Codici Segreti

Agostino Dovier

Dip di Scienze Matematiche, Informatiche, e Fisiche Univ. di Udine

24 febbraio 2016

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

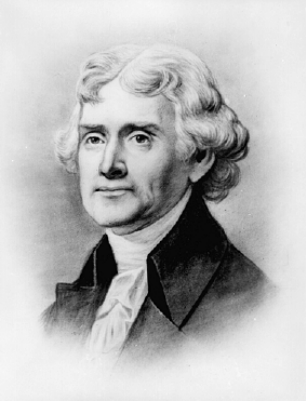
Trasposizioni

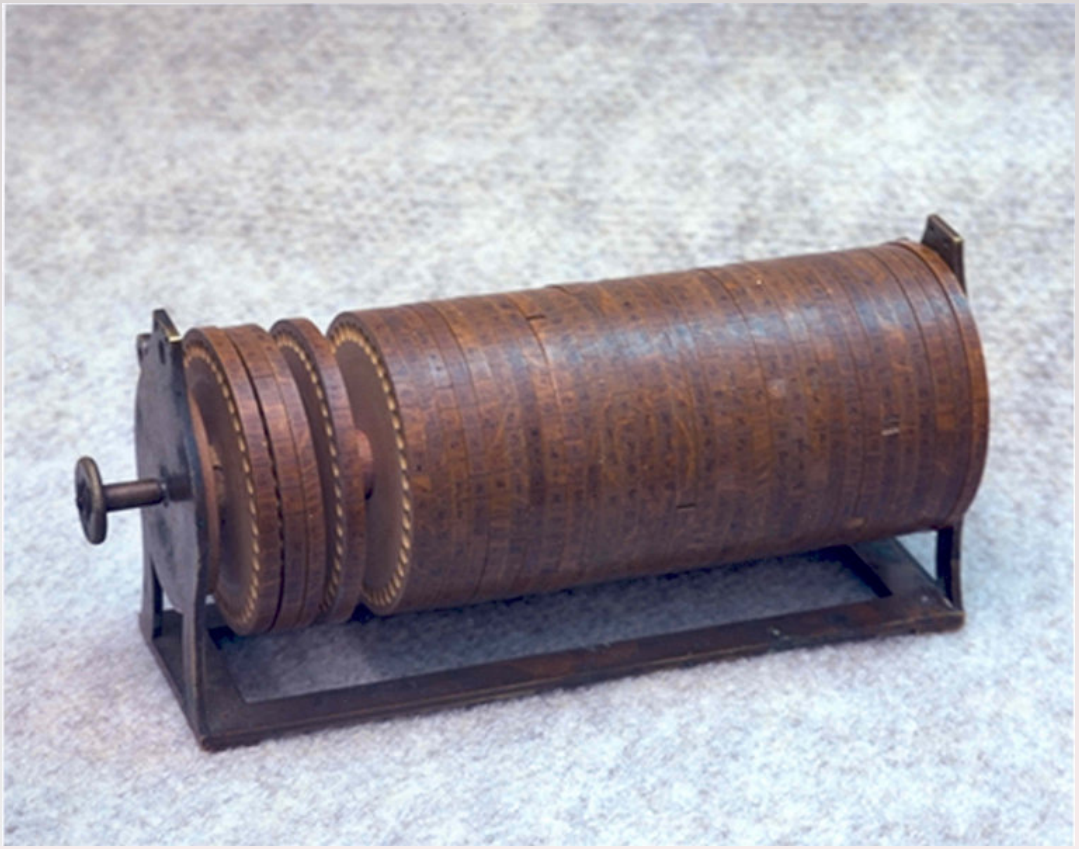
DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Automazione della crittografia

Il rotore di Thomas Jefferson (1743–1826)





Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

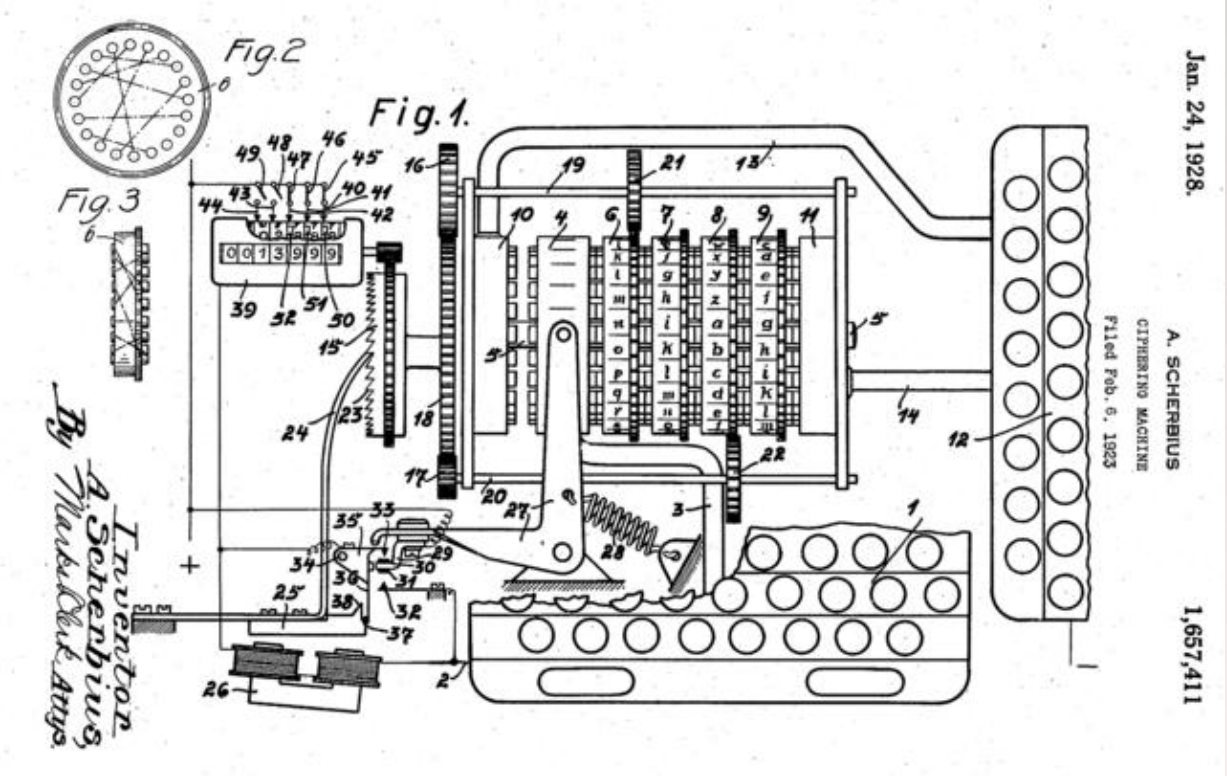
Decifrazione

Sicurezza

Automazione della crittografia

Arthur Scherbius (1878–1929)

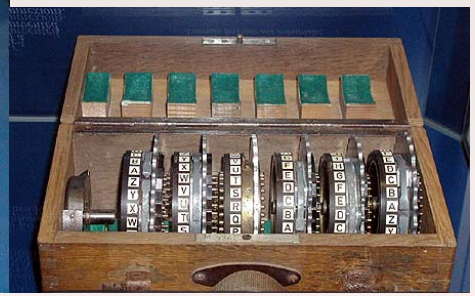
Nel 1918 brevetta una macchina da cifra a rotori (multipli)



Automazione della crittografia

Enigma

Nel 1923 Scherbius commercializza l'Enigma.



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

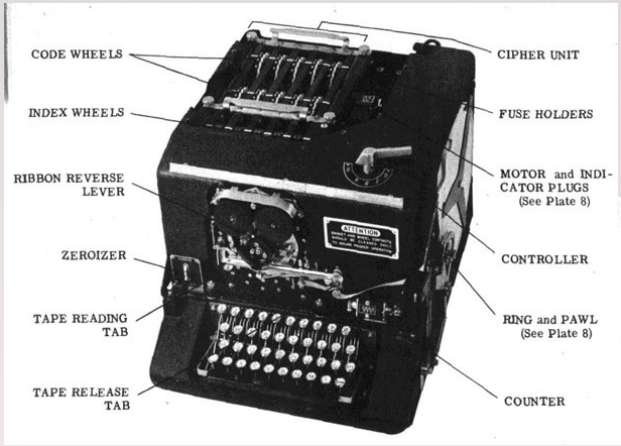
Decifrazione

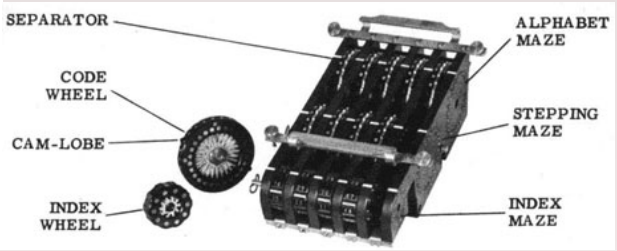
Sicurezza

Automazione della crittografia

Edward Hugh Hebern (1869–1952)

Negli USA nel 1932 Hebern progetta macchina analoga (con 15 rotori): SIGABA





Sarà usata dall'esercito/marina USA. Non fu mai forzato

C'è da dire che Turing non ci provò, essendo alleato.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

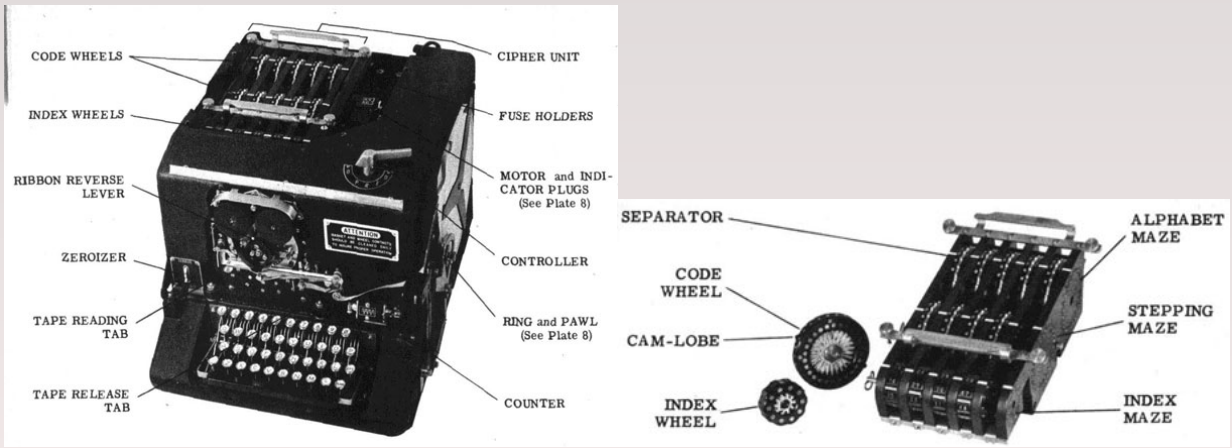
Decifrazione

Sicurezza

Automazione della crittografia

Edward Hugh Hebern (1869–1952)

Negli USA nel 1932 Hebern progetta macchina analoga (con 15 rotori): SIGABA



Sarà usata dall'esercito/marina USA. Non fu mai forzato
C'è da dire che Turing non ci provò, essendo alleato.

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

TURING . . .

ALAN MATHISON TURING 23/06/1912–07/06/1954

ATHLETICS

MARATHON AND DECATHLON CHAMPIONSHIPS

The Amateur Athletic Association championships for this year were concluded at Loughborough College Stadium, Leicestershire, on Saturday, with the second, and last, day of the Decathlon and the decision of the Marathon championship.

MARATHON CHAMPIONSHIP (26 miles 385 yds.) (record: 2hrs. 30min. 57.6sec., by H. W. Payne, Windsor to Stamford Bridge, on July 5, 1929; standard time: 3hrs. 5min.).—J. T. Holden (Tipton Harriers), 2hrs. 33min. 20 1-5sec., 1; T. Richards (South London Harriers), 2hrs. 36mni. 7sec., 2; D. McNab Robertson (Maryhill Harriers, Glasgow), 2hrs. 37min. 54 3-5sec., 3; J. E. Farrell (Maryhill Harriers), 2hrs. 39min. 46 2-5sec., 4; Dr. A. M. Turing (Walton A.C.), 2hrs. 46min. 3sec., 5; L. H. Griffiths (Reading A.C.), 2hrs. 47min. 50 2-5sec., 6.

DECATHLON CHAMPIONSHIP.—H. J. Moesgaard-Kjeldsen (Polytechnic Harriers, London), 5,965 points, 1; Captain H. Whittle (Army and Reading A.C.), 5,650, 2;

Nel 1948 (Olimpiadi di Londra) Delfo Cabrera vinse in 2h34’51”

AUTOMAZIONE DELLA CRITTOGRAFIA

L’ENIGMA

TURING A BLETCHLEY PARK

FUNZIONAMENTO DELL’ENIGMA

DECRITTAZIONE DELL’ENIGMA

FILMS E LIBRI

NOTE FINALI

TRASPOSIZIONI

DES

INTRODUZIONE

CIFRAZIONE

DECIFRAZIONE

DECRITTAZIONE

AES

INTRODUZIONE

FUNZIONAMENTO

TRASFORMAZIONI

CHIAVE

DECIFRAZIONE

SICUREZZA

TURING . . .

ALAN MATHISON TURING 23/06/1912–07/06/1954

ATHLETICS

MARATHON AND DECATHLON CHAMPIONSHIPS

The Amateur Athletic Association championships for this year were concluded at Loughborough College Stadium, Leicestershire, on Saturday, with the second, and last, day of the Decathlon and the decision of the Marathon championship.

MARATHON CHAMPIONSHIP (26 miles 385 yds.) (record: 2hrs. 30min. 57.6sec., by H. W. Payne, Windsor to Stamford Bridge, on July 5, 1929; standard time: 3hrs. 5min.).—J. T. Holden (Tipton Harriers), 2hrs. 33min. 20 1-5sec., 1; T. Richards (South London Harriers), 2hrs. 36mni. 7sec., 2; D. McNab Robertson (Maryhill Harriers, Glasgow), 2hrs. 37min. 54 3-5sec., 3; J. E. Farrell (Maryhill Harriers), 2hrs. 39min. 46 2-5sec., 4; Dr. A. M. Turing (Walton A.C.), 2hrs. 46min. 3sec., 5; L. H. Griffiths (Reading A.C.), 2hrs. 47min. 50 2-5sec., 6.

DECATHLON CHAMPIONSHIP.—H. J. Moesgaard-Kjeldsen (Polytechnic Harriers, London), 5,965 points, 1; Captain H. Whittle (Army and Reading A.C.), 5,650, 2;

Nel 1948 (Olimpiadi di Londra) Delfo Cabrera vinse in 2h34’51”

AUTOMAZIONE DELLA CRITTOGRAFIA

L’ENIGMA

TURING A BLETCHLEY PARK

FUNZIONAMENTO DELL’ENIGMA

DECRITTAZIONE DELL’ENIGMA

FILMS E LIBRI

NOTE FINALI

TRASPOSIZIONI

DES

INTRODUZIONE

CIFRAZIONE

DECIFRAZIONE

DECRITTAZIONE

AES

INTRODUZIONE

FUNZIONAMENTO

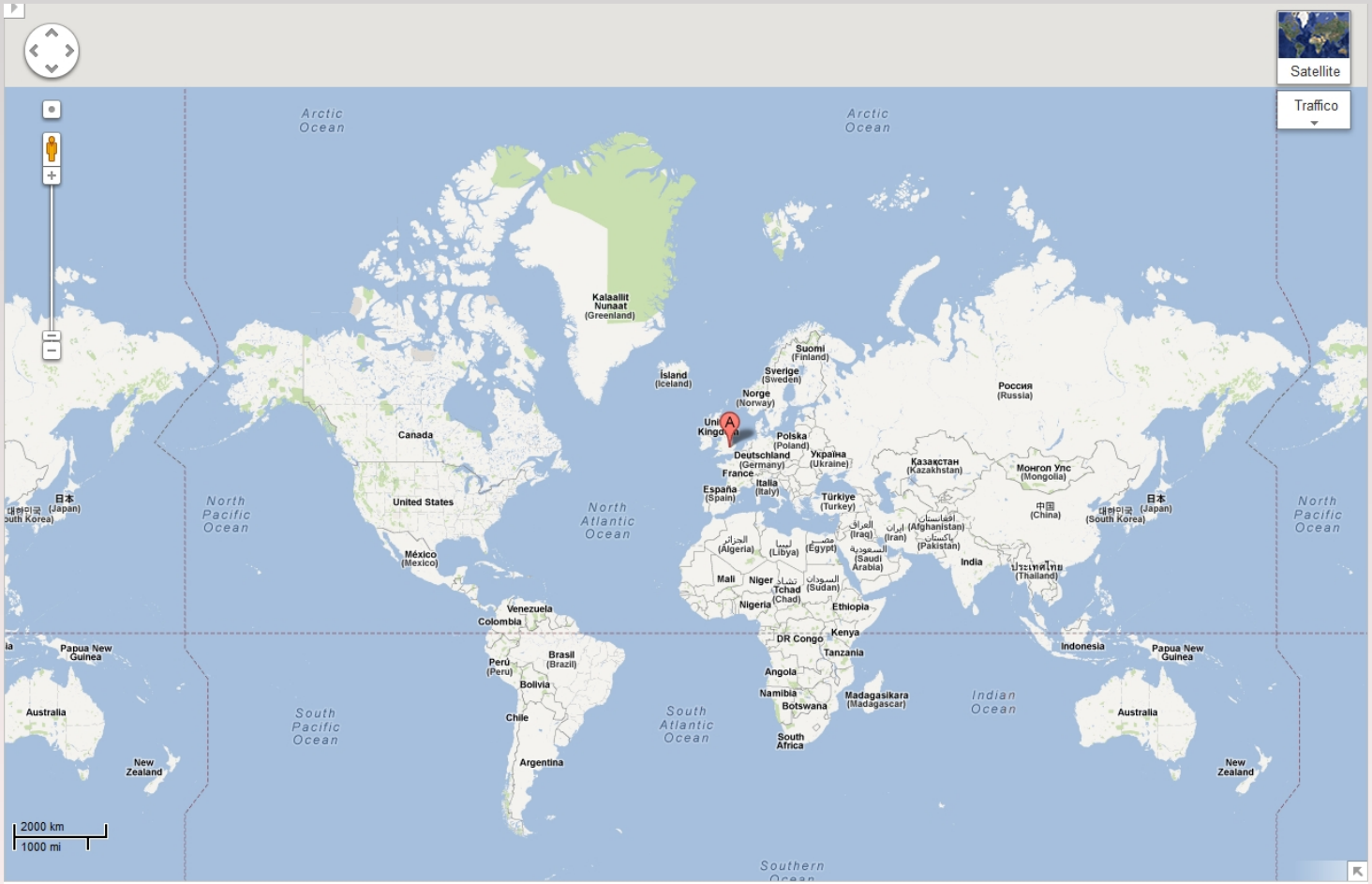
TRASFORMAZIONI

CHIAVE

DECIFRAZIONE

SICUREZZA

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

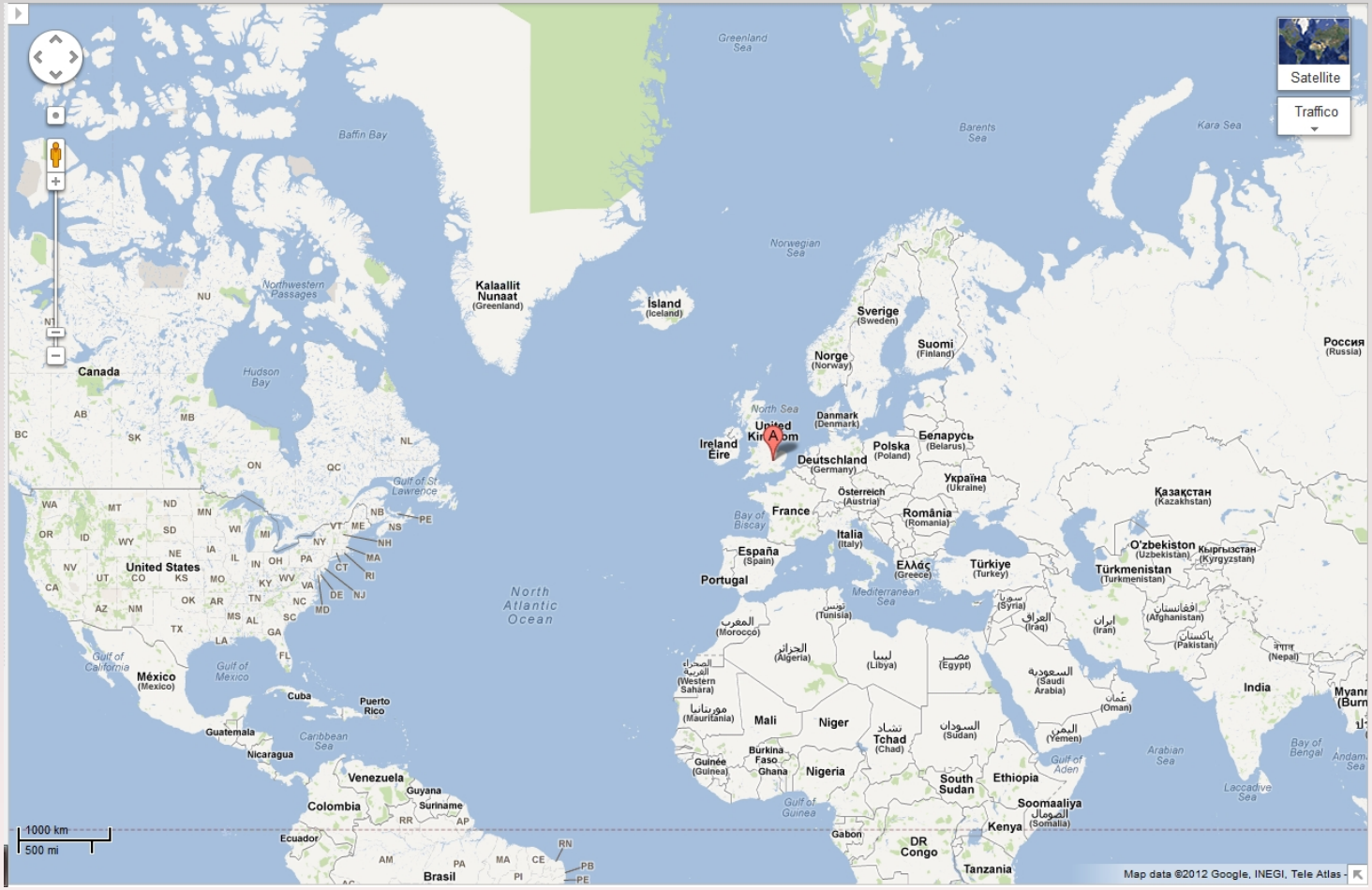
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

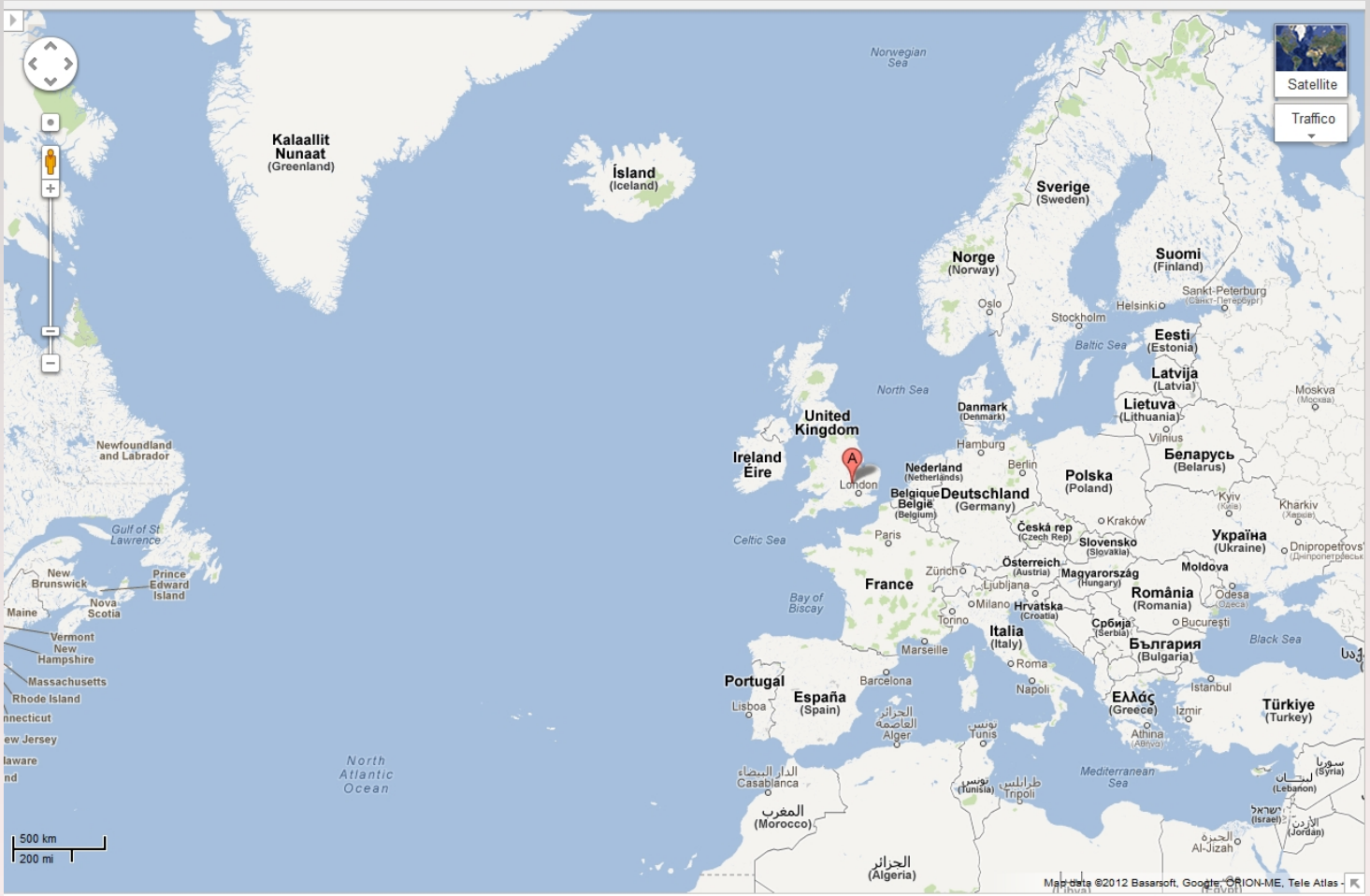
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

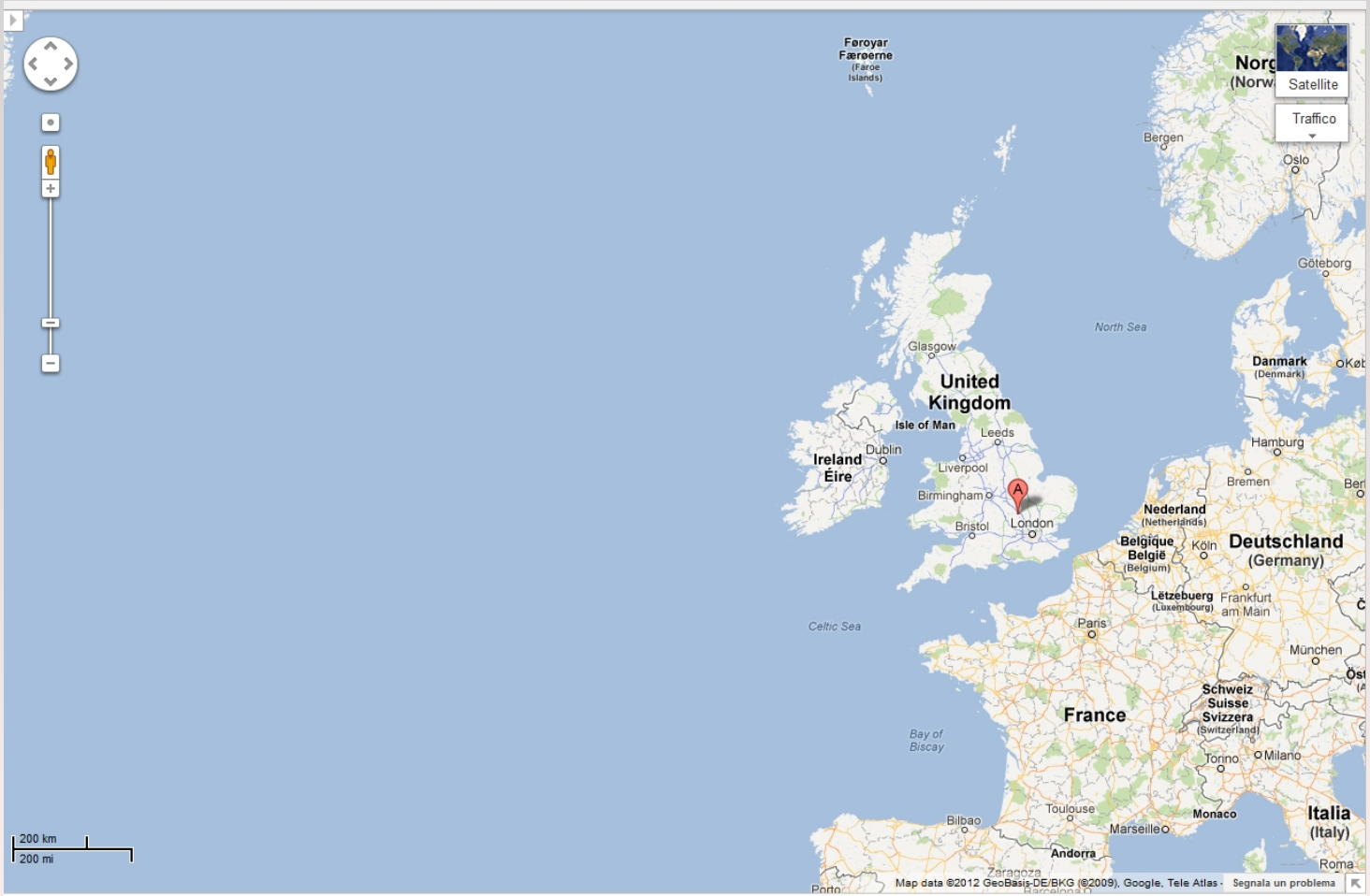
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

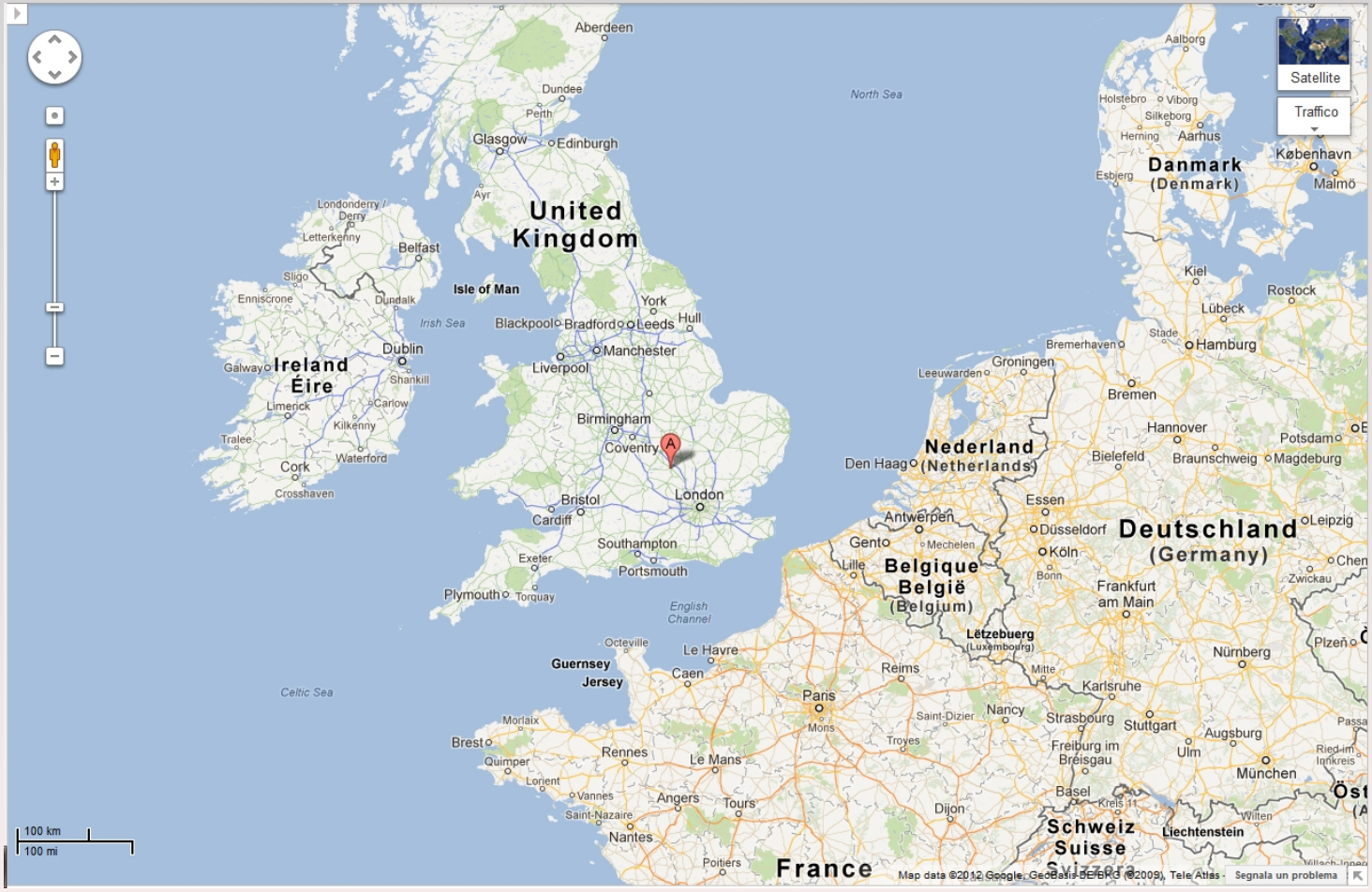
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

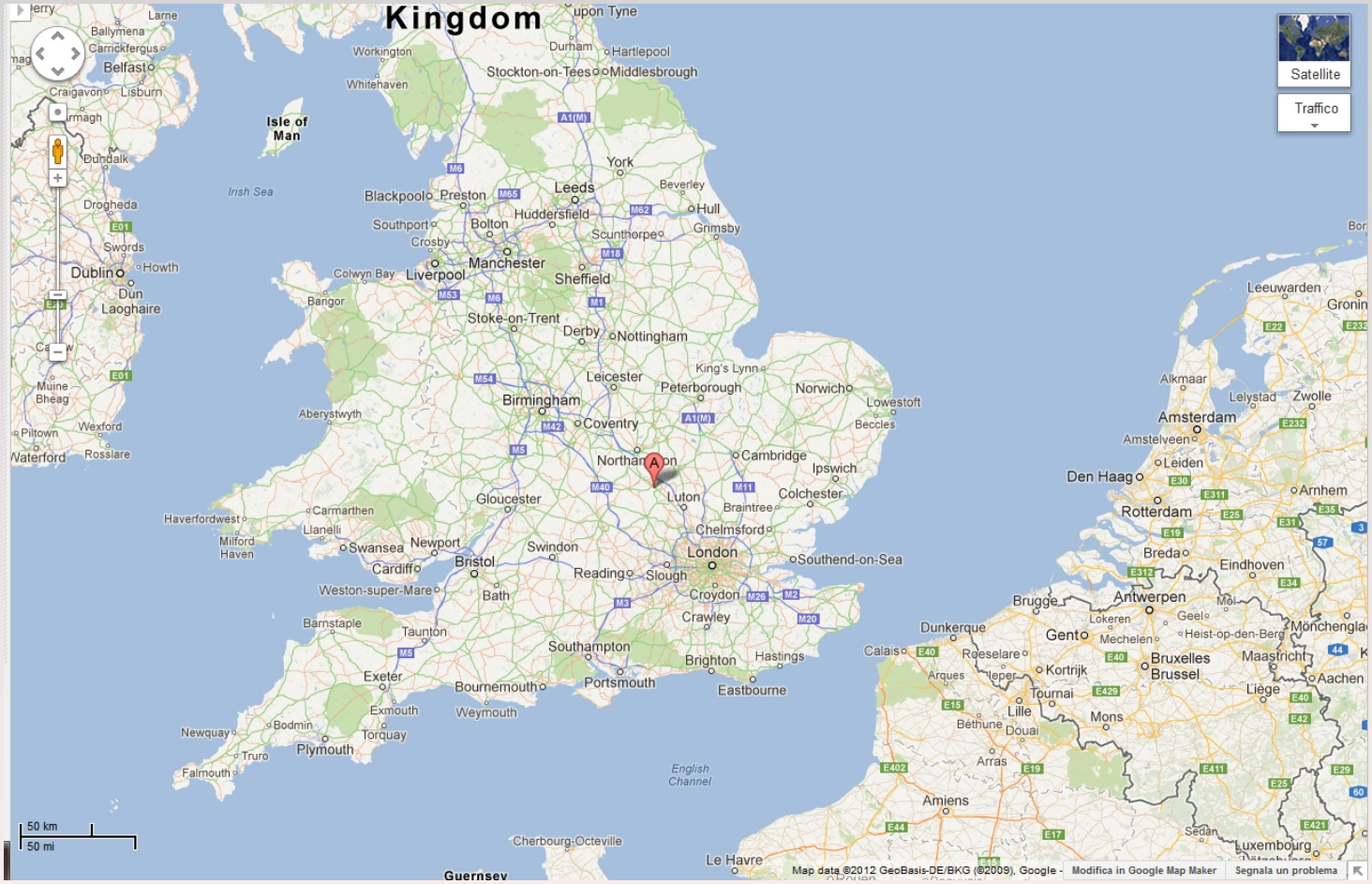
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

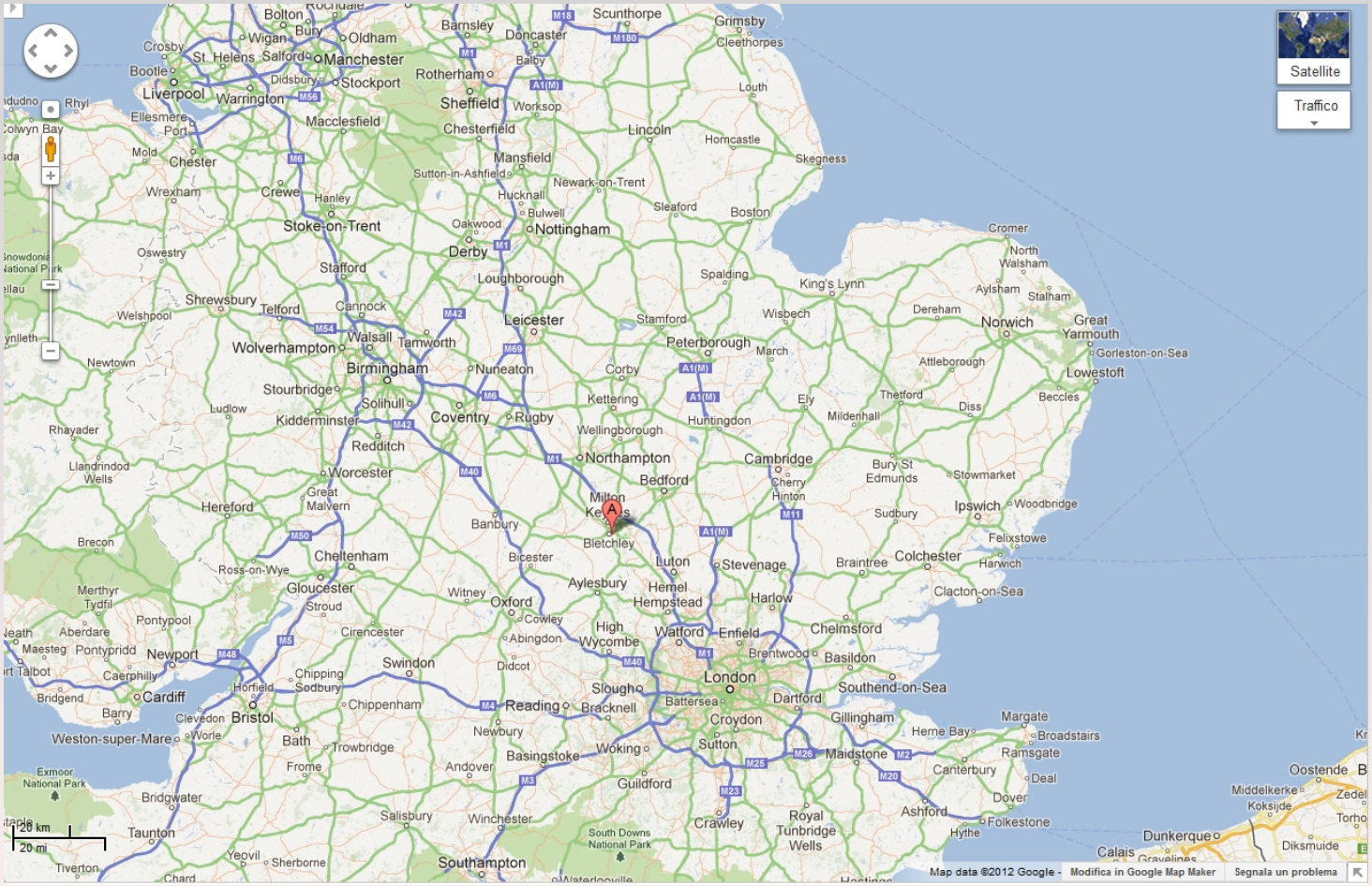
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

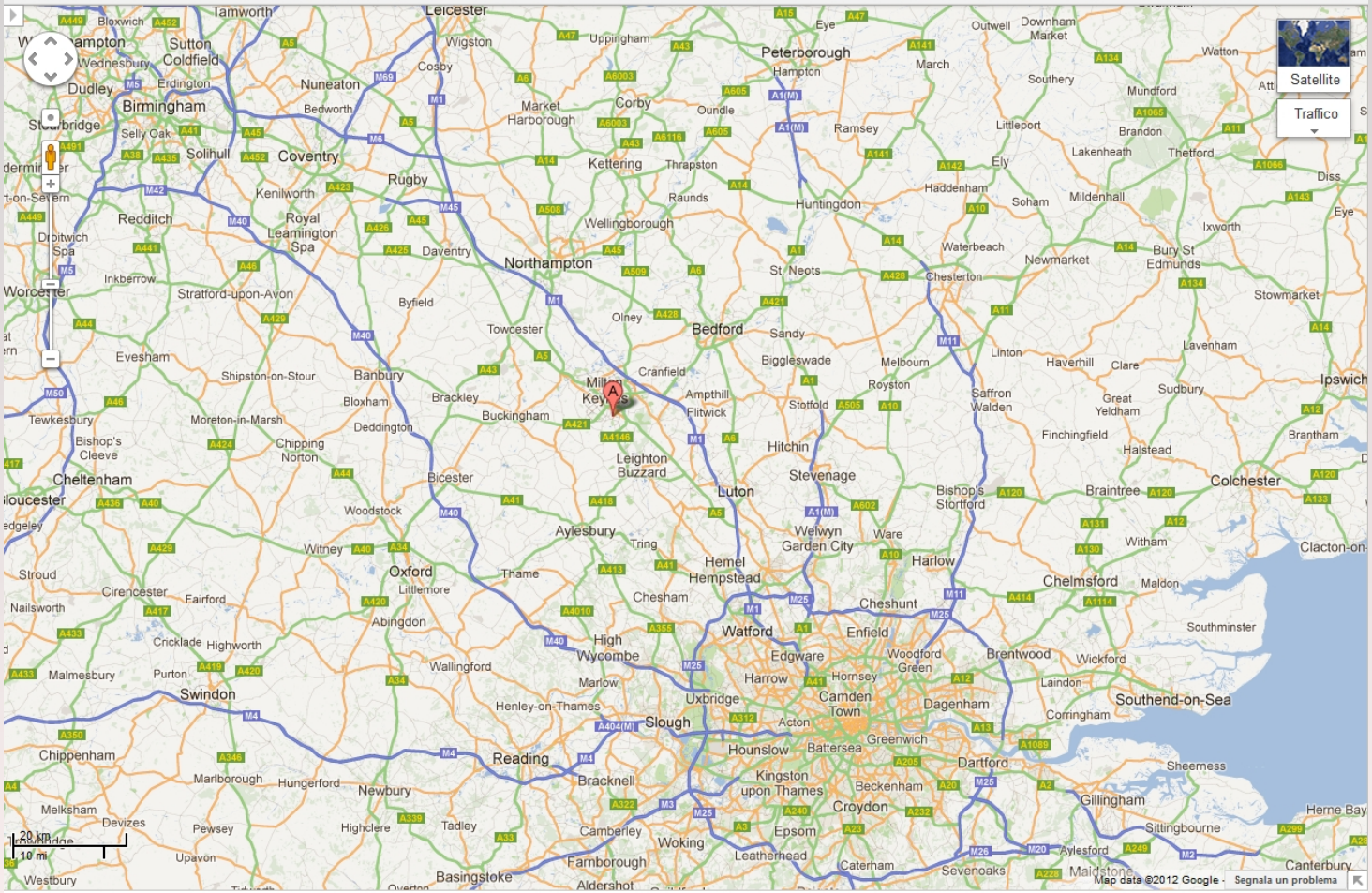
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

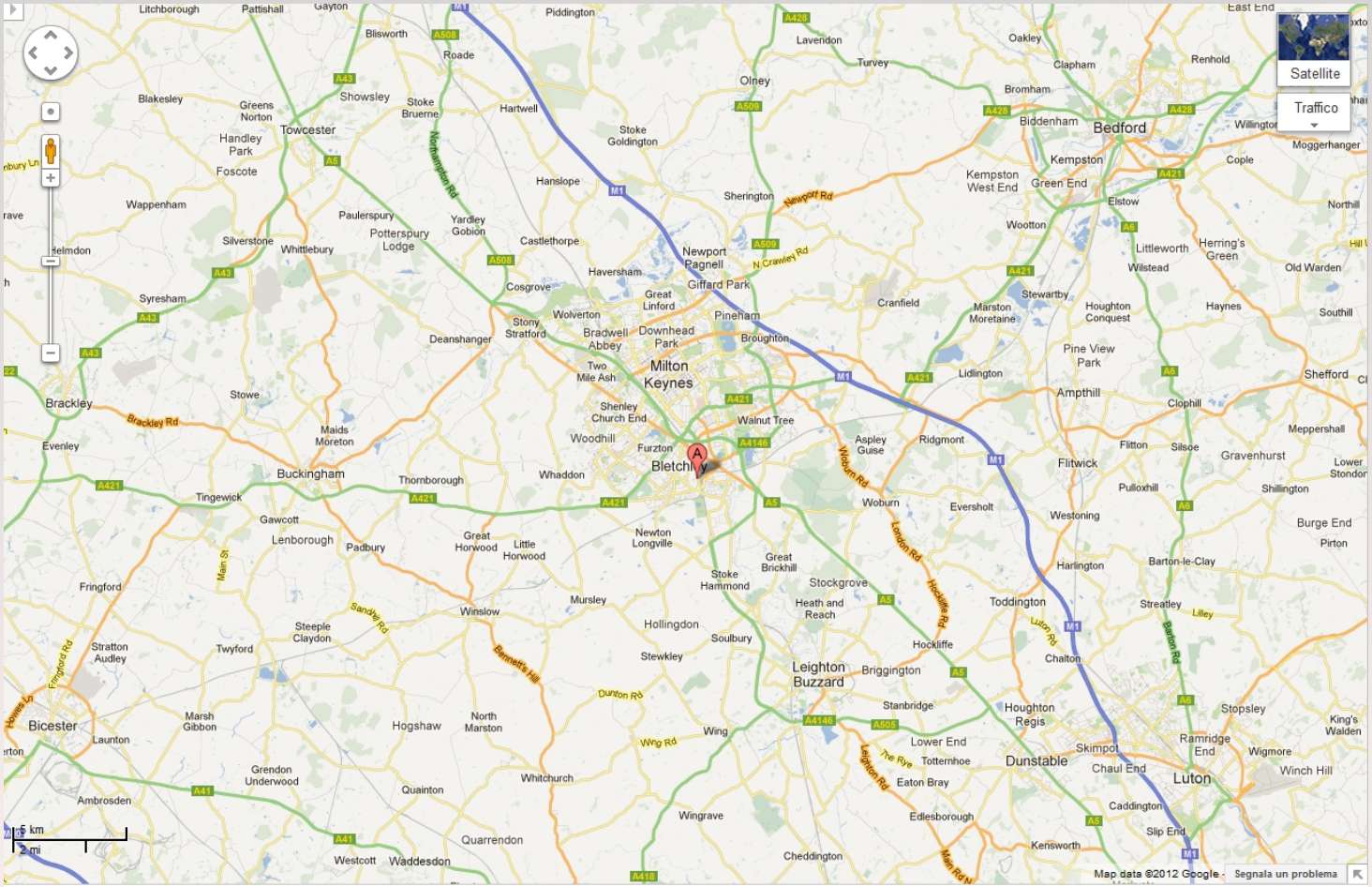
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

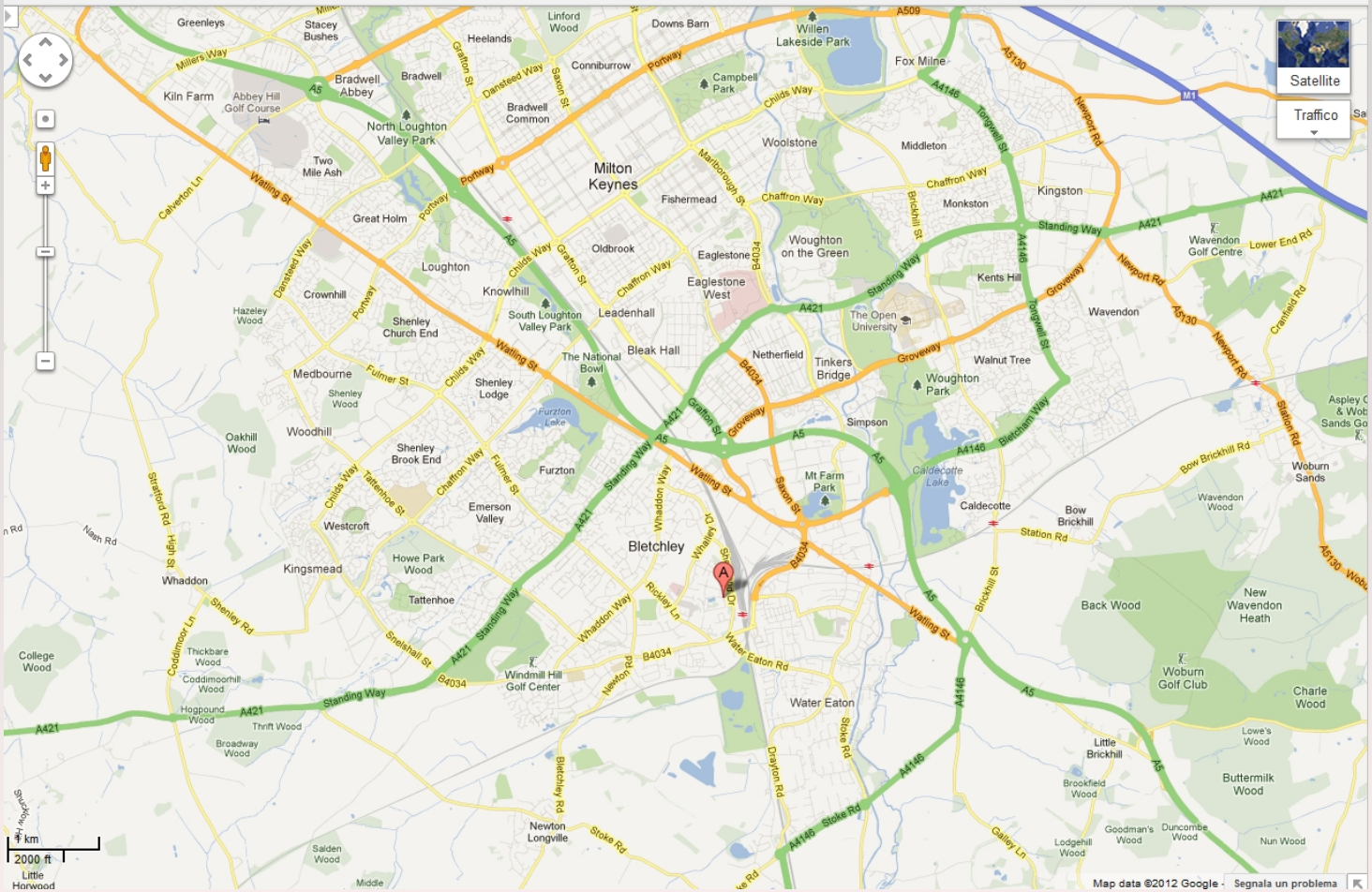
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

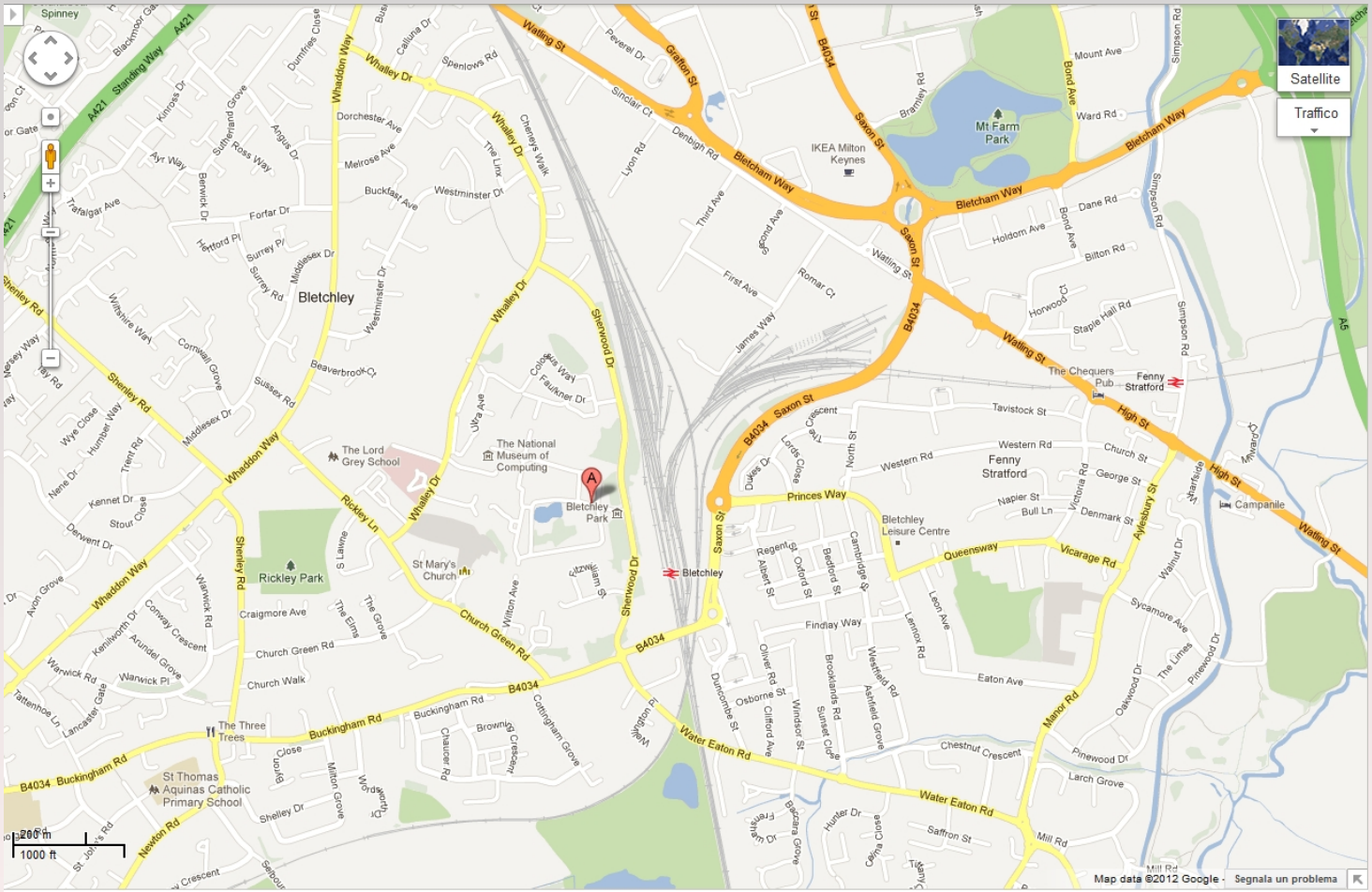
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

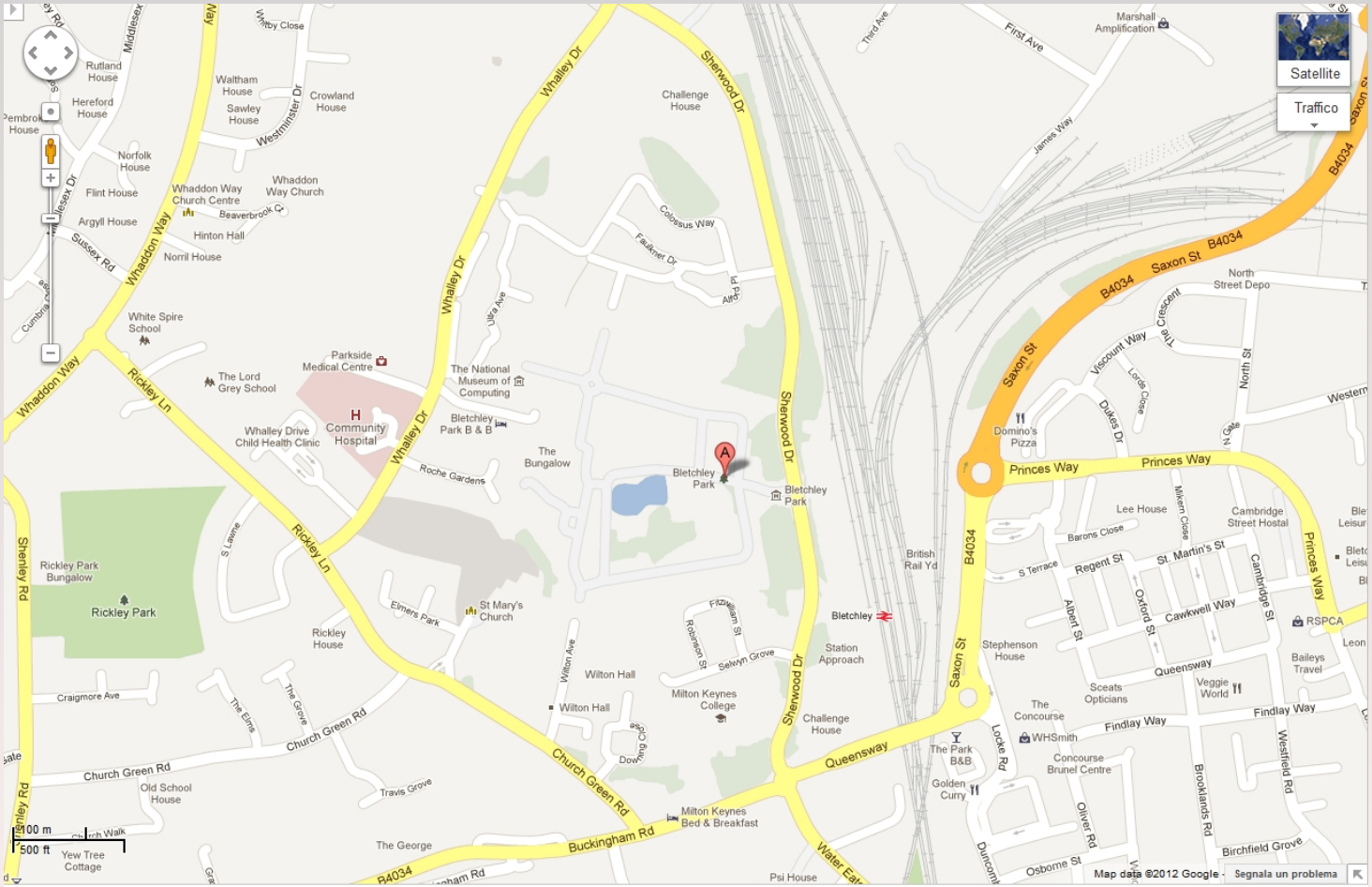
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

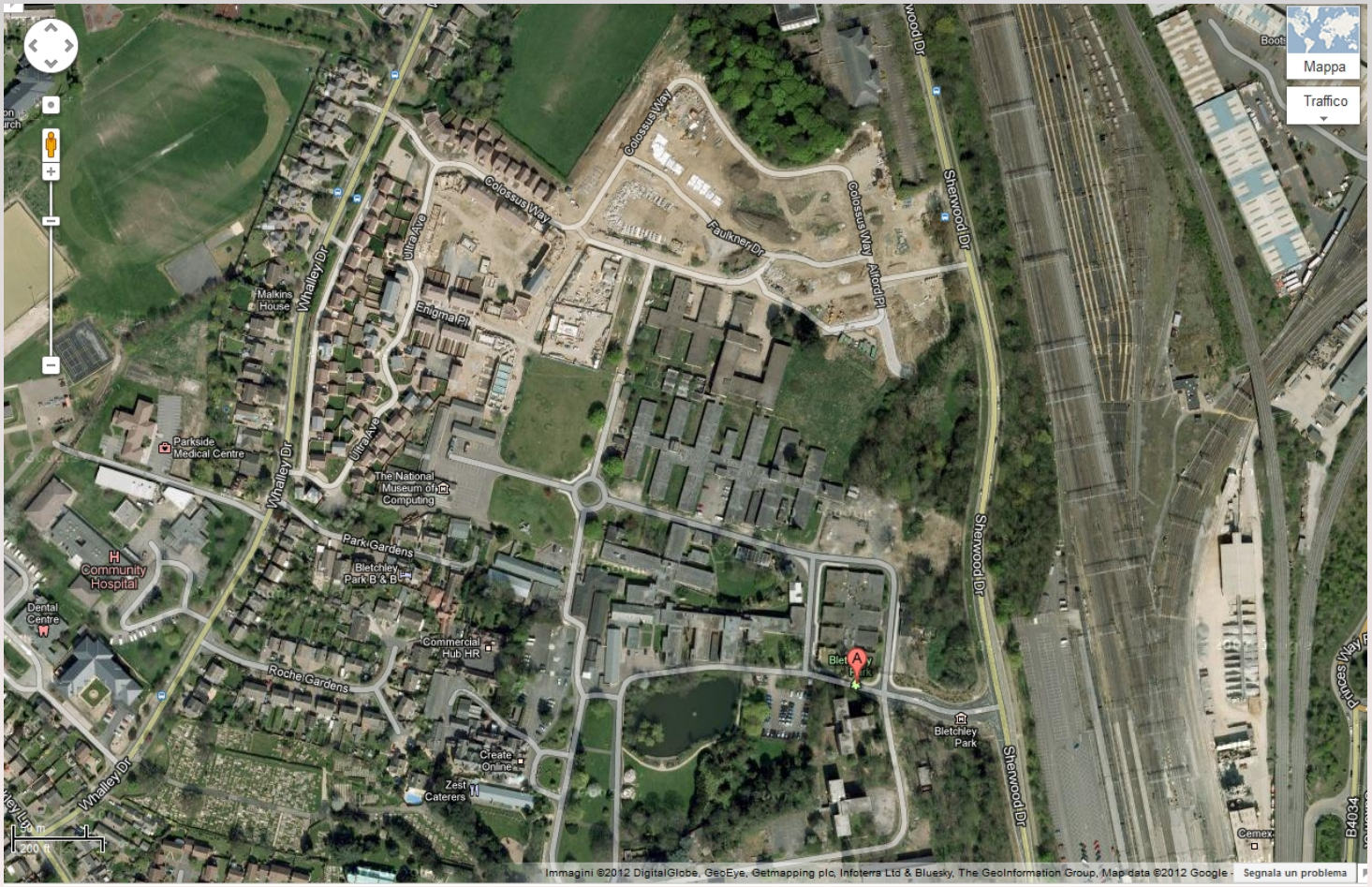
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . a Bletchley Park



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

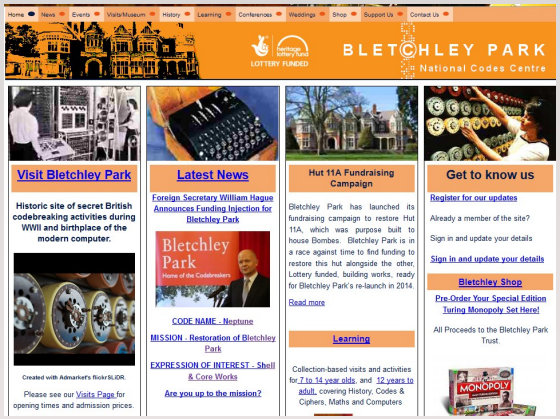
Trasformazioni

Chiave

Decifrazione

Sicurezza

. . . A BLETCHLEY PARK



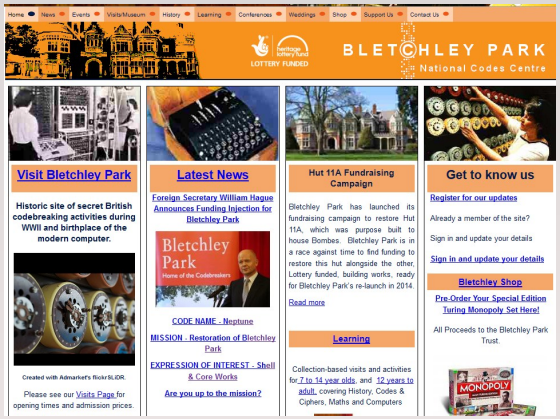
"The Government Code and Cypher School" originariamente di stanza a Londra aveva bisogno di un posto più sicuro dove lavorare e nel 1938 decise di installarsi a Bletchley Park. Nell'agosto 1939 divenne il centro operativo del controspionaggio inglese.

Ora è un museo (con qualche problema di finanziamenti)

Alan Turing ebbe un ruolo cruciale nel team per la decrittazione dell'Enigma, la "macchina da cifra" impiegata dall'esercito e dalla marina tedesca.

AUTOMAZIONE DELLA CRITTOGRAFIA
L'ENIGMA
TURING A BLETCHLEY PARK
FUNZIONAMENTO DELL'ENIGMA
DECRITTAZIONE DELL'ENIGMA
FILMS E LIBRI
NOTE FINALI
TRASPOSIZIONI
DES
INTRODUZIONE
CIFRAZIONE
DECIFRAZIONE
DECRITTAZIONE
AES
INTRODUZIONE
FUNZIONAMENTO
TRASFORMAZIONI
CHIAVE
DECIFRAZIONE
SICUREZZA

. . . A BLETCHLEY PARK



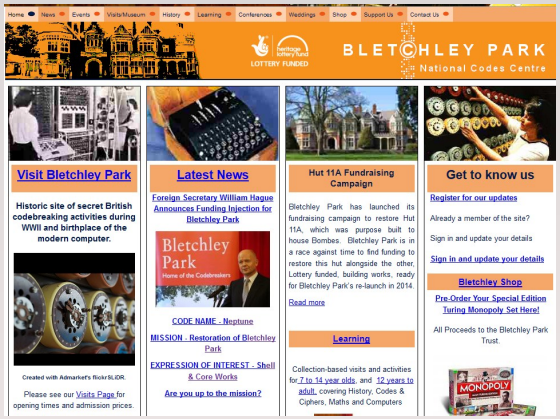
"The Government Code and Cypher School" originariamente di stanza a Londra aveva bisogno di un posto più sicuro dove lavorare e nel 1938 decise di installarsi a Bletchley Park. Nell'agosto 1939 divenne il centro operativo del controspionaggio inglese.

Ora è un museo (con qualche problema di finanziamenti)

Alan Turing ebbe un ruolo cruciale nel team per la decrittazione dell'Enigma, la "macchina da cifra" impiegata dall'esercito e dalla marina tedesca.

AUTOMAZIONE DELLA CRITTOGRAFIA
L'ENIGMA
TURING A BLETCHLEY PARK
FUNZIONAMENTO DELL'ENIGMA
DECRITTAZIONE DELL'ENIGMA
FILMS E LIBRI
NOTE FINALI
TRASPOSIZIONI
DES
INTRODUZIONE
CIFRAZIONE
DECIFRAZIONE
DECRITTAZIONE
AES
INTRODUZIONE
FUNZIONAMENTO
TRASFORMAZIONI
CHIAVE
DECIFRAZIONE
SICUREZZA

. . . A BLETCHLEY PARK



"The Government Code and Cypher School" originariamente di stanza a Londra aveva bisogno di un posto più sicuro dove lavorare e nel 1938 decise di installarsi a Bletchley Park. Nell'agosto 1939 divenne il centro operativo del controspionaggio inglese.

Ora è un museo (con qualche problema di finanziamenti)

Alan Turing ebbe un ruolo cruciale nel team per la decrittazione dell'Enigma, la "macchina da cifra" impiegata dall'esercito e dalla marina tedesca.

AUTOMAZIONE DELLA CRITTOGRAFIA

L'ENIGMA

TURING A BLETCHLEY PARK

FUNZIONAMENTO DELL'ENIGMA

DECRITTAZIONE DELL'ENIGMA

FILMS E LIBRI

NOTE FINALI

TRASPOSIZIONI

DES

INTRODUZIONE

CIFRAZIONE

DECIFRAZIONE

DECRITTAZIONE

AES

INTRODUZIONE

FUNZIONAMENTO

TRASFORMAZIONI

CHIAVE

DECIFRAZIONE

SICUREZZA

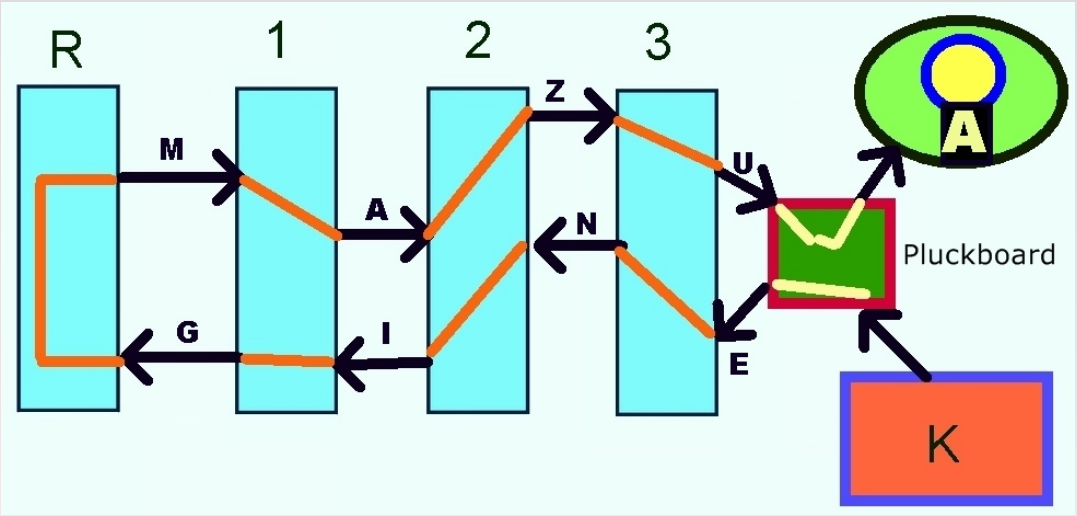
Enigma: funzionamento

- Si tratta di un cifrario polialfabetico.
- Un punto di forza è che la lunghezza del periodo (o della chiave nel senso di Vigenère) è maggiore della lunghezza dei messaggi, il che rende apparentemente simile al one-time-pad.
- Le tecniche statistiche viste per Vigenère non si possono applicare.
- L'altro punto di forza (per l'epoca) era l'automazione elettrica della trasformazione (sia per cifrare che per decifrare) e la relativa semplicità d'uso (anche se mancava la stampante).

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Enigma: funzionamento

Si tratta di una macchina a rotori non fissi che si muovono con moto odometrico dopo ogni lettera codificata—stepping motion (come i vecchi contachilometri o i contatori dell'acqua o del gas).



Ogni rotore ha 26 contatti su una faccia e 26 sull'altra e implementa una sostituzione monoalfabetica (completa).

Il reflector garantisce simmetria. Inoltre (brevetto) mai una lettera era codificata in sè stessa.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

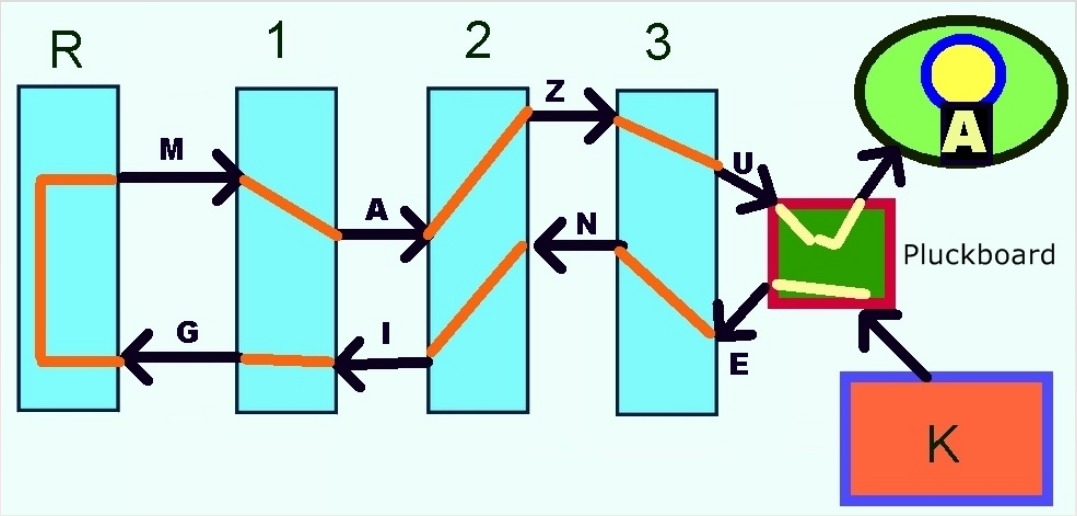
Chiave

Decifrazione

Sicurezza

Enigma: funzionamento

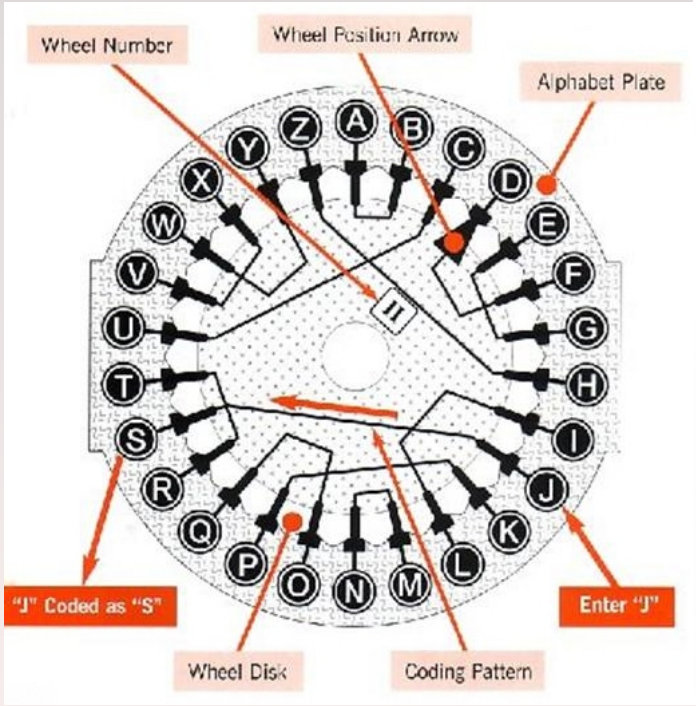
Si tratta di una macchina a rotori non fissi che si muovono con moto odometrico dopo ogni lettera codificata—stepping motion (come i vecchi contachilometri o i contatori dell'acqua o del gas).



Ogni rotore ha 26 contatti su una faccia e 26 sull'altra e implementa una sostituzione monoalfabetica (completa). Il reflector garantisce simmetria. Inoltre (brevetto) mai una lettera era codificata in sè stessa.

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Enigma: funzionamento



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Enigma: funzionamento

Oltre ai 3 (o 4) rotori c'era una pluckboard (pannello elettrico) che permetteva un'ulteriore (e più libera) sostituzione:

Inoltre c'era una sostituzione iniziale tra tastiera e primo rotore (fissa, ma poteva cambiare cambiando il modello della macchina).

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Enigma: funzionamento

- Diverse varianti sono state usate. Concentriamoci su quelle a 3 rotori (per quella a 4, $\times 26$).
- Fissati i rotori, le possibili chiavi iniziali erano $26^3 = 17576$ (456976 per 4 rotori)
- Tale numero è anche la lunghezza del *periodo* (o della chiave nel senso di Vigenère—a dire il vero $26 \cdot 25 \cdot 26$)
- Erano possibili 6 posizioni per i rotori.
- In versioni più evolute veniva fornita una scatola con 5 o, per la marina, 8 rotori da cui sceglierne 3 (o 4). Allora potevano esserci $6 \times \binom{8}{3} = 536$ posizioni.
- Inoltre c'erano i collegamenti sulla plugboard. Con 6 cavi ci sono $\sim 10^{11}$ possibilità.
- In generale, per k cavi ($k = 1, \ldots, 13$) abbiamo:

$$\binom{26}{2k} \frac{\binom{2k}{2}\binom{2k-2}{2}\cdots\binom{2}{2}}{k!}$$

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

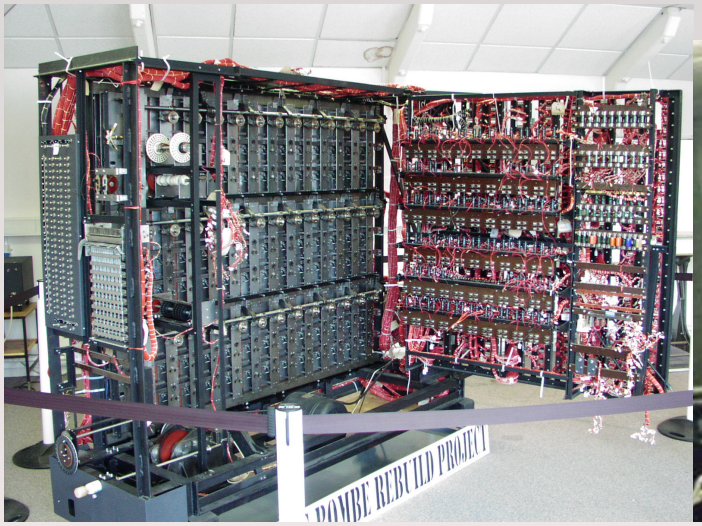
Enigma: attacco

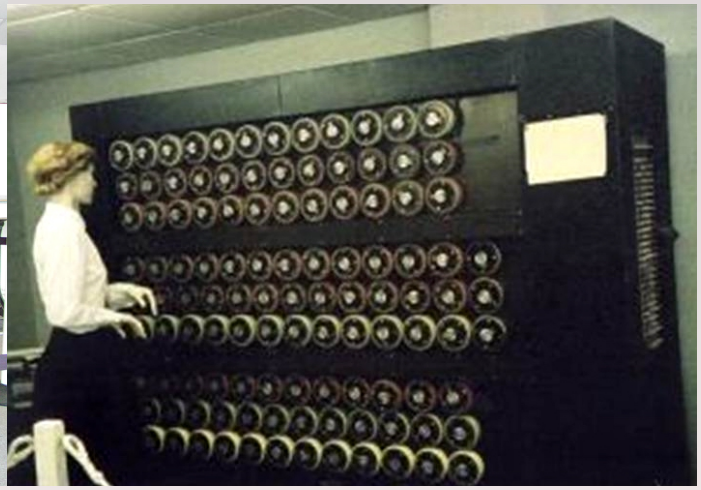
- Le configurazioni iniziali dell'Enigma venivano comunicate segretamente e duravano brevi intervalli di tempo (p.es. plugboard: trimestrale, ordine dei rotori: mensile, carattere di partenza: giornaliero).
- All'inizio del messaggio arrivava codice (in cifra) per modificare ordine rotori.
- L'obiettivo del team di Turing era quello di indovinare rotori/cavi in plugboard/chiave iniziale.
- Furono progettate le bombe che simulavano elettromeccanicamente molti Enigma contemporaneamente.
- La forza bruta, coi numeri visti, non era sufficiente.

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Enigma: attacco

Nel 1940 fu costruita la prima Bombe





Ne furono costruite 210 operate da circa 2000 Wrens (Women's Royal naval Service).

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Enigma: (poche) debolezze

- Prima debolezza: una lettera non veniva mai crittata in sè stessa: se sospettiamo ci sia un certo testo (l'inizio di una lettera, la frase Keine besonderen Ereignisse—niente da segnalare) eseguiamo un allineamento e vediamo dove è possibile che ci sia. Questo ci fornisce delle informazioni verificabili con simulazione. (crib-based decryption).
- Seconda debolezza: il funzionamento generale è, sempre, simmetrico. Fissata chiave etc, se la A va in L, allora la L va in A. Questo è comodo per usare la stessa macchina per codificare e decodificare, non è una buona proprietà crittografica in quanto dà informazioni alla spia.
- Simile per le connessioni sulla plugboard (e.g., A e L vengono collegate e scambiate tra loro nell'encoding).

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Enigma: (poche) debolezze

- Terza debolezza: per correggere eventuali errori di trasmissione, le posizioni iniziali dei rotori (3 caratteri) venivano ripetute due volte.
- Altre particolarità (più che debolezze) costruttive sui rotori.
- Negli anni '30 (prima della guerra) tre giovani matematici polacchi del Cipher Bureau (Marian Rejewski, Henryk Zygalski e Jerzy Różycki) studiarono a fondo le caratteristiche matematico-logiche dell'Enigma.

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Enigma: (poche) debolezze

- Supponiamo di aver intercettato (oggi) 4 messaggi, inizianti con:

$$\begin{array}{ccccccc} A & B & C & D & E & F & \dots \\ Q & W & E & R & T & Y & \dots \\ E & N & I & G & M & A & \dots \\ M & A & L & I & G & N & \dots \end{array}$$

- All'inizio vengono ripetute le posizioni iniziali dei tre rotori, diversi in ogni messaggio, ma tutti del tipo:

$$\alpha\beta\gamma\alpha\beta\gamma$$

- Dal primo messaggio so che un simbolo (che non è nè A nè D) va in A e in D nella prima e quarta posizione, dal secondo so che un simbolo va in Q e R, dal terzo in E e G, dal quarto in M e I)
- Similmente ragionando su II e V posizione e su III e VI.
- Questo permette di avere informazioni su quali configurazioni non provare nemmeno.

Automazione della crittografia

L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali

Trasposizioni

DES
Introduzione
Cifrazione
Decifrazione
Decrittazione

AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Enigma: (poche) debolezze

- Rejewski et al. realizzarono (a mano) un catalogo di 105456 settings iniziali e i corrispondenti parametri quali lunghezza ciclo di permutazioni.
- Alla fine degli anni '30 le comunicarono agli inglesi.
- Turing mise insieme queste informazioni più altre che derivavano dalla cattura di macchine ENIGMA e di libri di utilizzo destinati agli ufficiali tedeschi e se ne servì per ridurre lo spazio di ricerca delle bombe, riuscendo a forzare "shark" (squalo), l'ENIGMA a 4 rotori usato dai sommergibili.

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Enigma: (poche) debolezze

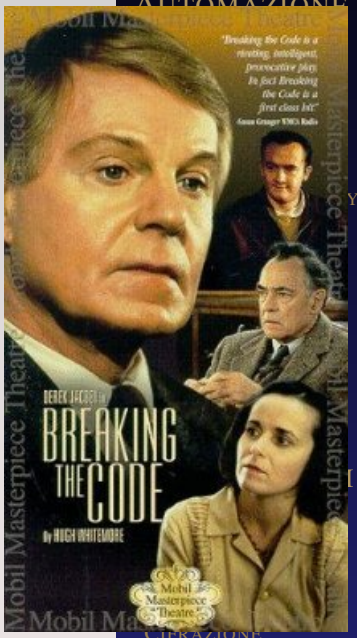
- Rejewski et al. realizzarono (a mano) un catalogo di 105456 settings iniziali e i corrispondenti parametri quali lunghezza ciclo di permutazioni.
- Alla fine degli anni '30 le comunicarono agli inglesi.
- Turing mise insieme queste informazioni più altre che derivavano dalla cattura di macchine ENIGMA e di libri di utilizzo destinati agli ufficiali tedeschi e se ne servì per ridurre lo spazio di ricerca delle bombe, riuscendo a forzare "shark" (squalo), l'ENIGMA a 4 rotori usato dai sommergibili.

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Films 'su' Turing

The Imitation Game
2014
Morten Tyldum

Enigma
2001
M. Adept



Breaking the Code
1996
Derek Jacobi

Un sito che rapporta meglio T.I.G. nella storia reale:
`http://www.historyvshollywood.com/reelfaces/imitation-game/`

Libri dove approfondire

Il ruolo di Turing. **Storico/scientifici:**

- M. Davis. *Il calcolatore universale*
- A. Hodges. *The Enigma* (da cui è tratto “The imitation game”)

Romanzi:

- Robert Harris. *ENIGMA* (1995) (da cui è tratto il film “ENIGMA”)
- Neal Stephenson. *Cryptonomicon* (1999)

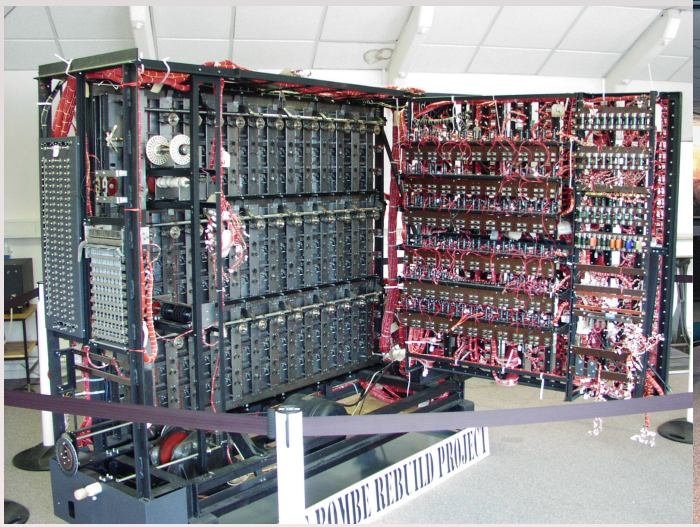
Oltre ovviamente ai contributi scientifici scritti da Turing reperibili da:
`http://www.turingarchive.org/`

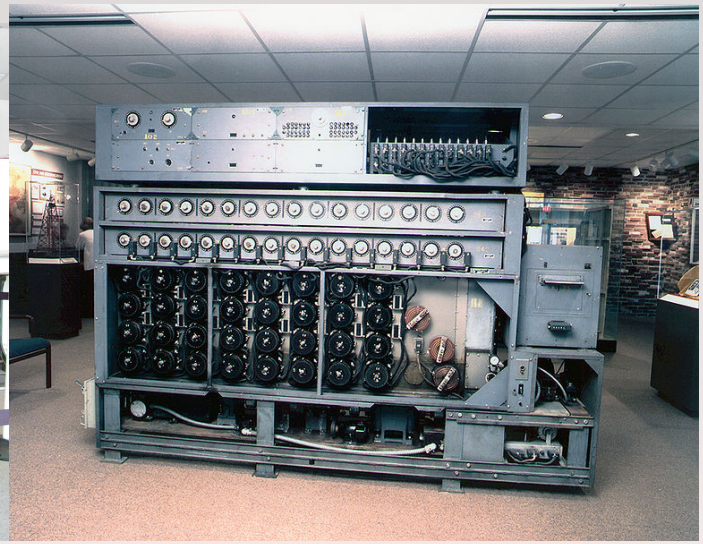
Automazione della crittografia
L’Enigma
Turing a Bletchley Park
Funzionamento dell’Enigma
Decrittazione dell’Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Codici Segreti

Decrittazione informatica: Bombe e Colossi

Nel 1940 fu costruita la prima Bombe





Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

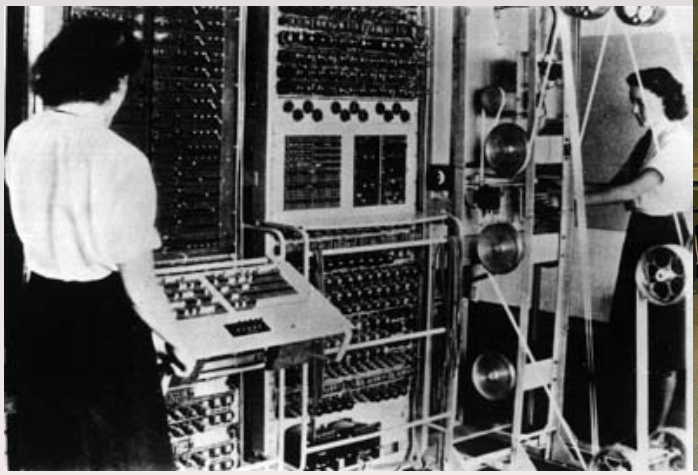
Trasformazioni

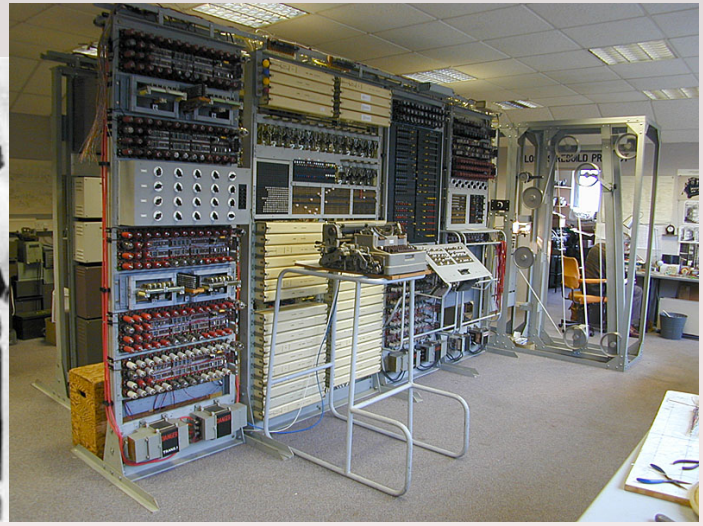
Chiave

Decifrazione

Sicurezza

I tedeschi cambiarono metodologia di codifica con Enigma (e.g., uso di 4 rotori per i sommergibili).

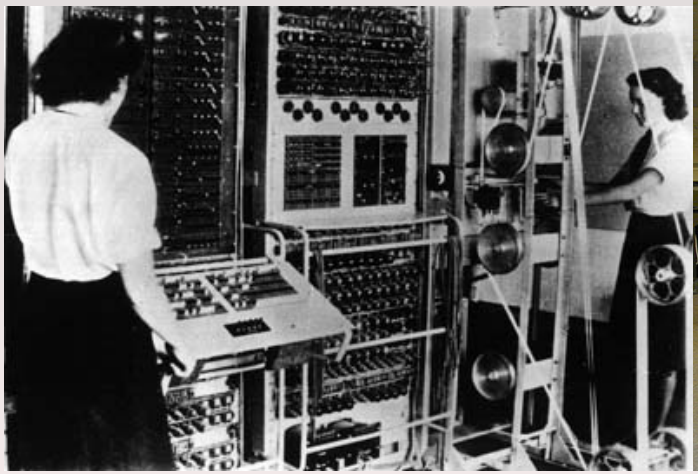


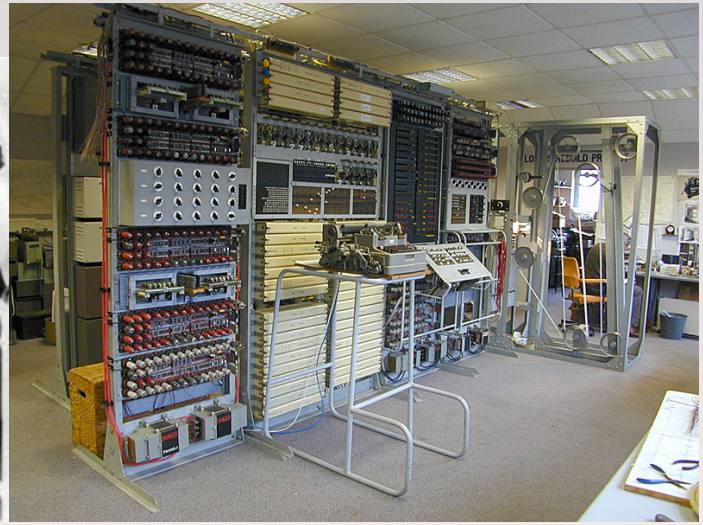


Furono costruiti i colossi.

CODICI SEGRETI
A. DOVIER
AUTOMAZIONE DELLA CRITTOGRAFIA
L'ENIGMA
TURING A BLETCHLEY PARK
FUNZIONAMENTO DELL'ENIGMA
DECRITTAZIONE DELL'ENIGMA
FILMS E LIBRI
NOTE FINALI
TRASPOSIZIONI
DES
INTRODUZIONE
CIFRAZIONE
DECIFRAZIONE
DECRITTAZIONE
AES
INTRODUZIONE
FUNZIONAMENTO
TRASFORMAZIONI
CHIAVE
DECIFRAZIONE
SICUREZZA

I tedeschi cambiarono metodologia di codifica con Enigma (e.g., uso di 4 rotori per i sommergibili).





Furono costruiti i colossi.

CODICI SEGRETI
A. DOVIER
AUTOMAZIONE DELLA CRITTOGRAFIA
L'ENIGMA
TURING A BLETCHLEY PARK
FUNZIONAMENTO DELL'ENIGMA
DECRITTAZIONE DELL'ENIGMA
FILMS E LIBRI
NOTE FINALI
TRASPOSIZIONI
DES
INTRODUZIONE
CIFRAZIONE
DECIFRAZIONE
DECRITTAZIONE
AES
INTRODUZIONE
FUNZIONAMENTO
TRASFORMAZIONI
CHIAVE
DECIFRAZIONE
SICUREZZA

- Il tutto però fu sempre più difficile computazionalmente con l'aumento dei rotori e le modifiche sui cavi sulla plugboard.
- Turing cercò di impadronirsi di queste importanti competenze, le esportò agli USA, dove avevano costruito delle Bombe più veloci ma che sfruttavano le simmetrie scoperte dai polacchi.
- Alla fine si riuscì ad avere uno speed-up nei tempi grazie alla progettazione dei colossi.

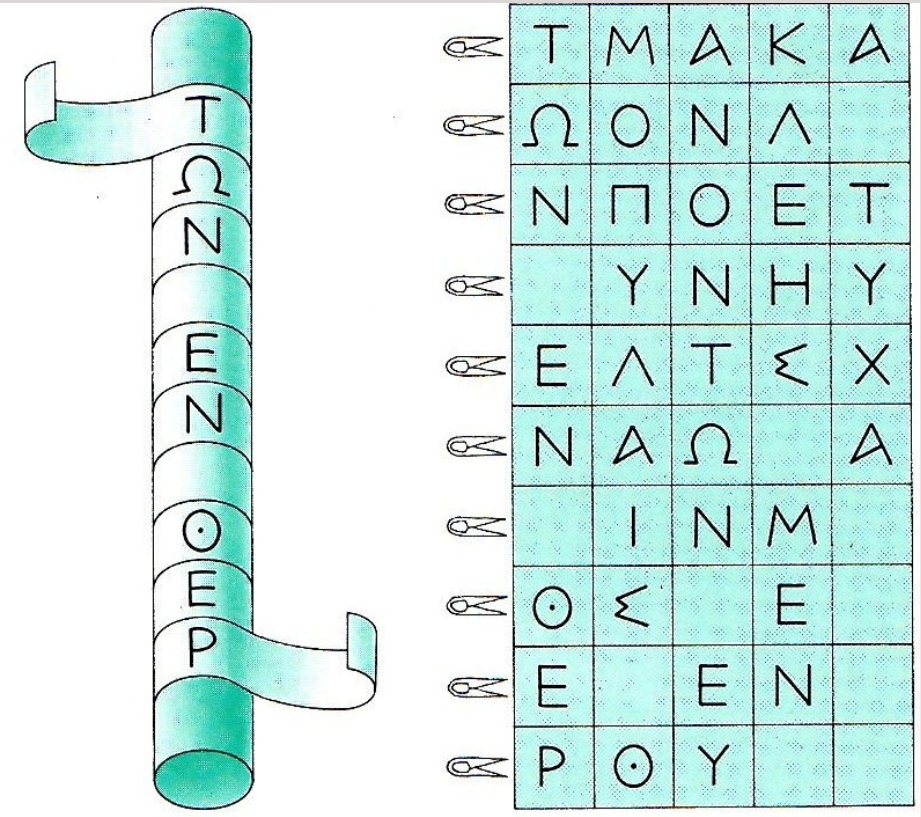
AUTOMAZIONE DELLA CRITTOGRAFIA
L'ENIGMA
TURING A BLETCHLEY PARK
FUNZIONAMENTO DELL'ENIGMA
DECRITTAZIONE DELL'ENIGMA
FILMS E LIBRI
NOTE FINALI
TRASPOSIZIONI
DES
INTRODUZIONE
CIFRAZIONE
DECIFRAZIONE
DECRITTAZIONE
AES
INTRODUZIONE
FUNZIONAMENTO
TRASFORMAZIONI
CHIAVE
DECIFRAZIONE
SICUREZZA

- Giusto per avere dei numeri (anche se ovviamente non tutto è stato reso noto e per le stesse ragioni anche i colossi, i primi computer elettronici, non ebbero l'influsso meritato nella storia del calcolatore).
- A Bletchey Park e nelle sedi dipendenti variamente dislocate per limitare gli eventuali effetti di un attacco aereo sono state dislocate 210 bombe operate da circa 2000 Wrens (Women's Royal naval Service).
- Furono costruiti anche dieci colossi.

AUTOMAZIONE DELLA CRITTOGRAFIA
L'ENIGMA
TURING A BLETCHLEY PARK
FUNZIONAMENTO DELL'ENIGMA
DECRITTAZIONE DELL'ENIGMA
FILMS E LIBRI
NOTE FINALI
TRASPOSIZIONI
DES
INTRODUZIONE
CIFRAZIONE
DECIFRAZIONE
DECRITTAZIONE
AES
INTRODUZIONE
FUNZIONAMENTO
TRASFORMAZIONI
CHIAVE
DECIFRAZIONE
SICUREZZA

Cifrari a trasposizione

Scitala spartana (≈ 400 AC)



Cifrari a trasposizione

Jules Verne (1828–1905): la griglia di Mattia Sandorf

ihnalz	zaemen	ruiopn
arnuro	trvree	mtqssl
odxhnp	estlev	eeuart
aeeeil	ennios	noupvg
spesdr	erssur	ouitse
eedgnc	toeedt	artuee

hazrxeirg nohaledec nadnepedn ilruopess
ssepourlindependancedelahongriexrzah
[ma]sse pour l'independance de la Hongrie. Xrzah

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Cifrari a trasposizione

Jules Verne (1828–1905): la griglia di Mattia Sandorf

i	h	n	a	l	z
a	r	n	u	r	o
o	d	x	h	n	p
a	e	e	e	i	l
s	p	e	s	d	r
e	e	d	g	n	c

hazrxeirg nohaledec nadnepedn ilruopess
ssepourlindependancedelahongriexrzah
[ma]sse pour l'independance de la Hongrie. Xrzah

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

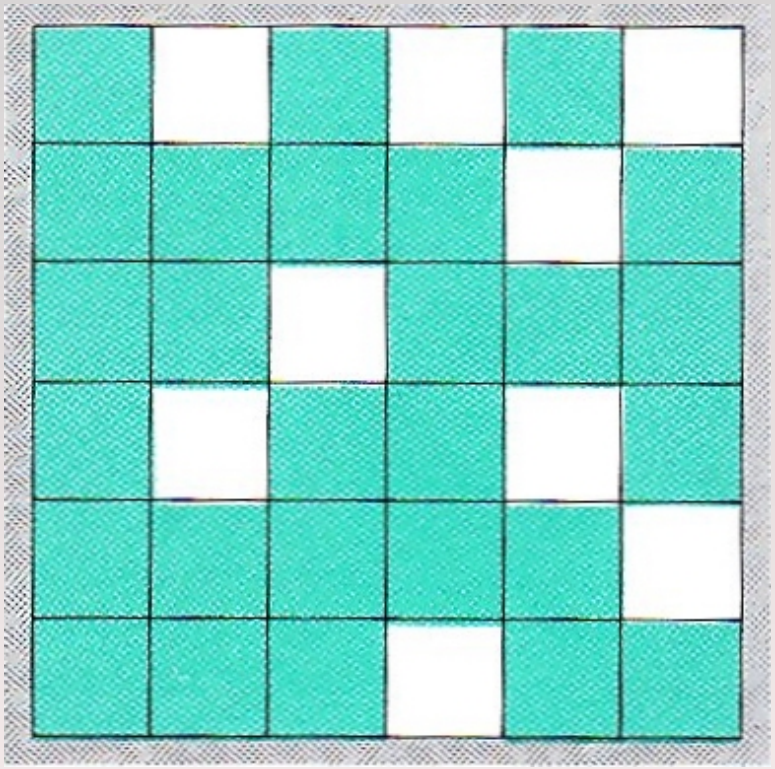
Chiave

Decifrazione

Sicurezza

Cifrari a trasposizione

Jules Verne (1828–1905): la griglia di Mattia Sandorf



hazrxeirg nohaledec nadnepedn ilruopess
ssepourlindependancedelahongriexrzah
[ma]sse pour l'independance de la Hongrie. Xrzah

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

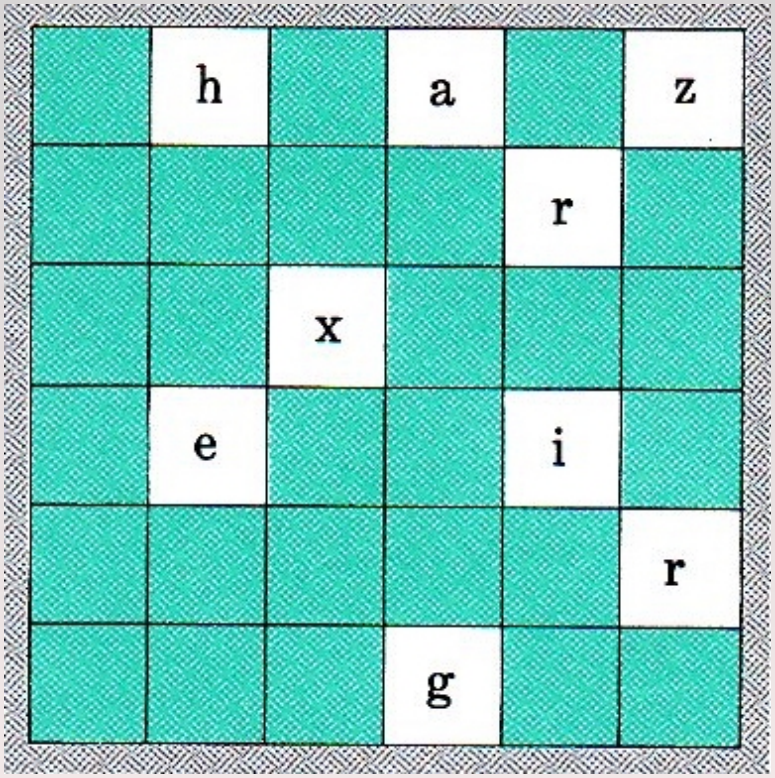
Chiave

Decifrazione

Sicurezza

Cifrari a trasposizione

Jules Verne (1828–1905): la griglia di Mattia Sandorf



hazrxeirg nohaledec nadnepedn ilruopess ssepourlindependancedelahongriexrzah [ma]sse pour l'independance de la Hongrie. Xrzah

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

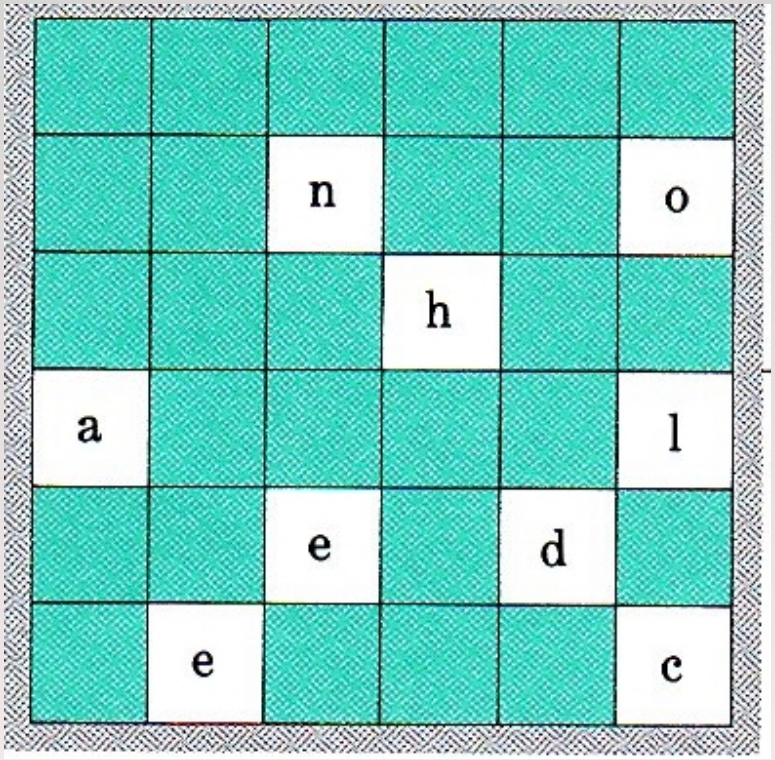
Chiave

Decifrazione

Sicurezza

Cifrari a trasposizione

Jules Verne (1828–1905): la griglia di Mattia Sandorf



hazrxeirg nohaledec nadnepedn ilruopess ssepourlindependancedelahongriexrzah [ma]sse pour l'independance de la Hongrie. Xrzah

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

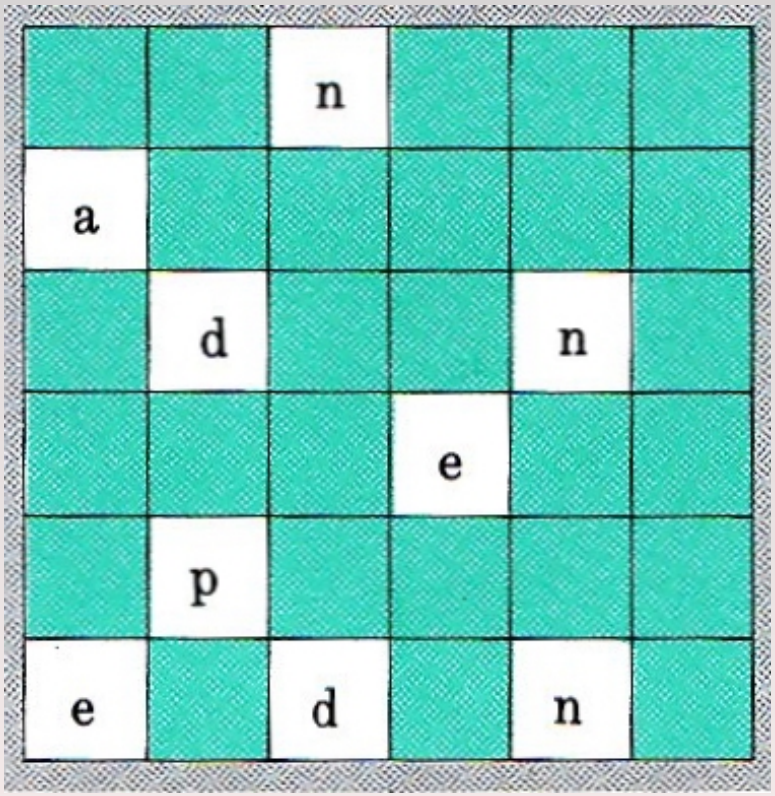
Chiave

Decifrazione

Sicurezza

Cifrari a trasposizione

Jules Verne (1828–1905): la griglia di Mattia Sandorf



hazrxeirg nohaledec nadnepedn ilruopess
ssepourlindependancedelahongriexrzah
[ma]sse pour l'independance de la Hongrie. Xrzah

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

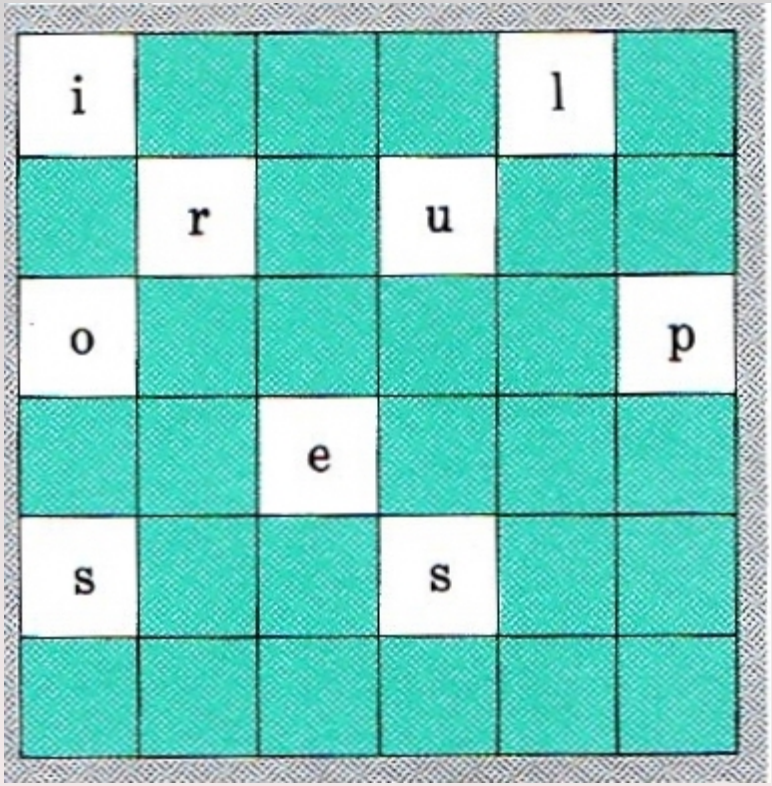
Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Cifrari a trasposizione

Jules Verne (1828–1905): la griglia di Mattia Sandorf



hazrxeirg nohaledec nadnepedn ilruopess

ssepourlindependancedelahongriexrzah

[ma]sse pour l'independance de la Hongrie. Xrzah

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

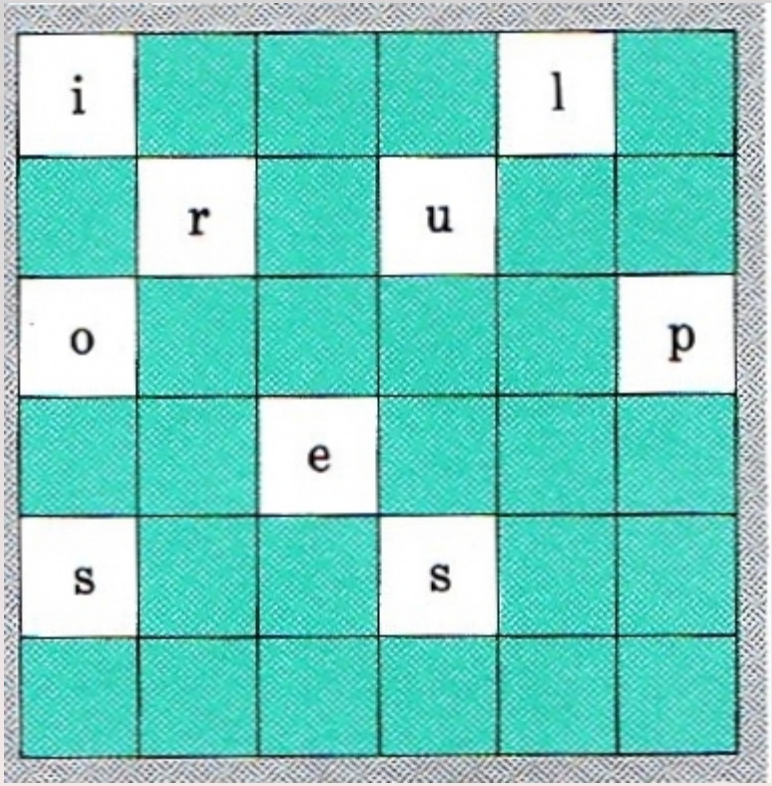
Chiave

Decifrazione

Sicurezza

Cifrari a trasposizione

Jules Verne (1828–1905): la griglia di Mattia Sandorf

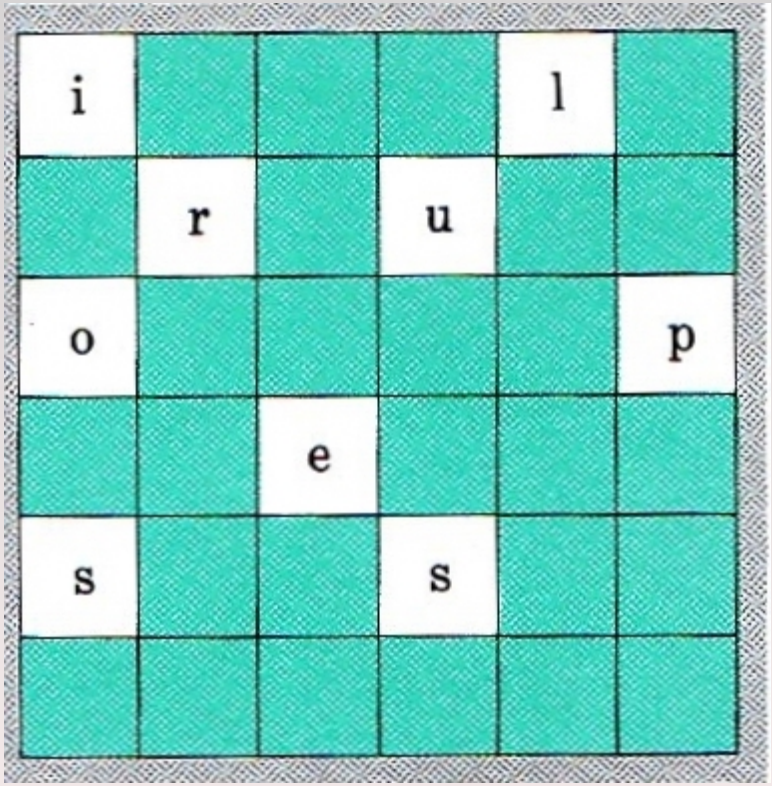


hazrxeirg nohaledec nadnepedn ilruopess
ssepourlindependancedelahongriexrzah
[ma]sse pour l'independance de la Hongrie. Xrzah

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Cifrari a trasposizione

Jules Verne (1828–1905): la griglia di Mattia Sandorf



hazrxeirg nohaledec nadnepedn ilruopess
ssepourlindependancedelahongriexrzah
[ma]sse pour l'independance de la Hongrie. Xrzah

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Data Encryption Standard

Breve storia

- 1973 L'NBS (National Bureau of Standards) ora NIST (National Institute of Standards and Technology) richiede un algoritmo standard di cifratura
- 1975 IBM (Horst Feistel et al) pubblica il DES nel Federal Register
- 1976/77 Il DES è approvato/pubblicato come standard
- Il funzionamento del DES è pubblico (soddisfa il principio di Kerckhoffs). Non sono necessariamente rese note le *ragioni* di alcune scelte.
- 1990 Biham e Shamir usando la crittanalisi differenziale, forzano un DES-like a 15 fasi. Ma il DES ne ha 16.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Data Encryption Standard

Breve storia

- Nel 1997 e 1998 il DES viene violato pubblicamente in risposta ad una competizione organizzata dalla RSA.
- 1998 Il DES cracker viola una chiave DES in 56 ore.
- 1999 DES cracker e distributed.net assieme violano una chiave DES in 22 ore e 15 minuti.
- 1999 Il DES raccomanda di usare la versione Triple DES (chiave di 168 bit)
- 2001 AES (Rijndael) viene pubblicato come standard per sostituire il DES.

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Data Encryption Standard

Chiave

- Del DES tutto è noto tranne la chiave.
- La chiave del DES è costituita da 8 bytes.
- L'ultimo bit di ogni byte è un bit di disparità.
- Dunque la vera lunghezza della chiave è 56 bits (spazio di $2^{56} \approx 7.2 \times 10^{16}$).
- La codifica di un messaggio avviene dividendolo in blocchi di 64 bits e processandone uno alla volta.

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Data Encryption Standard

Chiave

- Del DES tutto è noto tranne la chiave.
- La chiave del DES è costituita da 8 bytes.
- L'ultimo bit di ogni byte è un bit di disparità.
- Dunque la vera lunghezza della chiave è 56 bits (spazio di $2^{56} \approx 7.2 \times 10^{16}$).
- La codifica di un messaggio avviene dividendolo in blocchi di 64 bits e processandone uno alla volta.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Data Encryption Standard

Fase 0: trasposizione iniziale

Il blocco $I = x_1 x_2 \ldots x_{64}$ in ingresso viene trasposto mediante la trasposizione iniziale TI e diventa

$$T_0 = \mathrm{TI}(I)$$

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Precisamente $T_0 = x_{58} x_{50} x_{42} \ldots x_{15} x_7$.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

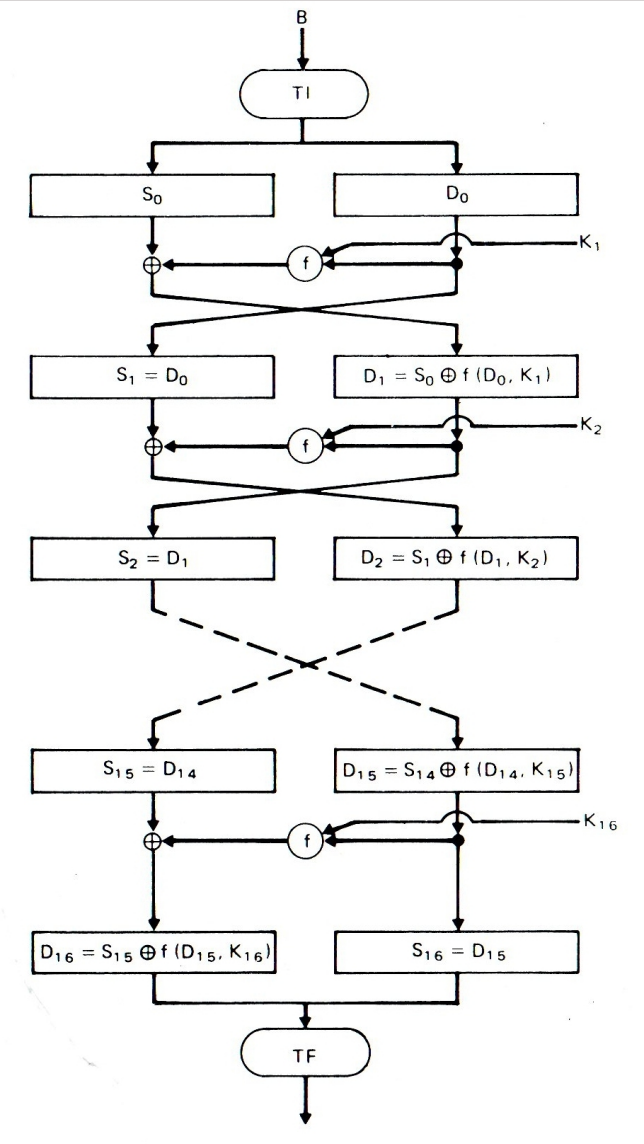
Chiave

Decifrazione

Sicurezza

Data Encryption Standard

Fase 1–16: Algoritmo principale



- $T_0 = \mathrm{TI}(I)$
- Per $i > 0$, sia T_i il risultato (64 bit) della i-esima iterazione.
- Per $i \geq 0$, siano S_i e D_i t.c. $T_i = S_i D_i$, $|S_i| = |D_i| = 32$.
- Per $i = 1, \ldots, 16$, sia:

$$\begin{cases} S_i &= D_{i-1} \\ D_i &= S_{i-1} \oplus f(D_{i-1}, K_i) \end{cases}$$

- Ricordiamoci di $T_{16} = S_{16} D_{16}$
- Descriviamo ora f e K_i

Data Encryption Standard

La funzione f

Dobbiamo calcolare $f(D_{i-1}, K_i)$.
Prima D_{i-1} (32 bit) viene espanso in un blocco di 48 bit $E(D_{i-1})$ usando la tabella

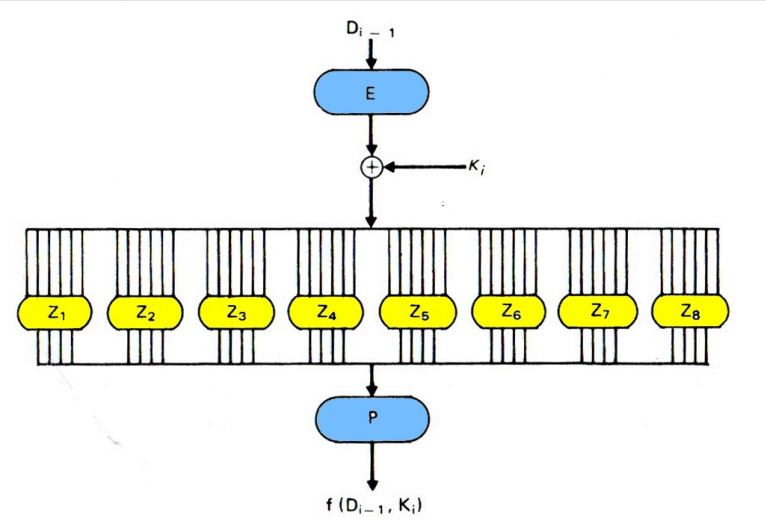
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Se $D_{i-1} = d_1 d_2 \cdots d_{32}$ allora $E(D_{i-1}) = d_{32} d_1 d_2 \cdots d_{32} d_1$.

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Data Encryption Standard

La funzione f



- Si calcola la chiave K_i (48 bits).
- Si calcola $E(D_{i-1}) \oplus K_i$ e lo si legge come 8 blocchetti di 6 bits $\beta_1 \cdots \beta_8$.
- Ogni blocchetto di 6 bits viene trasformato in un blocchetto da 4 bits mediante la sostituzione Z_j con $j = 1, \ldots, 8$.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Data Encryption Standard

La funzione f

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	Z_1
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	Z_2
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	Z_3
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	Z_4
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	Z_5
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	Z_6
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	Z_7
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	Z_8
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

- Consideriamo i bits $b_1 \ldots b_6$ del blocco j.
- I bits $b_1 b_2$ individuano la riga, i bits $b_2 b_3 b_4 b_5$ la colonna.
- L'intero trovato viene codificato in binario con 4 bits.

Data Encryption Standard

La funzione f

La concatenazione degli 8×4 bits (sia $b_1 \ldots b_{32}$) viene dunque trasposta usando la seguente tabella:

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

ottenendo dunque $b_{16} b_7 \cdots b_4 b_{25}$.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

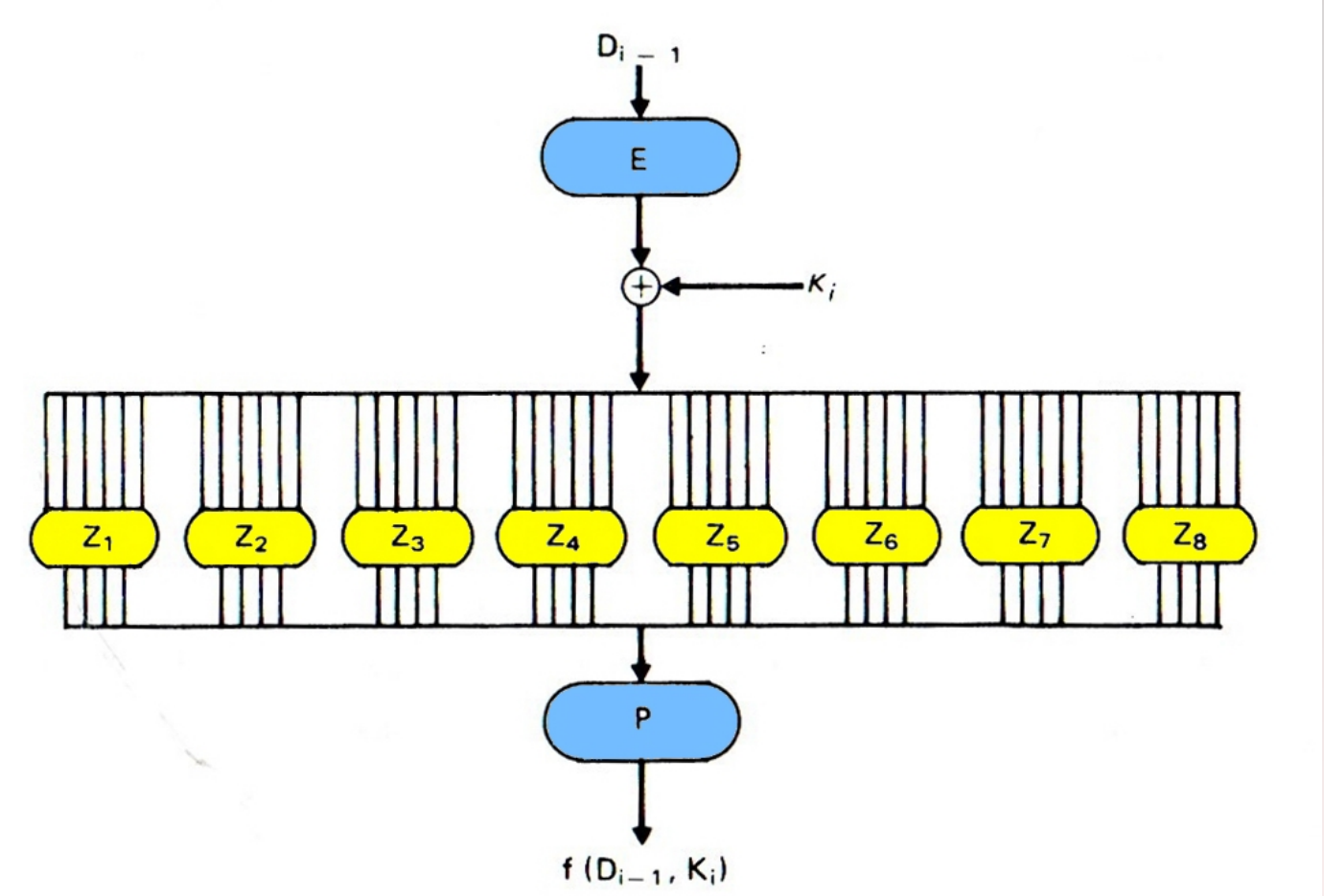
Chiave

Decifrazione

Sicurezza

Data Encryption Standard

La funzione *f* (riassunto)



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Data Encryption Standard

Calcolo delle chiavi parziali

La chiave K ha 64 bits (inclusi quelli di disparità) $k_1 \ldots k_{64}$.
Usiamo la seguente tabella TK per trasporla:

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Otteniamo 56 bits $k_{57}k_{49} \cdots k_{12}k_4$.
Li spezziamo nei semiblocchi s_0 e d_0 da 28 bits.

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Data Encryption Standard

Calcolo delle chiavi parziali

I blocchi s_0 e d_0 vengono shiftati ciclicamente a sinistra di uno o due posizioni usando la tabella a destra.
Si ottengono:

$$\langle s_1, d_1 \rangle$$
$$\langle s_2, d_2 \rangle$$
$$\vdots$$
$$\langle s_{16}, d_{16} \rangle$$

TABELLA 4.8 *Le rotazioni a sinistra RS*

Iterazione	Ampiezza della rotazione a sinistra
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Data Encryption Standard

Calcolo delle chiavi parziali

Le varie coppie $\langle s_i, d_i \rangle$ ottenute, sono filtrate e trasposte usando la matrice CK a fianco.
Di 56 bits ne rimangono solo 48.

TABELLA 4.7 *La compressione CK*

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

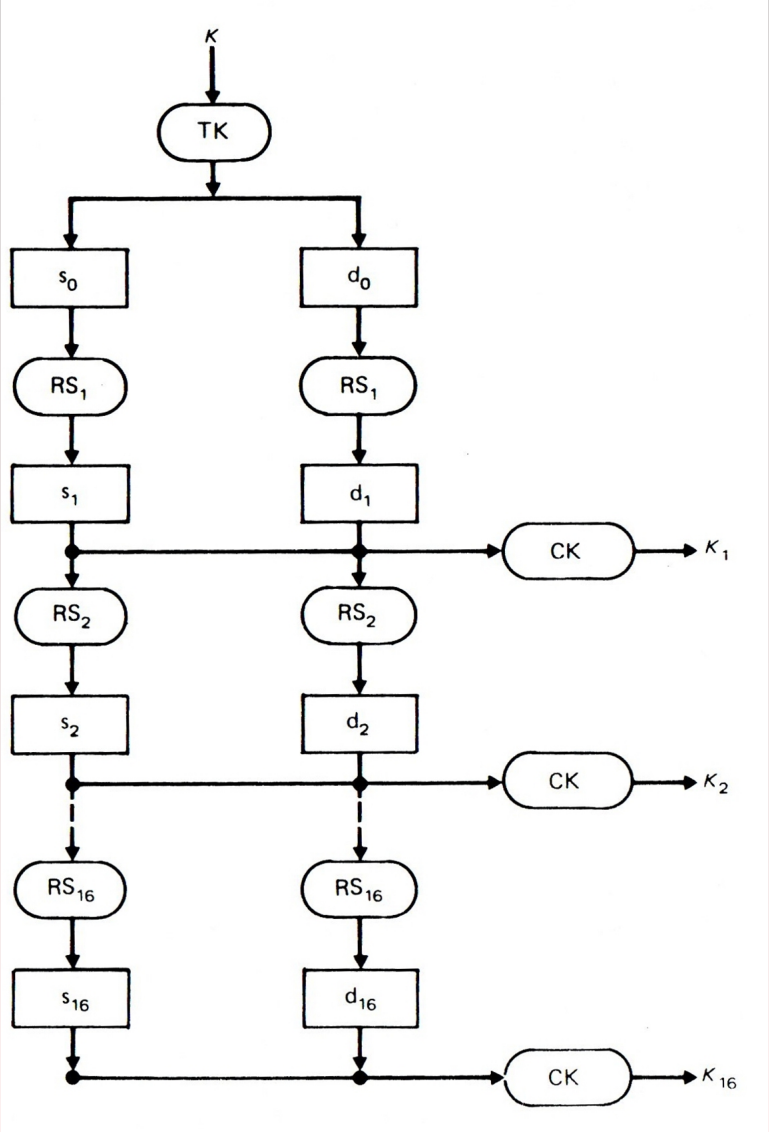
Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Data Encryption Standard

Calcolo delle chiavi parziali: schema



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Data Encryption Standard

Calcolo delle chiavi parziali: schema

Alla fine T_{16} viene data in pasto alla trasposizione finale TF:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Che è inversa della trasposizione iniziale TI

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Data Encryption Standard

Decifrazione

- L'algoritmo è lo stesso.
- Unica differenza: le chiavi parziali si usano in ordine invertito (prima $\langle s_{16}, d_{16} \rangle$, ultima $\langle s_1, d_1 \rangle$).

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Data Encryption Standard

Decrittazione: crittanalisi differenziale

- Idea di Biham–Shamir 1990.
- Si basa sull'assunzione di aver accesso alla "macchina" con chiave fissata (ma ignota).
- Si generano molti messaggi in chiaro ottenendo i corrispondenti crittogrammi.
- Si lavora sulla differenza tra messaggi in ingresso e messaggi in uscita.
- Nel libro Wade–Trappe vedete come funziona con un DES-like (Feistel system) con tre o quattro iterazioni.
- In realtà si mostra che il metodo ha dei buoni risultati fino a 15 iterazioni.
- Ma il DES ne ha 16. Dunque i progettisti del DES sapevano quel che facevano.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Data Encryption Standard

Decrittazione: forza bruta (e HW dedicato)

- Lo spazio di 2^{56} sembrò "piccolo" fin dal principio.
- Già nel 1975 Diffie e Hellman stimarono che con circa 20 milioni di dollari si potesse costruire un calcolatore in grado di forzarlo in circa un giorno.
- Nel 1977 fu approvato come "standard".
- Ogni 5 anni nasceva discussione circa il rinnovo di tale licenza
- Nel 1987, in barba a Kerckoffs, l'NSA propose un nuovo sistema (SW) di cui solo loro sapevano l'architettura (e garantivano forte protezione verso reverse engineering). Non andò in porto.
- Gli attacchi differenziali si dimostrarono inefficaci (e basati su un'ipotesi comunque molto forte).
- Il DES fu ricertificato anche nel 1992.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Data Encryption Standard

Decrittazione: forza bruta (e HW dedicato)

- Nel 1996 maturarono due (*) linee di attacco al DES:
  - Parallelismo massivo ditribuito (forza bruta a basso costo)
  - Architettura ad hoc (Michael Wiener, Bell, 1993)
- Nel 1997 i “rivali” della RSA (di cui parleremo a lungo) misero in palio 10000 $ per chi sarebbe stato in grado di trovare la chiave di un messaggio creato e cifrato da loro.
- Rocke Verser preparò un programma in grado di distribuire il lavoro su PC vari collegati in Internet. La partecipazione era invogliata economicamente (si sarebbe ricevuto il 40% della vincita nel caso il proprio PC fosse quello che trovava la chiave).

Automazione della crittografia
L’Enigma
Turing a Bletchley Park
Funzionamento dell’Enigma
Decrittazione dell’Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Data Encryption Standard

Decrittazione: forza bruta (e HW dedicato)

- Il messaggio era: Strong cryptography makes the world a safer place.
- Furono necessari 5 mesi (ovviamente con carico piuttosto irregolare). Fu esplorato circa il 25% dello spazio.
- L'anno successivo (1998) l'RSA ripetè il concorso, con il messaggio Many hands make light work.
- In questo caso la chiave fu trovata dopo 39 giorni, visitando l'85% dello spazio di ricerca.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Data Encryption Standard

Decrittazione: forza bruta (e HW dedicato)

- Nel 1998 la EFF (Electronic Frontier Foundation) mise a disposizione un budget di 200.000$ ad un team per lo sviluppo del DES cracker.
- Ad un PC tradizionale furono associati circa 1500 chips dedicati (a 40MHz) che emulavano il DES.
- Ogni chip aveva 24 unità di ricerca ed era delegato ad una porzione delle chiavi possibili.
- Un testo di 16 Bytes era diviso in due blocchi da 8 Bytes da analizzarsi in cascata.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Data Encryption Standard

Doppio e Triplo DES

- La chiave era promettente se sui primi 8 Bytes generava un testo in cui i simboli erano numero, lettera, o simbolo di punteggiatura.
- Se la chiave era promettente, si ripeteva sulla seconda metà.
- Numeri: $\frac{69}{256} \simeq \frac{1}{4}$ sono gli ASCII buoni. Dunque la chance che sia promettente è $\sim \left(\frac{1}{4}\right)^8 = 2^{-16}$. Combinando con la seconda metà si arriva a 2^{-32}. Rimangono per la CPU principale $2^{(56-32)} = 2^{24} \approx 16$ milioni di tentativi.
- A 100 tentativi al secondo sono 40 ore nel caso peggiore.

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Data Encryption Standard

Doppio e Triplo DES

- Urge allora abbandonare il DES. Fu suggerito di usare il doppio DES o il triplo DES.
- Il doppio DES usa due codifiche consecutive $c = DES_{k_1}(DES_{k_2}(m))$
- La chiave ora è lunga 112 bits. Inoltre la combinazione di due codifiche non dà una singola codifica diversa (cosa che succede con altri codici).
- Tuttavia, avendo una copia m, c, la decrittazione è poco più complicata del singolo DES ($\sim 2^{57}$) (meet-in-the-middle attack).
- Il triplo DES si può ottenere in diversi modi, anche usando una chiave come *inversa*. Anche con il meet-in-the-middle attack lo spazio rimane (per oggi) considerevole ($\sim 2^{113}$).

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Advanced Encryption Standard

Introduzione

- AES fu annunciato dalla NIST come standard nel 2002, dopo diversi di discussioni e una competizione, vinta dall'algoritmo Rijndael
- Gli autori di Rijndael sono i belgi Joan Daemen and Vincent Rijmen.

Advanced Encryption Standard

Introduzione

- Come per il DES, il funzionamento è totalmente pubblico.
- AES è in tre versioni differenziate dalla lunghezza della chiave: AES-128, AES-192 e AES-256.
- La cifrazione avviene comunque sempre con blocchi di 128 bits.
- Usa una “substitution permutation network” invece di una “Feistel network”.
- Può essere esteso con blocchi fino a 256 bits, ma con chiavi di lunghezza illimitata.
- C’è largo uso dell’algebra in $GF(2^8)$.
- Spiegazione originale in: `http://csrc.nist.gov/archive/aes/rijndael/misc/nissc2.pdf`

Automazione della crittografia

L’Enigma
- Turing a Bletchley Park
- Funzionamento dell’Enigma
- Decrittazione dell’Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Advanced Encryption Standard

Introduzione

- Come per il DES, il funzionamento è totalmente pubblico.
- AES è in tre versioni differenziate dalla lunghezza della chiave: AES-128, AES-192 e AES-256.
- La cifrazione avviene comunque sempre con blocchi di 128 bits.
- Usa una “substitution permutation network” invece di una “Feistel network”.
- Può essere esteso con blocchi fino a 256 bits, ma con chiavi di lunghezza illimitata.
- C’è largo uso dell’algebra in $GF(2^8)$.
- Spiegazione originale in: `http://csrc.nist.gov/archive/aes/rijndael/misc/nissc2.pdf`

Automazione della crittografia

L’Enigma
- Turing a Bletchley Park
- Funzionamento dell’Enigma
- Decrittazione dell’Enigma
- Films e Libri
- Note finali

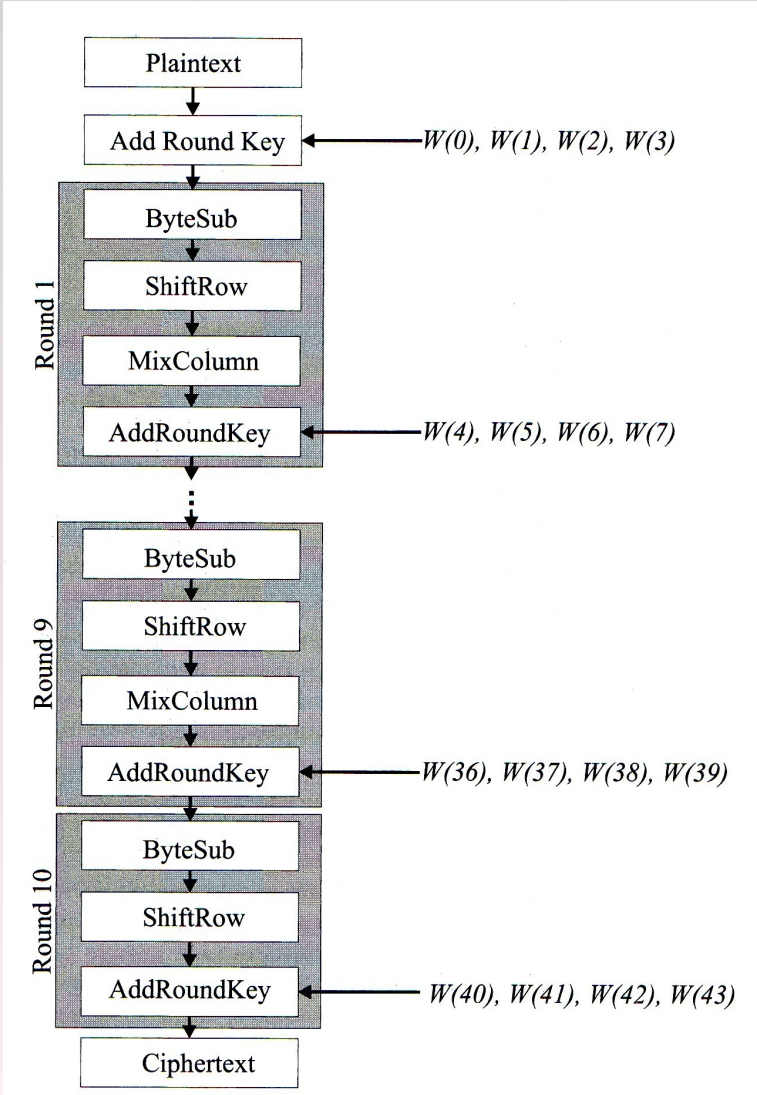
Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Advanced Encryption Standard

Funzionamento



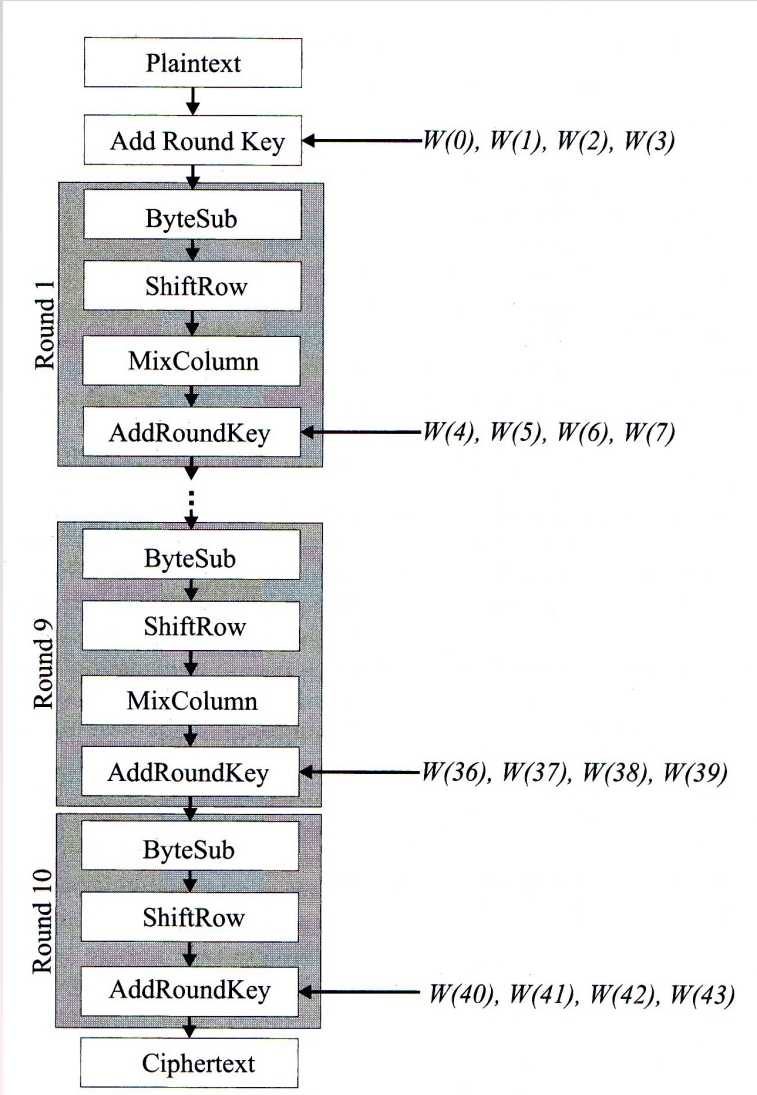
Con la chiave a 128 bits (192, 256), l'algoritmo a sinistra consta di 10 (12, 14) iterazioni.

In ogni iterazione ci sono 4 passi:

1. ByteSub Transformation.
2. ShiftRow Transformation.
3. MixColumn Transformation.
4. AddRoundKey.

Advanced Encryption Standard

Funzionamento



Con la chiave a 128 bits (192, 256), l'algoritmo a sinistra consta di 10 (12, 14) iterazioni.
In ogni iterazione ci sono 4 passi:

1. ByteSub Transformation.
2. ShiftRow Transformation.
3. MixColumn Transformation.
4. AddRoundKey.

Advanced Encryption Standard

Funzionamento

I 128 input bit sono raggruppati in 16 Bytes:

$$a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, \ldots, a_{2,3} a_{3,3}$$

organizzati in una matrice

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

Ogni $a_{i,j}$ è visto come un elemento di $GF(2^8)$ con polinomio irriducibile:$X^8 + X^4 + X^3 + X + 1$

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento

I 128 input bit sono raggruppati in 16 Bytes:

$$a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, \ldots, a_{2,3} a_{3,3}$$

organizzati in una matrice

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

Ogni $a_{i,j}$ è visto come un elemento di $GF(2^8)$ con polinomio irriducibile: $X^8 + X^4 + X^3 + X + 1$

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Advanced Encryption Standard

Funzionamento

I 128 input bit sono raggruppati in 16 Bytes:

$$a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, \ldots, a_{2,3} a_{3,3}$$

organizzati in una matrice

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

Ogni $a_{i,j}$ è visto come un elemento di $GF(2^8)$ con polinomio irriducibile:$X^8 + X^4 + X^3 + X + 1$

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento: $GF(2^8)$ con $p(X) = X^8 + X^4 + X^3 + X + 1$

Le somme sono or-esclusivi bit per bit

$$\begin{array}{r} X^7+X^5+X^4+X^3+X+ \\ X^6+X^5+X^4+X^2+X+1 \\ \hline X^7+X^6+X^3+X^2+1 \end{array} = \begin{array}{r} 10111010 \\ 01110111 \\ \hline 11001101 \end{array} \oplus =$$

I prodotti sono invece operazioni in $GF(2^8)$ modulo $p(X)$:

$$\begin{array}{r} (X^5+X^4+X^3+X) \\ (X^6+X) \\ \hline X^{11}+X^{10}+X^9+X^7+X^6+X^5+X^4+X^2 \\ \hline X^6+X^5+X^4+X^2+X \end{array} = \begin{array}{r} 00111010 \\ 01000010 \\ \hline 01110110 \end{array} \times \times =$$

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento: $GF(2^8)$ con $p(X) = X^8 + X^4 + X^3 + X + 1$

Le somme sono or-esclusivi bit per bit

$$\begin{array}{r} X^7+X^5+X^4+X^3+X+ \\ X^6+X^5+X^4+X^2+X+1 \\ \hline X^7+X^6+X^3+X^2+1 \end{array} = \quad \begin{array}{r} 10111010 \oplus \\ 01110111 = \\ \hline 11001101 \end{array}$$

I prodotti sono invece operazioni in $GF(2^8)$ modulo $p(X)$:

$$\begin{array}{r} (X^5+X^4+X^3+X) \\ (X^6+X) \\ \hline X^{11}+X^{10}+X^9+X^7+X^6+X^5+X^4+X^2 \\ \hline X^6+X^5+X^4+X^2+X \end{array} \begin{array}{c} \times \\ = \\ = \end{array} \quad \begin{array}{r} 00111010 \times \\ 01000010 = \\ \hline 01110110 \end{array}$$

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento: ByteSub Transformation

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Sia $a_7 \cdots a_0$ un elemento della matrice.

Si guarda la riga $a_7 a_6 a_5 a_4$ e la colonna $a_3 a_2 a_1 a_0$.

Si rappresenta con un byte il numero indicato.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento: ByteSub Transformation

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Sia $a_7 \cdots a_0$ un elemento della matrice.

Si guarda la riga $a_7 a_6 a_5 a_4$ e la colonna $a_3 a_2 a_1 a_0$.

Si rappresenta con un byte il numero indicato.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento: ByteSub Transformation

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Sia $a_7 \cdots a_0$ un elemento della matrice.
Si guarda la riga $a_7 a_6 a_5 a_4$ e la colonna $a_3 a_2 a_1 a_0$.
Si rappresenta con un byte il numero indicato.

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Advanced Encryption Standard

Funzionamento: ByteSub Transformation

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \Longrightarrow \underbrace{\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{pmatrix}}_{B}$$

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento: ShiftRow Transformation

$$\underbrace{\begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}}_{C} = \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,1} & b_{1,2} & b_{1,3} & b_{1,0} \\ b_{2,2} & b_{2,3} & b_{2,0} & b_{2,1} \\ b_{3,3} & b_{3,0} & b_{3,1} & b_{3,2} \end{pmatrix}$$

Le righe sono shiftate ciclicamente a sinistra di 0, 1, 2, 3.
Dunque $c_{i,j} = b_{i,(i+j) \mod 4}$

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento: MixColumn Transformation

$$\underbrace{\begin{pmatrix} X & X+1 & 1 & 1 \\ 1 & X & X+1 & 1 \\ 1 & 1 & X & X+1 \\ X+1 & 1 & 1 & X \end{pmatrix} \times \begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}}_{D}$$

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento: RoundKey Addition

K, detta RoundKey, è una matrice ottenuta dalla chiave che descriviamo dopo.

$$\underbrace{\overbrace{\begin{pmatrix} d_{0,0} & d_{0,1} & d_{0,2} & d_{0,3} \\ d_{1,0} & d_{1,1} & d_{1,2} & d_{1,3} \\ d_{2,0} & d_{2,1} & d_{2,2} & d_{2,3} \\ d_{3,0} & d_{3,1} & d_{3,2} & d_{3,3} \end{pmatrix}}^{D} \oplus \overbrace{\begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{pmatrix}}^{K}}_{E}$$

E è l'output (128 bit) dell'iterazione.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento: Chiave

- La chiave originale è di 128 bits, considerati in una matrice W 4×4 di bytes (o elementi di $GF(2^8)$)
- Siano $W(0), W(1), W(2), W(3)$ le quattro colonne di W
- La matrice è allargata aggiungendo altre 40 colonne $W(4), \ldots, W(43)$ usando la regola:

$$W(i) = \begin{cases} W(i-4) \oplus W(i-1) & \text{Se } i \bmod 4 \neq 0 \\ W(i-4) \oplus T(W(i-1)) & \text{Se } i \bmod 4 = 0 \end{cases}$$

  dove T la vediamo subito.
- La RoundKey per l'iterazione j consiste nella matrice: $(W(4j), W(4j+1), W(4j+2), W(4j+3))$.

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Advanced Encryption Standard

Funzionamento: Chiave

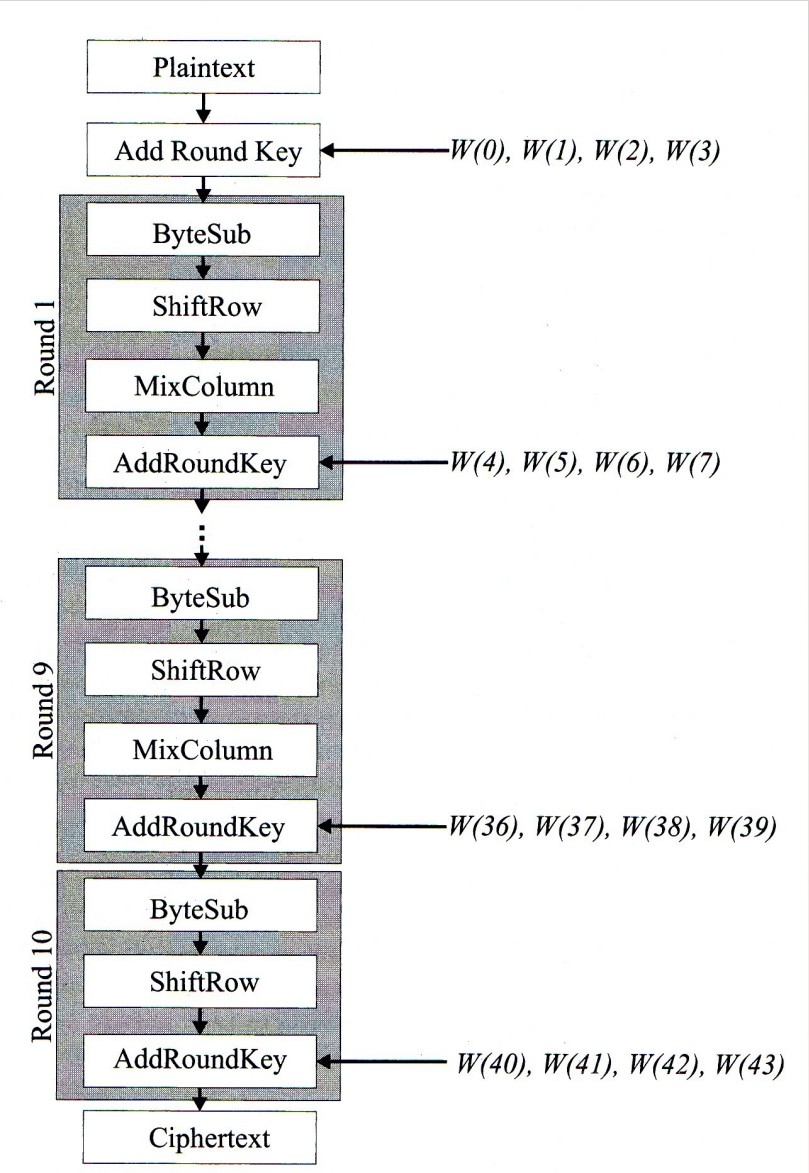
- Definiamo la trasformazione $T(W(i))$ (i multiplo di 4).
- $W(i)$ viene shiftato ciclicamente e poi sostituto usando la S-Box:

$$W(i) = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \xRightarrow{\text{shift}} \begin{pmatrix} b \\ c \\ d \\ a \end{pmatrix} \xRightarrow{\text{S-Box}} \begin{pmatrix} e \\ f \\ g \\ h \end{pmatrix}$$

- Si calcola $r(i) = X^{\left(\frac{i-4}{4}\right)}$ in $GF(2^8)$
- Si definisce $T(W(i)) = \begin{pmatrix} e \oplus r(i) \\ f \\ g \\ h \end{pmatrix}$

Advanced Encryption Standard

Funzionamento: Riassunto



Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Decifrazione

- Le varie operazioni sono invertibili.
- C'è l'inversa della S-Box
- C'è l'inversa della ShiftRow (basta shiftare a dx)
- C'è l'inversa della MixColumn (la matrice è invertibile)
- Per la RoundKey si usa la stessa.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Decifrazione

Cifrazione
ARK(0–3)
BS,SR, MC, ARK (4–7)
⋮
BS,SR, MC, ARK (36–39)
BS,SR, ARK (40–43)

Decifrazione
ARK (40–43), ISR, IBS
ARK (36–39), IMC, ISR, IBS
⋮
ARK (4–7), IMC, ISR, IBS
ARK (0–3)

Si può lavorare sulla decifrazione in modo da renderla un pò più simile (ma non uguale) alla cifrazione.
Il fatto che non siano uguali è un punto di forza.

Automazione della crittografia

L'Enigma
- Turing a Bletchley Park
- Funzionamento dell'Enigma
- Decrittazione dell'Enigma
- Films e Libri
- Note finali

Trasposizioni

DES
- Introduzione
- Cifrazione
- Decifrazione
- Decrittazione

AES
- Introduzione
- Funzionamento
- Trasformazioni
- Chiave
- Decifrazione
- Sicurezza

Advanced Encryption Standard

Decifrazione

Cifrazione
ARK(0–3)
BS,SR, MC, ARK (4–7)
⋮
BS,SR, MC, ARK (36–39)
BS,SR, ARK (40–43)

Decifrazione
ARK (40–43), ISR, IBS
ARK (36–39), IMC, ISR, IBS
⋮
ARK (4–7), IMC, ISR, IBS
ARK (0–3)

Si può lavorare sulla decifrazione in modo da renderla un pò più simile (ma non uguale) alla cifrazione.

Il fatto che non siano uguali è un punto di forza.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Decifrazione

Cifrazione
ARK(0–3)
BS,SR, MC, ARK (4–7)
⋮
BS,SR, MC, ARK (36–39)
BS,SR, ARK (40–43)

Decifrazione
ARK (40–43), ISR, IBS
ARK (36–39), IMC, ISR, IBS
⋮
ARK (4–7), IMC, ISR, IBS
ARK (0–3)

Si può lavorare sulla decifrazione in modo da renderla un pò più simile (ma non uguale) alla cifrazione.
Il fatto che non siano uguali è un punto di forza.

Automazione della crittografia
L'Enigma
Turing a Bletchley Park
Funzionamento dell'Enigma
Decrittazione dell'Enigma
Films e Libri
Note finali
Trasposizioni
DES
Introduzione
Cifrazione
Decifrazione
Decrittazione
AES
Introduzione
Funzionamento
Trasformazioni
Chiave
Decifrazione
Sicurezza

Advanced Encryption Standard

Funzionamento: S-Box

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Funzionamento: S-Box

- La matrice S-Box non è casuale.
- Consideriamo il byte $\vec{b} = b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0$
- Sia $\vec{e} = e_7 e_6 e_5 e_4 e_3 e_2 e_1 e_0$ il suo inverso in $GF(2^8)$ (assumiamo che l'inverso di $\vec{0}$ sia lui stesso).
- Passare all'inverso spezza sia attacchi lineari, che differenziali, che di interpolazione.
- $\vec{z}$ si ottiene moltiplicando una matrice (simmetrica) per $\vec{e}$ e sommando al risultato il vettore $(1, 1, 0, 0, 0, 1, 1, 0)$.
- $z_7 z_6 z_5 z_4 z_3 z_2 z_1 z_0$ è la entry nella S-box.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza

Advanced Encryption Standard

Considerazioni finali

- S-Box che usa l'inverso spezza sia attacchi lineari, che differenziali, che di interpolazione.
- ShiftRow serve a resistere a due attacchi denominati *differenziali troncati* e *square*.
- MixColumn serve a spargere rapidamente la chiave tra i vari bits
- Il numero di iterazioni (10, 12, 14) serve in quanto ci sono attacchi migliori della forza bruta per 6 iterazioni. 10 è un valore di tranquillità.

Automazione della crittografia

L'Enigma

Turing a Bletchley Park

Funzionamento dell'Enigma

Decrittazione dell'Enigma

Films e Libri

Note finali

Trasposizioni

DES

Introduzione

Cifrazione

Decifrazione

Decrittazione

AES

Introduzione

Funzionamento

Trasformazioni

Chiave

Decifrazione

Sicurezza