per l'elaborazione di un'ipotesi detta *crib*
- Confronto *crib*-crittogramma: corrispondenza lettera in chiaro-lettera cifrata

Esempio:

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

# Cenni sulla tecnica di Alan Turing

- Struttura rigida dei messaggi intercettati, ad esempio bollettini metereologici
- Metodo intuitivo per l'elaborazione di un'ipotesi detta *crib*
- Confronto *crib*-crittogramma: corrispondenza lettera in chiaro-lettera cifrata

Esempio:

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

# Cenni sulla tecnica di Alan Turing

- Struttura rigida dei messaggi intercettati, ad esempio bollettini metereologici
- Metodo intuitivo per l'elaborazione di un'ipotesi detta *crib*
- Confronto *crib*-crittogramma: corrispondenza lettera in chiaro-lettera cifrata

Esempio:

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



# Cenni sulla tecnica di Alan Turing

- Struttura rigida dei messaggi intercettati, ad esempio bollettini metereologici
- Metodo intuitivo per l'elaborazione di un'ipotesi detta *crib*
- Confronto *crib*-crittogramma: corrispondenza lettera in chiaro-lettera cifrata

Esempio:

```

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
  
```

# Cenni sulla tecnica di Alan Turing

- Associazione di un numero ad ogni coppia di lettere rappresentante uno dei possibili stati della macchina che permetteva di ottenere quella cifratura:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
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

- Individuazione di percorsi chiusi di lettere, detti *loop*, sfruttando le corrispondenze trovate.  
Ad esempio:  $E \rightarrow 5 \rightarrow T \rightarrow 3 \rightarrow I \rightarrow 21 \rightarrow A \rightarrow 23 \rightarrow E$
- Possibile rappresentazione di questi *loop* con dei circuiti elettrici e successiva meccanizzazione della ricerca di ordine e posizione corretti dei rotori

# Cenni sulla tecnica di Alan Turing

- Associazione di un numero ad ogni coppia di lettere rappresentante uno dei possibili stati della macchina che permetteva di ottenere quella cifratura:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
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

- Individuazione di percorsi chiusi di lettere, detti *loop*, sfruttando le corrispondenze trovate.  
Ad esempio:  $E \rightarrow 5 \rightarrow T \rightarrow 3 \rightarrow I \rightarrow 21 \rightarrow A \rightarrow 23 \rightarrow E$
- Possibile rappresentazione di questi *loop* con dei circuiti elettrici e successiva meccanizzazione della ricerca di ordine e posizione corretti dei rotori

# Cenni sulla tecnica di Alan Turing

- Associazione di un numero ad ogni coppia di lettere rappresentante uno dei possibili stati della macchina che permetteva di ottenere quella cifratura:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
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

- Individuazione di percorsi chiusi di lettere, detti *loop*, sfruttando le corrispondenze trovate.  
Ad esempio:  $E \rightarrow 5 \rightarrow T \rightarrow 3 \rightarrow I \rightarrow 21 \rightarrow A \rightarrow 23 \rightarrow E$
- Possibile rappresentazione di questi *loop* con dei circuiti elettrici e successiva meccanizzazione della ricerca di ordine e posizione corretti dei rotori

# Cenni sulla tecnica di Alan Turing

- Associazione di un numero ad ogni coppia di lettere rappresentante uno dei possibili stati della macchina che permetteva di ottenere quella cifratura:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
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

- Individuazione di percorsi chiusi di lettere, detti *loop*, sfruttando le corrispondenze trovate.  
Ad esempio:  $E \rightarrow 5 \rightarrow T \rightarrow 3 \rightarrow I \rightarrow 21 \rightarrow A \rightarrow 23 \rightarrow E$
- Possibile rappresentazione di questi *loop* con dei circuiti elettrici e successiva meccanizzazione della ricerca di ordine e posizione corretti dei rotori

# Cenni sulla tecnica di Alan Turing

- Associazione di un numero ad ogni coppia di lettere rappresentante uno dei possibili stati della macchina che permetteva di ottenere quella cifratura:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
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

- Individuazione di percorsi chiusi di lettere, detti *loop*, sfruttando le corrispondenze trovate.  
Ad esempio:  $E \rightarrow 5 \rightarrow T \rightarrow 3 \rightarrow I \rightarrow 21 \rightarrow A \rightarrow 23 \rightarrow E$
- Possibile rappresentazione di questi *loop* con dei circuiti elettrici e successiva meccanizzazione della ricerca di ordine e posizione corretti dei rotori

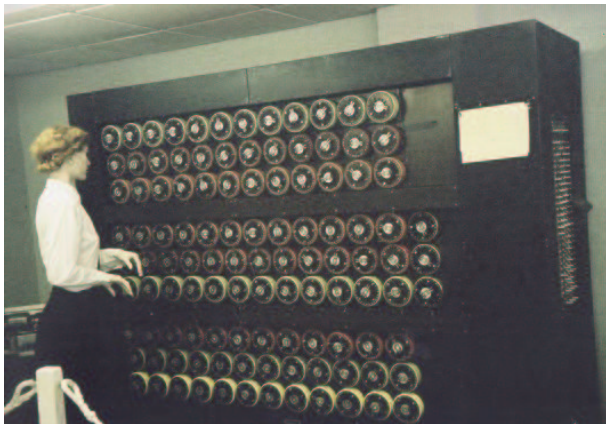
# Cenni sulla tecnica di Alan Turing

- Associazione di un numero ad ogni coppia di lettere rappresentante uno dei possibili stati della macchina che permetteva di ottenere quella cifratura:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
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

- Individuazione di percorsi chiusi di lettere, detti *loop*, sfruttando le corrispondenze trovate.  
Ad esempio:  $E \rightarrow 5 \rightarrow T \rightarrow 3 \rightarrow I \rightarrow 21 \rightarrow A \rightarrow 23 \rightarrow E$
- Possibile rappresentazione di questi *loop* con dei circuiti elettrici e successiva meccanizzazione della ricerca di ordine e posizione corretti dei rotori

# Costruzione della Bomba





# Costruzione della Bomba

- **Necessità di collegare più macchine Enigma insieme:** modifica della macchina originale, in modo che l'*output* di una costituisca l'*input* di un'altra: **macchina Enigma aperta**
- **Costruzione della Bomba:** pesava circa una tonnellata ed era contenuta in un involucro di metallo, largo circa 2.10m, alto poco meno 2m, e profondo 0.6m; divisa in tre batterie ognuna delle quali costituita da tre file di 12 tamburi del diametro di 12cm circa. Ogni colonna di ogni batteria costituiva una macchina Enigma aperta

# Costruzione della Bomba

- Necessità di collegare più macchine Enigma insieme: modifica della macchina originale, in modo che l'*output* di una costituisca l'*input* di un'altra: **macchina Enigma aperta**
- Costruzione della Bomba: pesava circa una tonnellata ed era contenuta in un involucro di metallo, largo circa 2.10m, alto poco meno 2m, e profondo 0.6m; divisa in tre batterie ognuna delle quali costituita da tre file di 12 tamburi del diametro di 12cm circa. Ogni colonna di ogni batteria costituiva una macchina Enigma aperta

# Costruzione della Bomba

- Necessità di collegare più macchine Enigma insieme: modifica della macchina originale, in modo che l'*output* di una costituisca l'*input* di un'altra: **macchina Enigma aperta**
- Costruzione della Bomba: pesava circa una tonnellata ed era contenuta in un involucro di metallo, largo circa 2.10m, alto poco meno 2m, e profondo 0.6m; divisa in tre batterie ognuna delle quali costituita da tre file di 12 tamburi del diametro di 12cm circa. Ogni colonna di ogni batteria costituiva una macchina Enigma aperta

# Costruzione della Bomba

- Necessità di collegare più macchine Enigma insieme: modifica della macchina originale, in modo che l'*output* di una costituisca l'*input* di un'altra: **macchina Enigma aperta**
- **Costruzione della Bomba**: pesava circa una tonnellata ed era contenuta in un involucro di metallo, largo circa  $2.10m$ , alto poco meno  $2m$ , e profondo  $0.6m$ ; divisa in tre batterie ognuna delle quali costituita da tre file di 12 tamburi del diametro di  $12cm$  circa. Ogni colonna di ogni batteria costituiva una macchina Enigma aperta

# Costruzione della Bomba

- Necessità di collegare più macchine Enigma insieme: modifica della macchina originale, in modo che l'*output* di una costituisca l'*input* di un'altra: **macchina Enigma aperta**
- Costruzione della Bomba: pesava circa una tonnellata ed era contenuta in un involucro di metallo, largo circa 2.10m, alto poco meno 2m, e profondo 0.6m; divisa in tre batterie ognuna delle quali costituita da tre file di 12 tamburi del diametro di 12cm circa. Ogni colonna di ogni batteria costituiva una macchina Enigma aperta

# Costruzione della Bomba

- Necessità di collegare più macchine Enigma insieme: modifica della macchina originale, in modo che l'*output* di una costituisca l'*input* di un'altra: **macchina Enigma aperta**
- Costruzione della Bomba: pesava circa una tonnellata ed era contenuta in un involucro di metallo, largo circa  $2.10m$ , alto poco meno  $2m$ , e profondo  $0.6m$ ; divisa in tre batterie ognuna delle quali costituita da tre file di 12 tamburi del diametro di  $12cm$  circa. Ogni colonna di ogni batteria costituiva una macchina Enigma aperta

# Costruzione della Bomba

- Necessità di collegare più macchine Enigma insieme: modifica della macchina originale, in modo che l'*output* di una costituisca l'*input* di un'altra: **macchina Enigma aperta**
- Costruzione della Bomba: pesava circa una tonnellata ed era contenuta in un involucro di metallo, largo circa  $2.10m$ , alto poco meno  $2m$ , e profondo  $0.6m$ ; divisa in tre batterie ognuna delle quali costituita da tre file di 12 tamburi del diametro di  $12cm$  circa. Ogni colonna di ogni batteria costituiva una macchina Enigma aperta

# La Macchina Enigma

- 1 Crittografia: un po' di storia
- 2 Cenni storici
  - La Macchina Enigma
  - Carta d'Identità
- 3 Struttura
  - Versione base
  - Modifiche
  - Combinazioni
- 4 Funzionamento
  - Assetto giornaliero
  - Cifratura e Decifratura
- 5 Guerra ad Enigma
  - I crittoanalisti polacchi
  - La Bomba di Turing
- 6 **La crittografia nella WW II**
  - **I successi dei crittoanalisti**



# La Battaglia dell'Atlantico

- Dal 1940, i Nazisti impiegarono una flotta di sottomarini (*U-boat*) per affondare le navi commerciali inglesi
- La comunicazione tra i sottomarini avveniva via radio attraverso dei messaggi crittati da **Enigma navale**, una macchina molto più sofisticata rispetto alla versione base
- Gli Inglesi riuscirono ad intercettare tali messaggi ma non furono in grado di decrittarli, fino al ritrovamento di una macchina Enigma in un sottomarino tedesco in avaria
- I crittoanalisti inglesi riuscirono a violare anche questo codice considerato inattaccabile evitando la sconfitta su mare

# La Battaglia dell'Atlantico

- Dal 1940, i Nazisti impiegarono una flotta di sottomarini (*U-boat*) per affondare le navi commerciali inglesi
- La comunicazione tra i sottomarini avveniva via radio attraverso dei messaggi crittati da **Enigma navale**, una macchina molto più sofisticata rispetto alla versione base
- Gli Inglesi riuscirono ad intercettare tali messaggi ma non furono in grado di decrittarli, fino al ritrovamento di una macchina Enigma in un sottomarino tedesco in avaria
- I crittoanalisti inglesi riuscirono a violare anche questo codice considerato inattaccabile evitando la sconfitta su mare

# La Battaglia dell'Atlantico

- Dal 1940, i Nazisti impiegarono una flotta di sottomarini (*U-boat*) per affondare le navi commerciali inglesi
- La comunicazione tra i sottomarini avveniva via radio attraverso dei messaggi crittati da **Enigma navale**, una macchina molto più sofisticata rispetto alla versione base
- Gli Inglesi riuscirono ad intercettare tali messaggi ma non furono in grado di decrittarli, fino al ritrovamento di una macchina Enigma in un sottomarino tedesco in avaria
- I crittoanalisti inglesi riuscirono a violare anche questo codice considerato inattaccabile evitando la sconfitta su mare

# La Battaglia dell'Atlantico

- Dal 1940, i Nazisti impiegarono una flotta di sottomarini (*U-boat*) per affondare le navi commerciali inglesi
- La comunicazione tra i sottomarini avveniva via radio attraverso dei messaggi crittati da **Enigma navale**, una macchina molto più sofisticata rispetto alla versione base
- Gli Inglesi riuscirono ad intercettare tali messaggi ma non furono in grado di decrittarli, fino al ritrovamento di una macchina Enigma in un sottomarino tedesco in avaria
- I crittoanalisti inglesi riuscirono a violare anche questo codice considerato inattaccabile evitando la sconfitta su mare

# La Battaglia dell'Atlantico

- Dal 1940, i Nazisti impiegarono una flotta di sottomarini (*U-boat*) per affondare le navi commerciali inglesi
- La comunicazione tra i sottomarini avveniva via radio attraverso dei messaggi crittati da **Enigma navale**, una macchina molto più sofisticata rispetto alla versione base
- Gli Inglesi riuscirono ad intercettare tali messaggi ma non furono in grado di decrittarli, fino al ritrovamento di una macchina Enigma in un sottomarino tedesco in avaria
- I crittoanalisti inglesi riuscirono a violare anche questo codice considerato inattaccabile evitando la sconfitta su mare

# La Battaglia dell'Atlantico

- Dal 1940, i Nazisti impiegarono una flotta di sottomarini (*U-boat*) per affondare le navi commerciali inglesi
- La comunicazione tra i sottomarini avveniva via radio attraverso dei messaggi crittati da **Enigma navale**, una macchina molto più sofisticata rispetto alla versione base
- Gli Inglesi riuscirono ad intercettare tali messaggi ma non furono in grado di decrittarli, fino al ritrovamento di una macchina Enigma in un sottomarino tedesco in avaria
- I crittoanalisti inglesi riuscirono a violare anche questo codice considerato inattaccabile **evitando la sconfitta su mare**

# La Battaglia dell'Atlantico

- Dal 1940, i Nazisti impiegarono una flotta di sottomarini (*U-boat*) per affondare le navi commerciali inglesi
- La comunicazione tra i sottomarini avveniva via radio attraverso dei messaggi crittati da **Enigma navale**, una macchina molto più sofisticata rispetto alla versione base
- Gli Inglesi riuscirono ad intercettare tali messaggi ma non furono in grado di decrittarli, fino al ritrovamento di una macchina Enigma in un sottomarino tedesco in avaria
- I crittoanalisti inglesi riuscirono a violare anche questo codice considerato inattaccabile evitando la sconfitta su mare

# Altri successi

- **La Battaglia di Capo Matapan (1941)**: la decrittazione da parte degli Inglesi di alcuni messaggi cifrati della marina tedesca circa l'esatta posizione della flotta italiana, ne causò la disfatta
- **Sbarco in Normandia (1944)**: gli Americani, in grado di leggere gran parte dei messaggi degli alti comandi tedeschi, ebbero conferma che Hitler aveva creduto alla falsa notizia di uno sbarco alleato nei pressi di Calais. Organizzarono così lo sbarco in Normandia sicuri di incontrare poca resistenza



# Altri successi

- **La Battaglia di Capo Matapan (1941)**: la decrittazione da parte degli Inglesi di alcuni messaggi cifrati della marina tedesca circa l'esatta posizione della flotta italiana, ne causò la disfatta
- **Sbarco in Normandia (1944)** gli Americani, in grado di leggere gran parte dei messaggi degli alti comandi tedeschi, ebbero conferma che Hitler aveva creduto alla falsa notizia di uno sbarco alleato nei pressi di Calais. Organizzarono così lo sbarco in Normandia sicuri di incontrare poca resistenza

# Altri successi

- **La Battaglia di Capo Matapan (1941)**: la decrittazione da parte degli Inglesi di alcuni messaggi cifrati della marina tedesca circa l'esatta posizione della flotta italiana, ne causò la disfatta
- **Sbarco in Normandia (1944)**: gli Americani, in grado di leggere gran parte dei messaggi degli alti comandi tedeschi, ebbero conferma che Hitler aveva creduto alla falsa notizia di uno sbarco alleato nei pressi di Calais. Organizzarono così lo sbarco in Normandia sicuri di incontrare poca resistenza

# Altri successi

- **La Battaglia di Capo Matapan (1941)**: la decrittazione da parte degli Inglesi di alcuni messaggi cifrati della marina tedesca circa l'esatta posizione della flotta italiana, ne causò la disfatta
- **Sbarco in Normandia (1944)**: gli Americani, in grado di leggere gran parte dei messaggi degli alti comandi tedeschi, ebbero conferma che Hitler aveva creduto alla falsa notizia di uno sbarco alleato nei pressi di Calais. Organizzarono così lo sbarco in Normandia sicuri di incontrare poca resistenza

## Altri successi

- **La Battaglia di Capo Matapan (1941)**: la decrittazione da parte degli Inglesi di alcuni messaggi cifrati della marina tedesca circa l'esatta posizione della flotta italiana, ne causò la disfatta
- **Sbarco in Normandia (1944)**: gli Americani, in grado di leggere gran parte dei messaggi degli alti comandi tedeschi, ebbero conferma che Hitler aveva creduto alla falsa notizia di uno sbarco alleato nei pressi di Calais. Organizzarono così lo sbarco in Normandia sicuri di incontrare poca resistenza

## Altri successi

- **La Battaglia di Capo Matapan (1941)**: la decrittazione da parte degli Inglesi di alcuni messaggi cifrati della marina tedesca circa l'esatta posizione della flotta italiana, ne causò la disfatta
- **Sbarco in Normandia (1944)**: gli Americani, in grado di leggere gran parte dei messaggi degli alti comandi tedeschi, ebbero conferma che Hitler aveva creduto alla falsa notizia di uno sbarco alleato nei pressi di Calais. Organizzarono così lo sbarco in Normandia sicuri di incontrare poca resistenza