CODICI SEGRETI

Agostino Dovier

Dip di Matematica e Informatica, Univ. di Udine

Ringrazio l'amico e maestro Andrea Sgarro per il materiale tratto dal suo meraviglioso quanto introvabile testo

CODICI SEGRETI

SOSTITUZIONE POLIALFABETICA ALGEBRICA (IN $\mathbb{Z}_{26}$)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Parola chiave: UDINE (=20,3,8,13,4). Testo in chiaro: Oggi la lezione è noiosa.

O	G	G	I	L	A	L	E	Z	I	O	N	E	E	N	O	I	O	S	A
14	6	6	8	11	1	11	4	25	8	13	14	4	4	13	14	8	14	18	1
20	3	8	13	4	20	3	8	13	4	20	3	8	13	4	20	3	8	13	4
8	9	14	21	15	21	14	12	12	12	7	17	12	17	17	8	11	22	5	5
I	J	O	V	P	V	O	M	M	M	H	Q	M	R	R	I	L	W	F	E

Testo in cifra: IJOVPVOMMMHQMRRILWFE
(ovviamente non usiamo gli accenti!)

Codici Segreti

Sostituzione polialfabetica algebrica (in $\mathbb{Z}_2$)

A B C D E	F G H I J	K L M N O	P Q R S T	U V W X Y	Z ♣ ◇ ♡ ♠	♭ ♯
0 1 2 3 4	5 6 7 8 9	10 11 12 13 14	15 16 17 18 19	20 21 22 23 24	25 26 27 28 29	30 31

Chiave: UDINE= 20,3,8,13,4 = 10100, 00011, 01000, 01101, 00100

Testo in chiaro: Oggi la lezione è noiosa.

O	G	G	I	L	A	L	E	Z	I
01110	00110	00110	01000	01011	00001	01011	00100	11001	01000
10100	00011	01000	01101	00100	10100	00011	01000	01101	00100
11010	00101	01110	00101	01111	10101	01000	01100	10100	01100
♣	F	O	F	P	V	Q	M	U	M

O	N	E	E	N	O	I	O	S	A
01101	01110	00100	00100	01101	01110	01000	01110	01010	00001
10100	00011	01000	01101	00100	10100	00011	01000	01101	00100
01001	01101	01100	01001	01001	11010	01011	00110	00111	00101
J	N	M	J	J	♣	L	G	H	F

Testo in cifra: ♣FOFPVQMUMJNMJJ♣LGHF

Codici Segreti

Sostituzione polialfabetica algebrica (in $\mathbb{Z}_2$)

- Lavorando in $\mathbb{Z}_2$ si perde un pò di contatto umano con la crittografia
- Ma il tutto diventa adatto all'automazione digitale.
- Per ogni i avremo che $e_i = m_i \oplus k_i$ ove $\oplus$ è or-esclusivo.
- La chiave è una stringa binaria. La statistica linguistica va eventualmente applicata ai bytes.
- Più lunga è la chiave meglio (intuitivamente) è.

Il cifrario perfetto

Gilbert Vernam (1890–1960): one-time-pad

- Ogni bit usato per cifrare viene generato da un lancio di moneta.
- La chiave è lunga quanto il testo e
- Non viene più riutilizzata
- Sembra indecifrabile.
- Lo è.
- Come comunichiamo la chiave?

Il cifrario perfetto

Gilbert Vernam (1890–1960): one-time-pad

- Ogni bit usato per cifrare viene generato da un lancio di moneta.
- La chiave è lunga quanto il testo e
- Non viene più riutilizzata
- Sembra indecifrabile.
- Lo è.
- Come comunichiamo la chiave?

Il cifrario perfetto

Gilbert Vernam (1890–1960): one-time-pad

- Ogni bit usato per cifrare viene generato da un lancio di moneta.
- La chiave è lunga quanto il testo e
- Non viene più riutilizzata
- Sembra indecifrabile.
- Lo è.
- Come comunichiamo la chiave?

Il cifrario perfetto

Indipendenza del messaggio cifrato da quello in chiaro

- Per ogni i: $e_i = m_i \oplus k_i$.
- Proviamo a calcolare $P(E_i = 0)$.

$$\begin{aligned} P(E_i = 0) &= P(E_i = 0|M_i = 0)P(M_i = 0) + \\ &\quad P(E_i = 0|M_i = 1)P(M_i = 1) \\ &= \frac{1}{2}P(M_i = 0) + \frac{1}{2}P(M_i = 1) \\ &= \frac{1}{2} \\ &= P(E_i = 1) \end{aligned}$$

- Dunque, se la moneta non è truccata, che esca 0 o 1 è equiprobabile e non dipende dal messaggio in chiaro!

Il cifrario perfetto

C. E. Shannon: Communication Theory of Secrecy Systems (1949)

- Il crittografo sa quasi tutto:
  - sistema di cifratura,
  - elenco $m_1, \ldots, m_\ell$ dei messaggi in chiaro possibili,
  - loro probabilità $P(M = m)$ a priori,
  - elenco di chiavi possibili,
  - elenco $e_1, \ldots, e_\ell$ di messaggi crittati possibili e,
  - la probabilità a posteriori $P(M = m|E = e)$ (la calcola usando ogni chiave possibile).
- Non sa la chiave.

Definition

Un cifrario è *perfetto* se per ogni coppia e, m

$$P(M = m|E = e) = P(M = m)$$

Il cifrario perfetto

C. E. Shannon: Communication Theory of Secrecy Systems (1949)

Theorem

Il cifrario one-time-pad è un cifrario perfetto.

- Sappiamo che $P(M = m|E = e) = \frac{P(E=e|M=m)P(M=m)}{P(E=e)}$
- Sappiamo che nel one-time-pad la monetina fa sí che $P(E = e|M = m) = P(E = e)$
- Dunque $P(M = m|E = e) = P(M = m)$: il cifrario è perfetto

Il cifrario perfetto

La linea rossa

Il cifrario one-time-pad fu usato nelle comunicazioni USA–URSS durante la guerra fredda.




Ci dev'essere stato un piccolo esercito di lanciatori di monete.

Il cifrario perfetto

La linea rossa

Il cifrario one-time-pad fu usato nelle comunicazioni USA–URSS durante la guerra fredda.




Ci dev'essere stato un piccolo esercito di lanciatori di monete.

Il cifrario perfetto

Numbers Station

- Le numbers stations sono stazioni radio in onde corte che trasmettono informazioni criptate.
- La codifica può essere effettuata in vari modi (che includono modulazione dell'audio). One-time-pad è uno di questi.
- Le spie concordano il codice one-time-pad assieme. Poi si spostano con la loro radio ricevente.
- Ricevendo il segnale con una radio e non si è tracciabili.
- Nel 1995–1998 c'è stato il caso della stazione cubana Atención e dell'arresto delle spie cubane denominate Wasp.

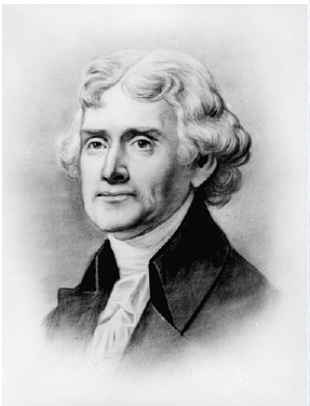
Il cifrario perfetto

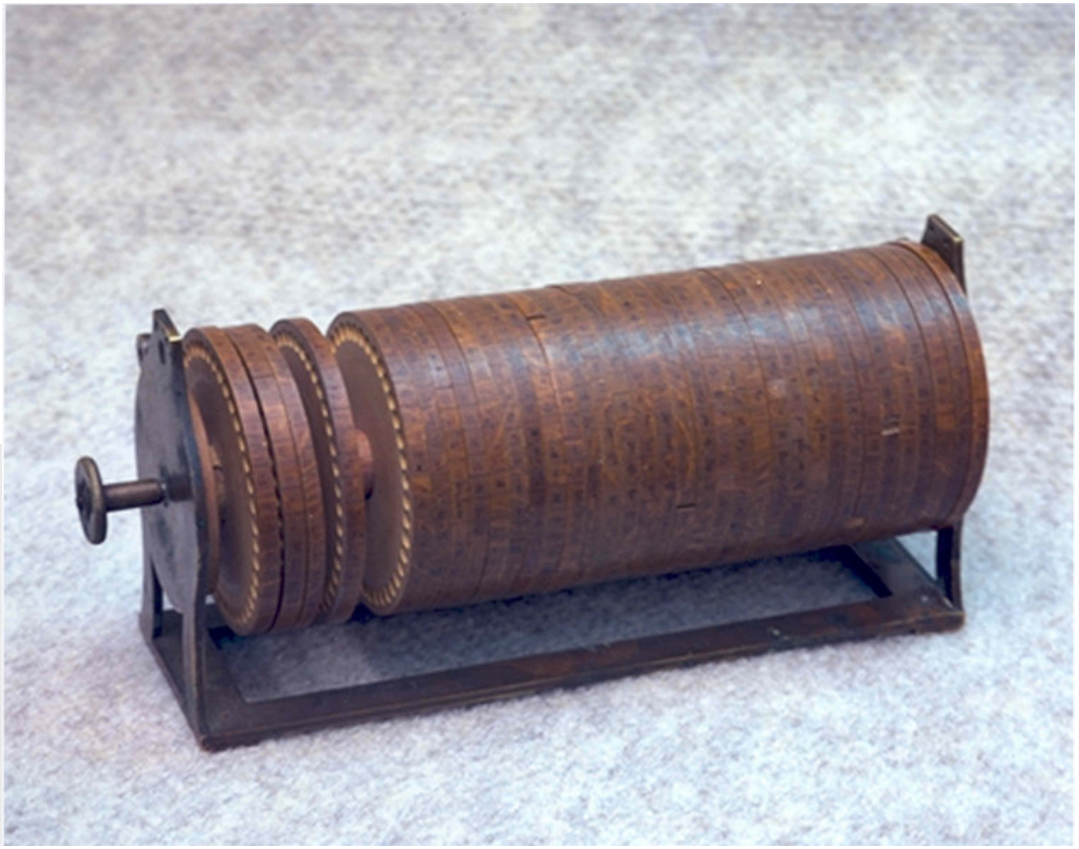
Numbers Station

- Le numbers stations sono stazioni radio in onde corte che trasmettono informazioni criptate.
- La codifica può essere effettuata in vari modi (che includono modulazione dell'audio). One-time-pad è uno di questi.
- Le spie concordano il codice one-time-pad assieme. Poi si spostano con la loro radio ricevente.
- Ricevendo il segnale con una radio e non si è tracciabili.
- Nel 1995–1998 c'è stato il caso della stazione cubana Atención e dell'arresto delle spie cubane denominate Wasp.

Automazione della crittografia

Il rotore di Thomas Jefferson (1743–1826)

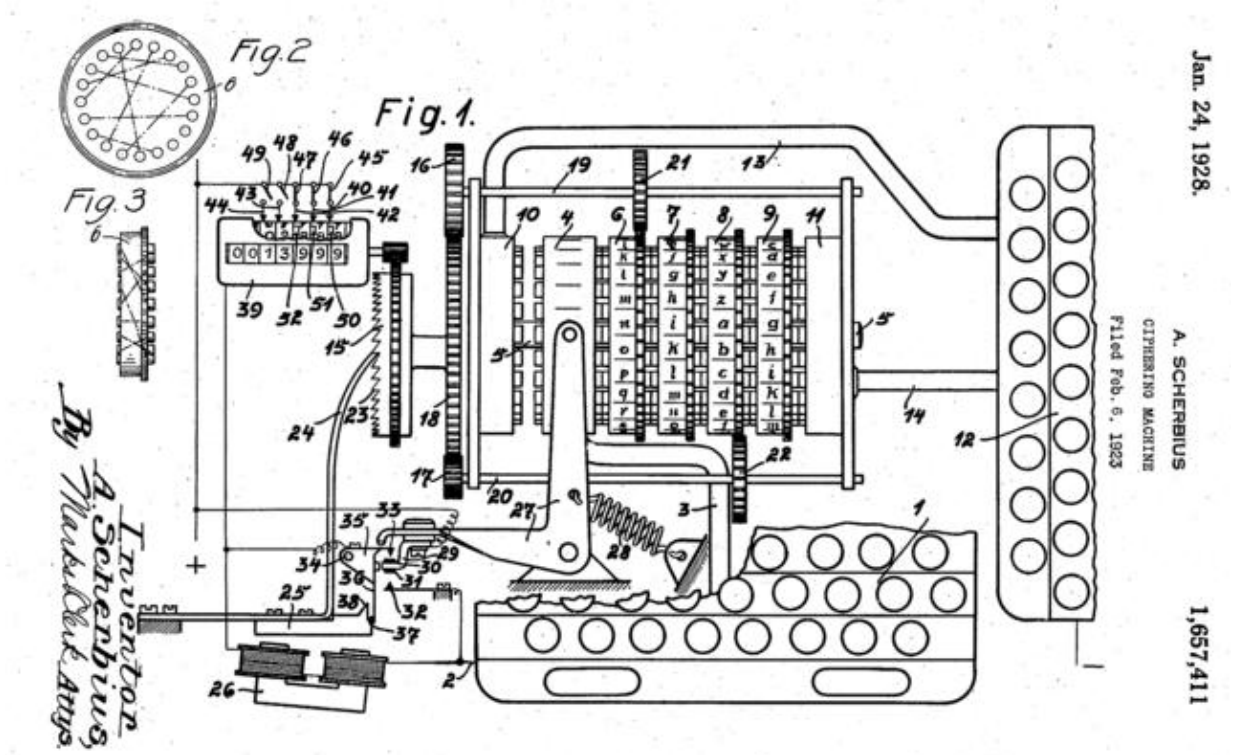




Automazione della crittografia

Arthur Scherbius (1878–1929)

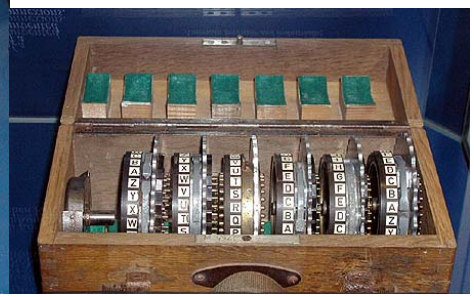
Nel 1918 brevetta una macchina da cifra a rotori (multipli)



Automazione della crittografia

Enigma

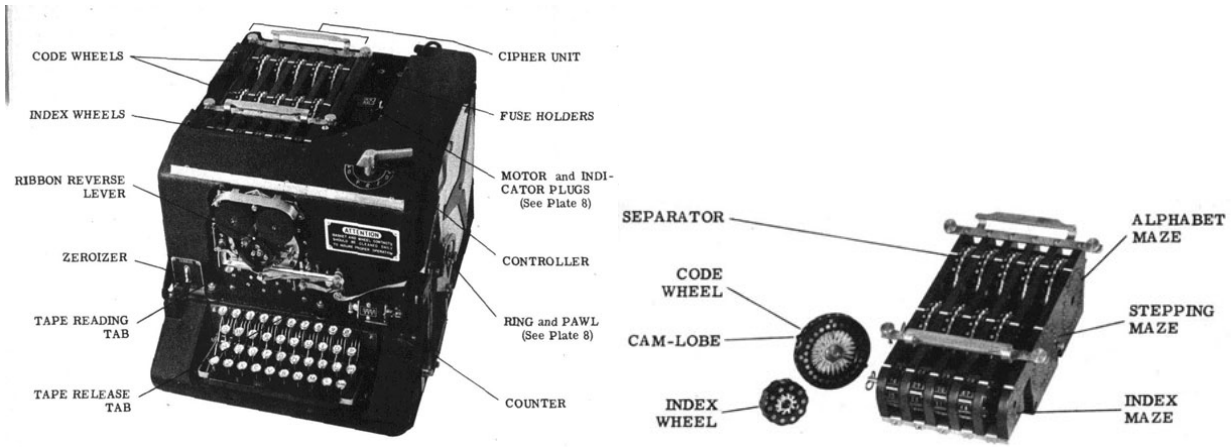
Nel 1923 Scherbius commercializza l'Enigma.



Automazione della crittografia

Edward Hugh Hebern (1869–1952)

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



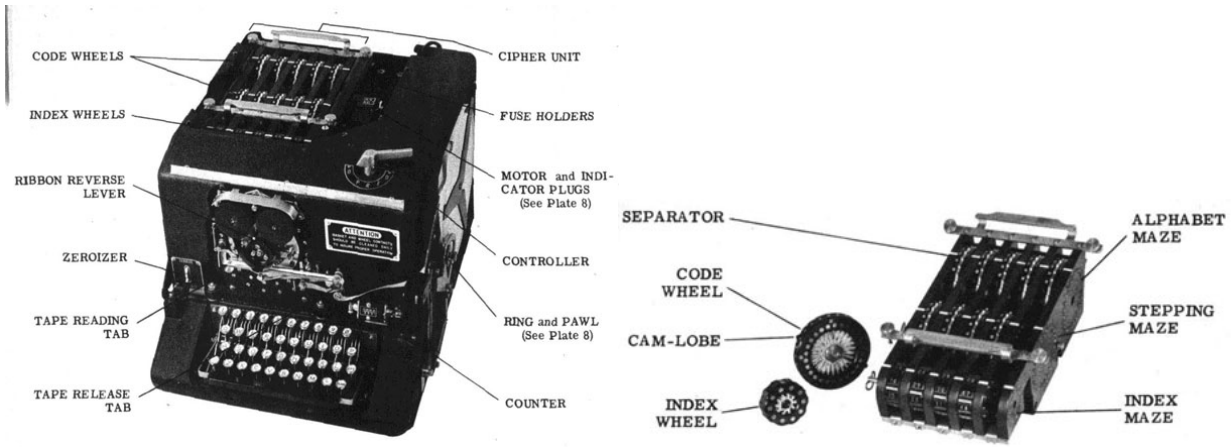
Sarà usata dall'esercito/marina USA. Non fu mai forzato

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

Automazione della crittografia

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.

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”

TURING . . .

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

ATHLETICS

MARATHON AND DECATHLON CHAMPIONSHIPS

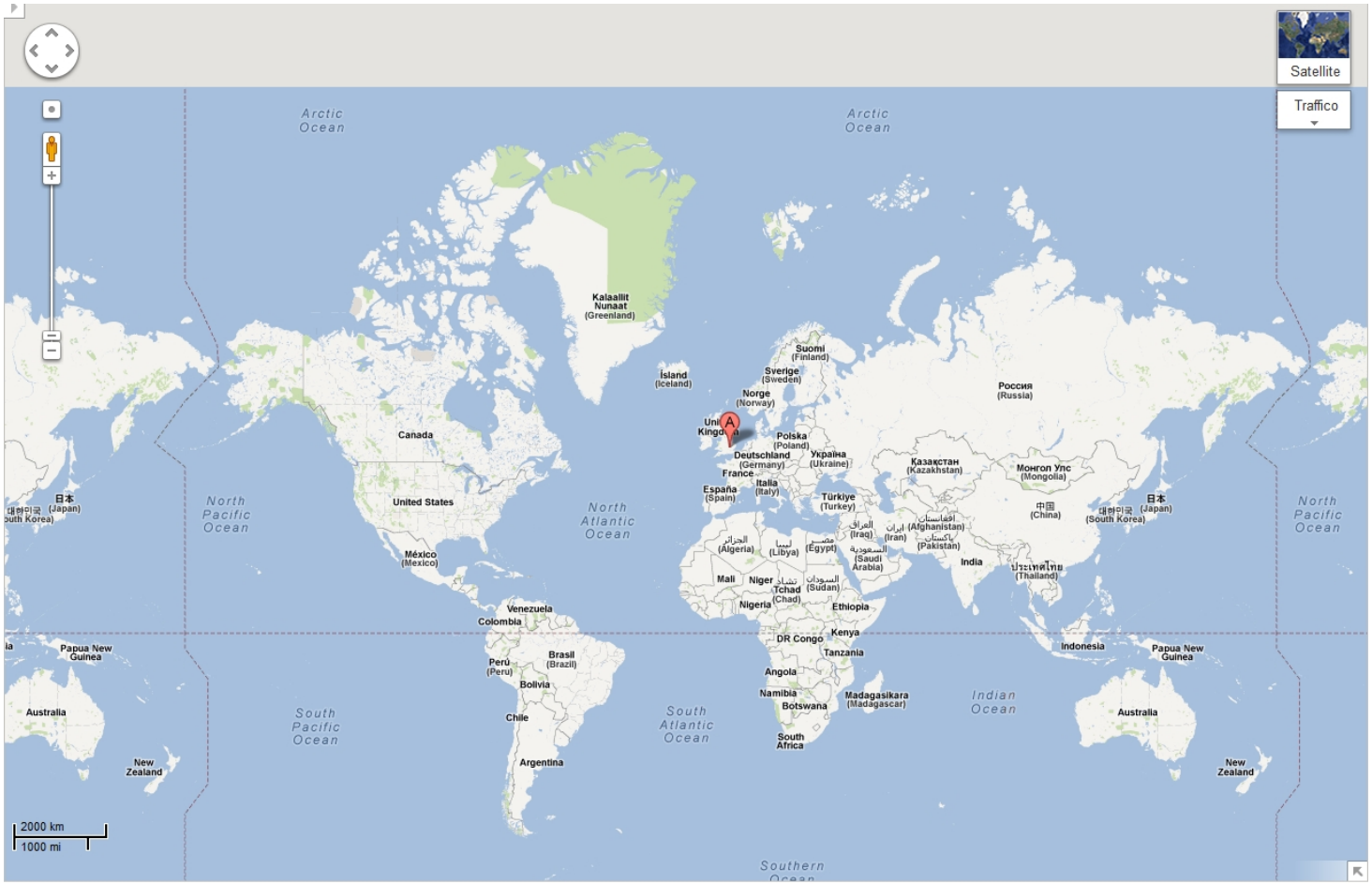
The Amateur Athletic Association championships for this year were concluded at Loughborough College Stadium, Leicestershire, on Saturday, with the second, and last, day of the Decathlon and the decision of the Marathon championship.

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.

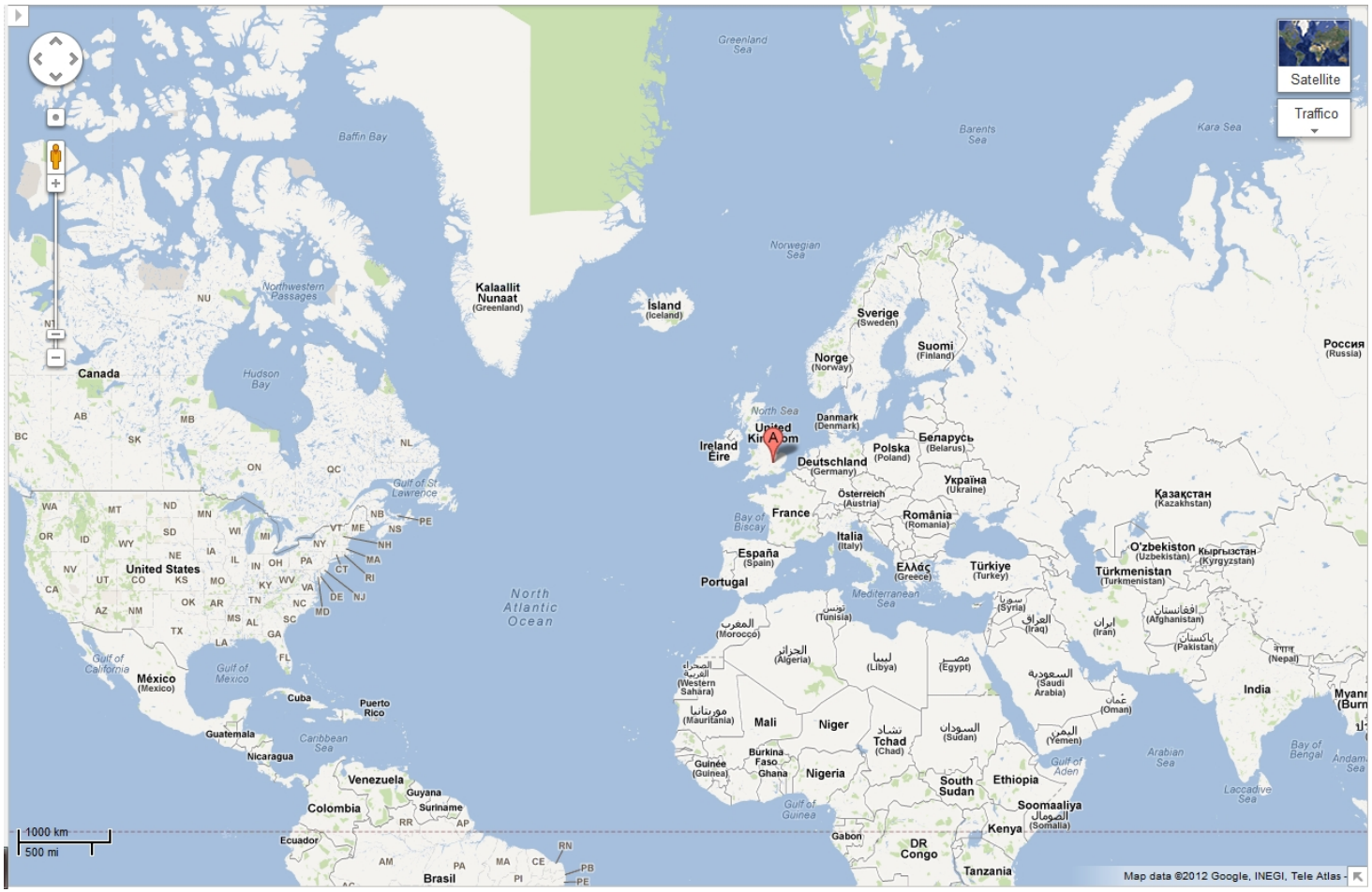
DECATHLON CHAMPIONSHIP.—H. J. Moesgaard-Kjeldsen (Polytechnic Harriers, London), 5,965 points, 1; Captain H. Whittle (Army and Reading A.C.), 5,650, 2;

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

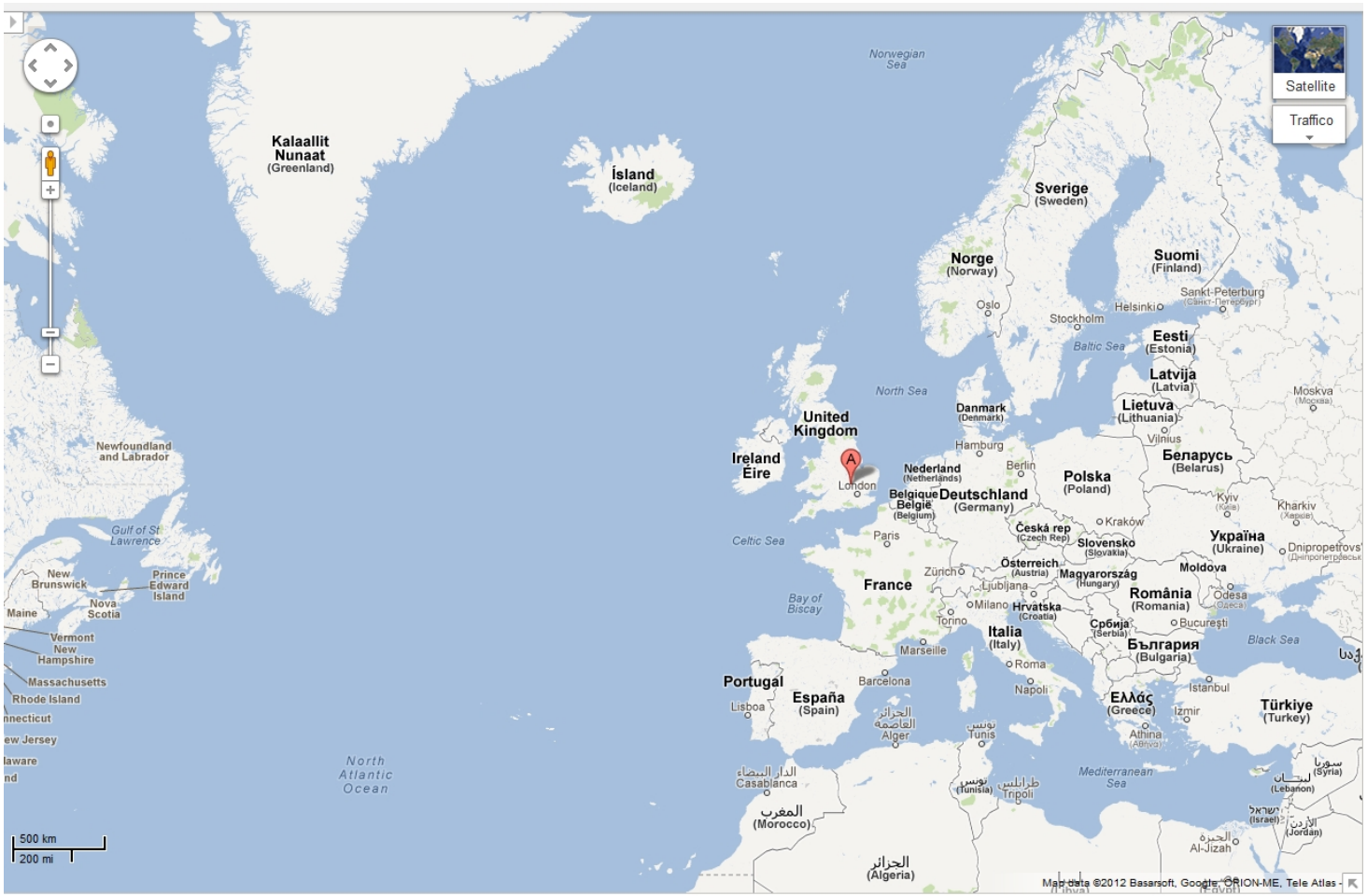
. . . a Bletchley Park



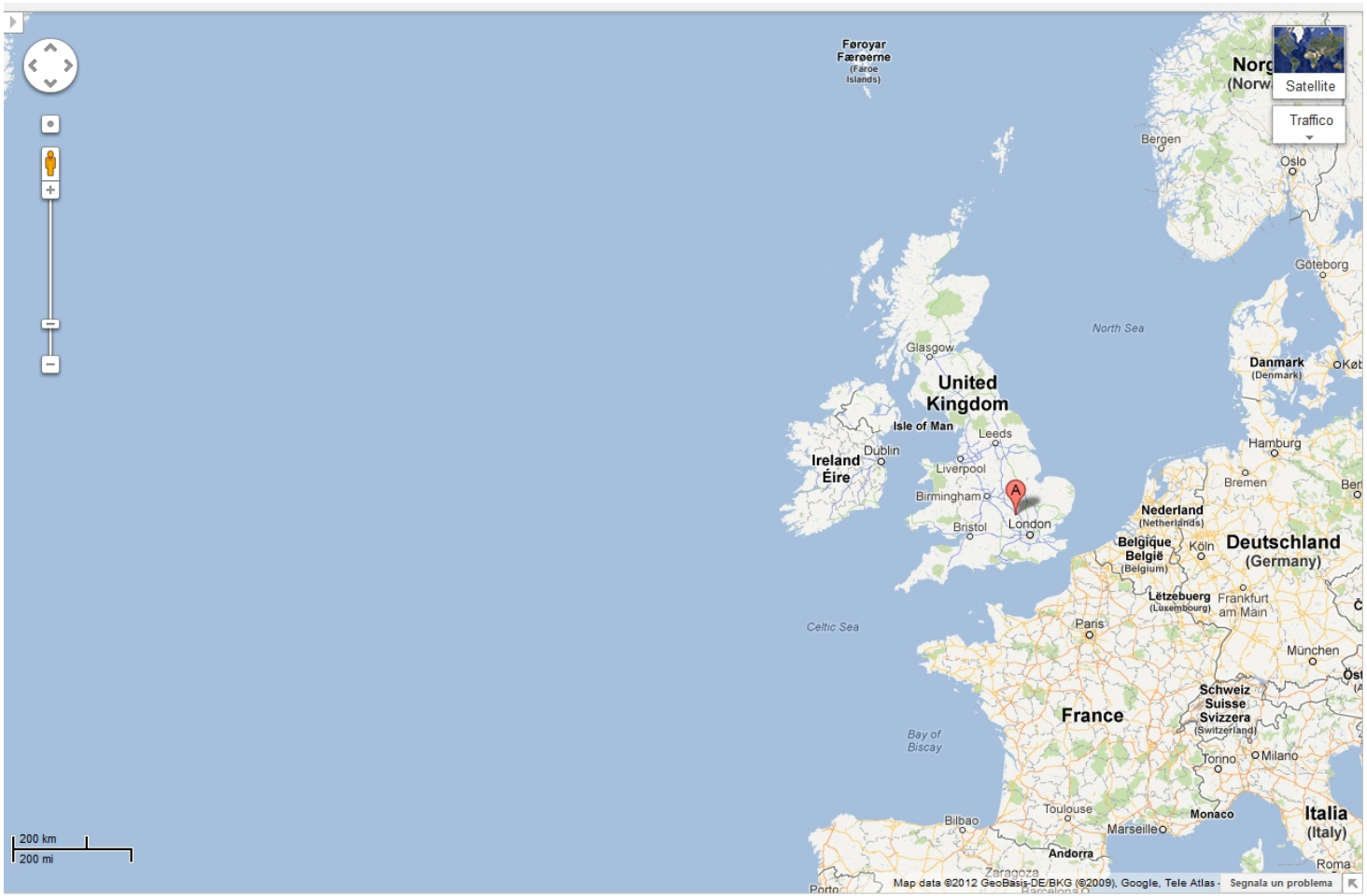
. . . a Bletchley Park



. . . a Bletchley Park



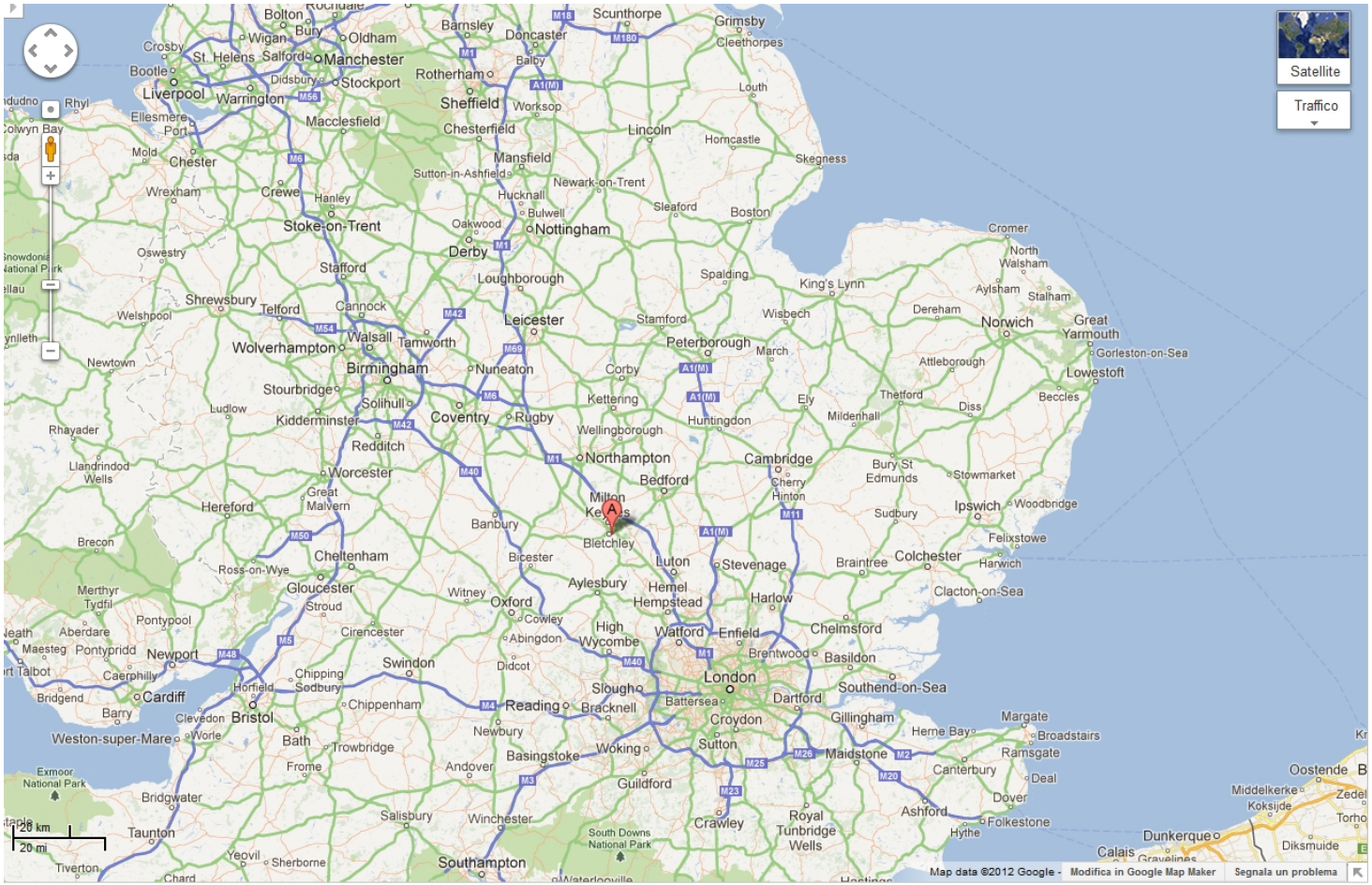
. . . a Bletchley Park



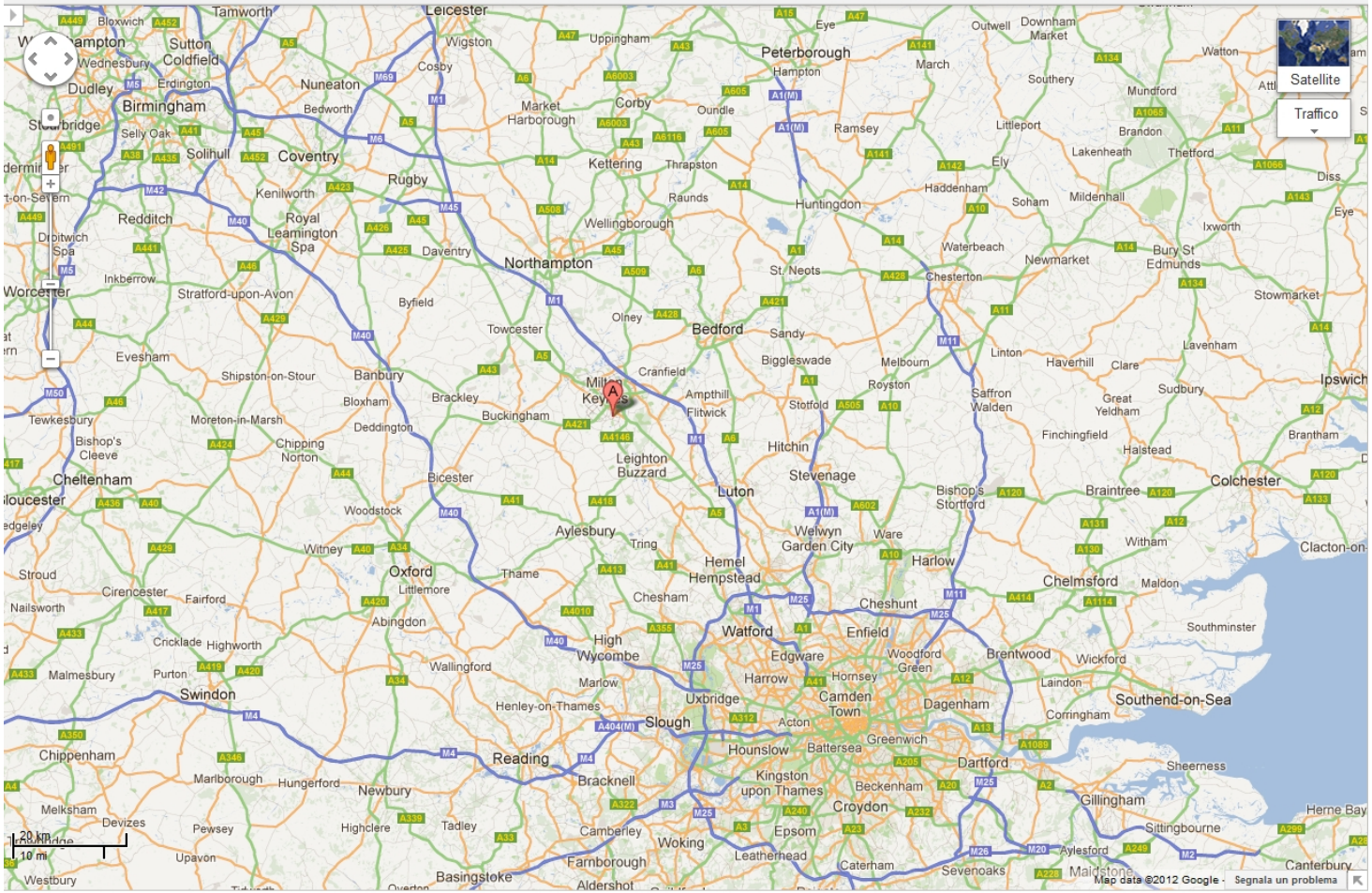
. . . a Bletchley Park

. . . a Bletchley Park

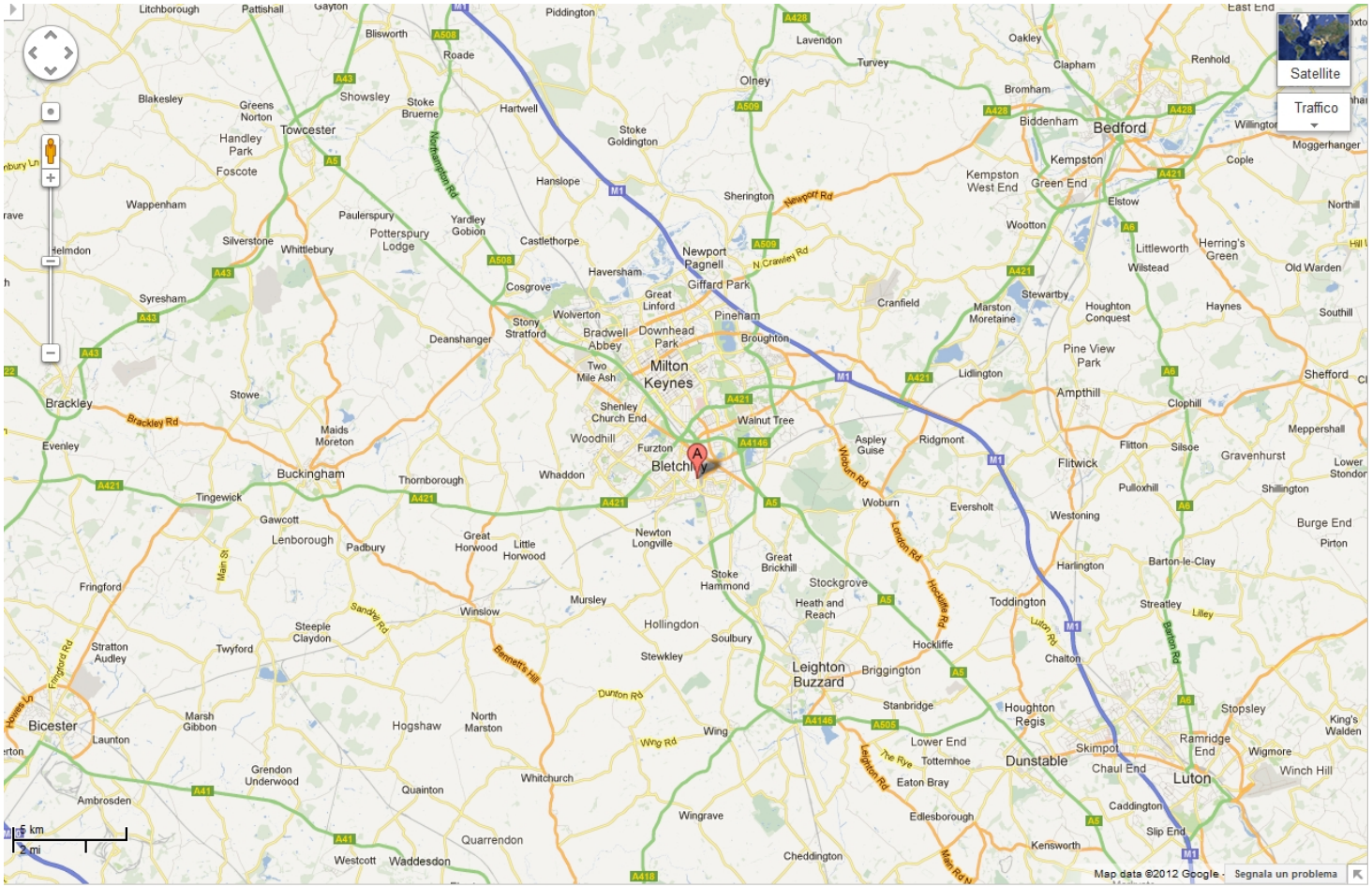
. . . a Bletchley Park



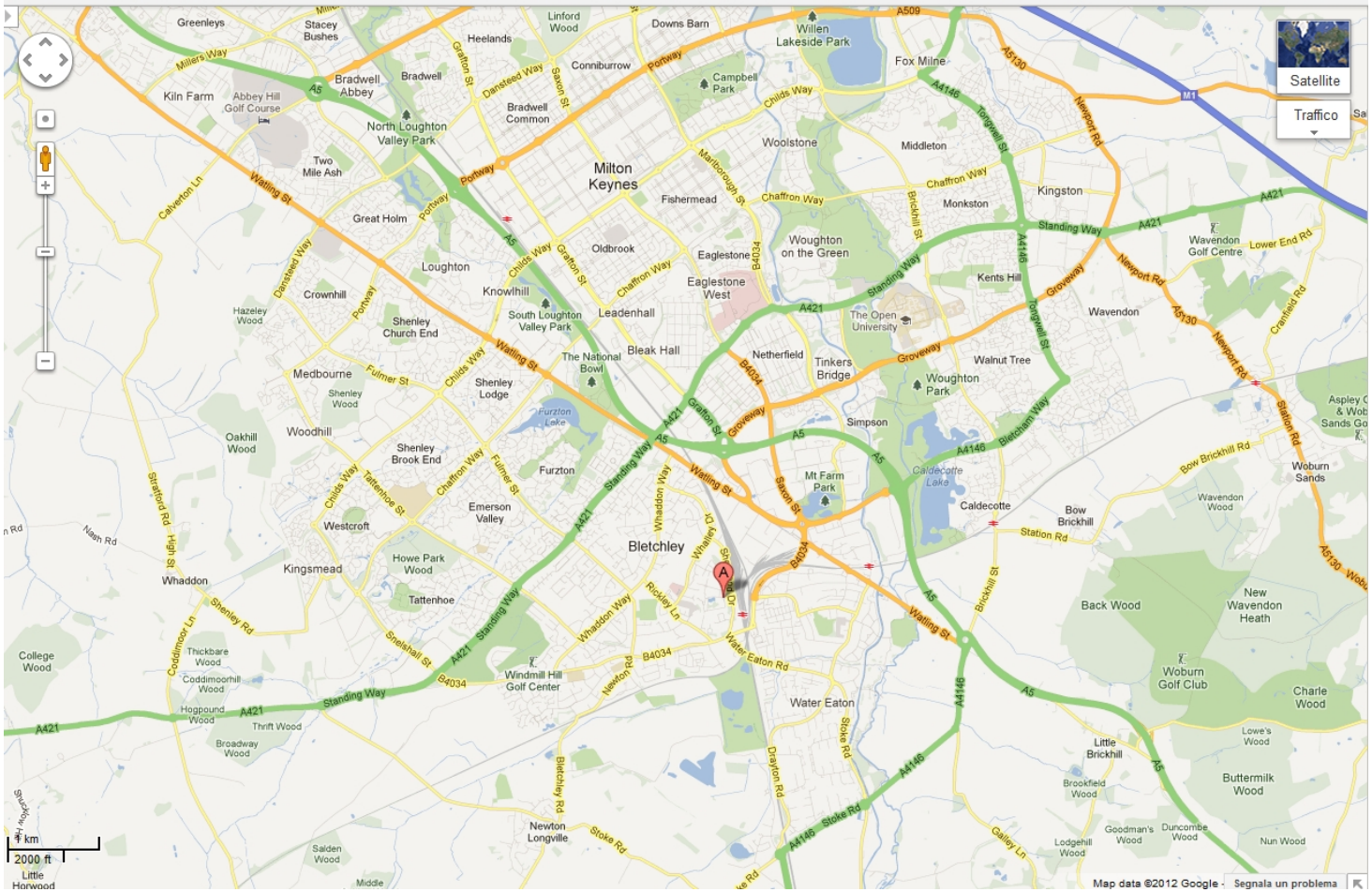
. . . a Bletchley Park



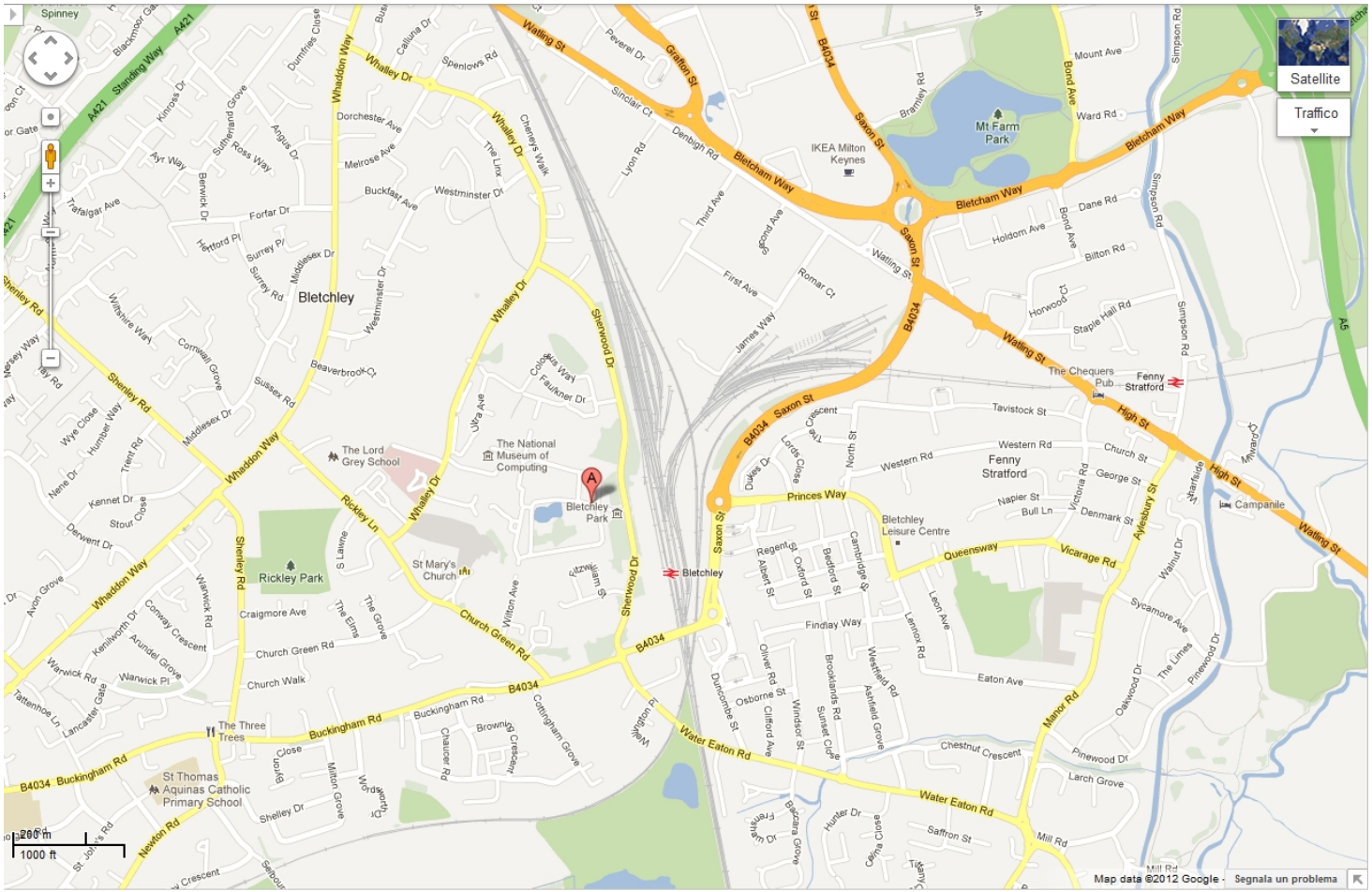
. . . a Bletchley Park



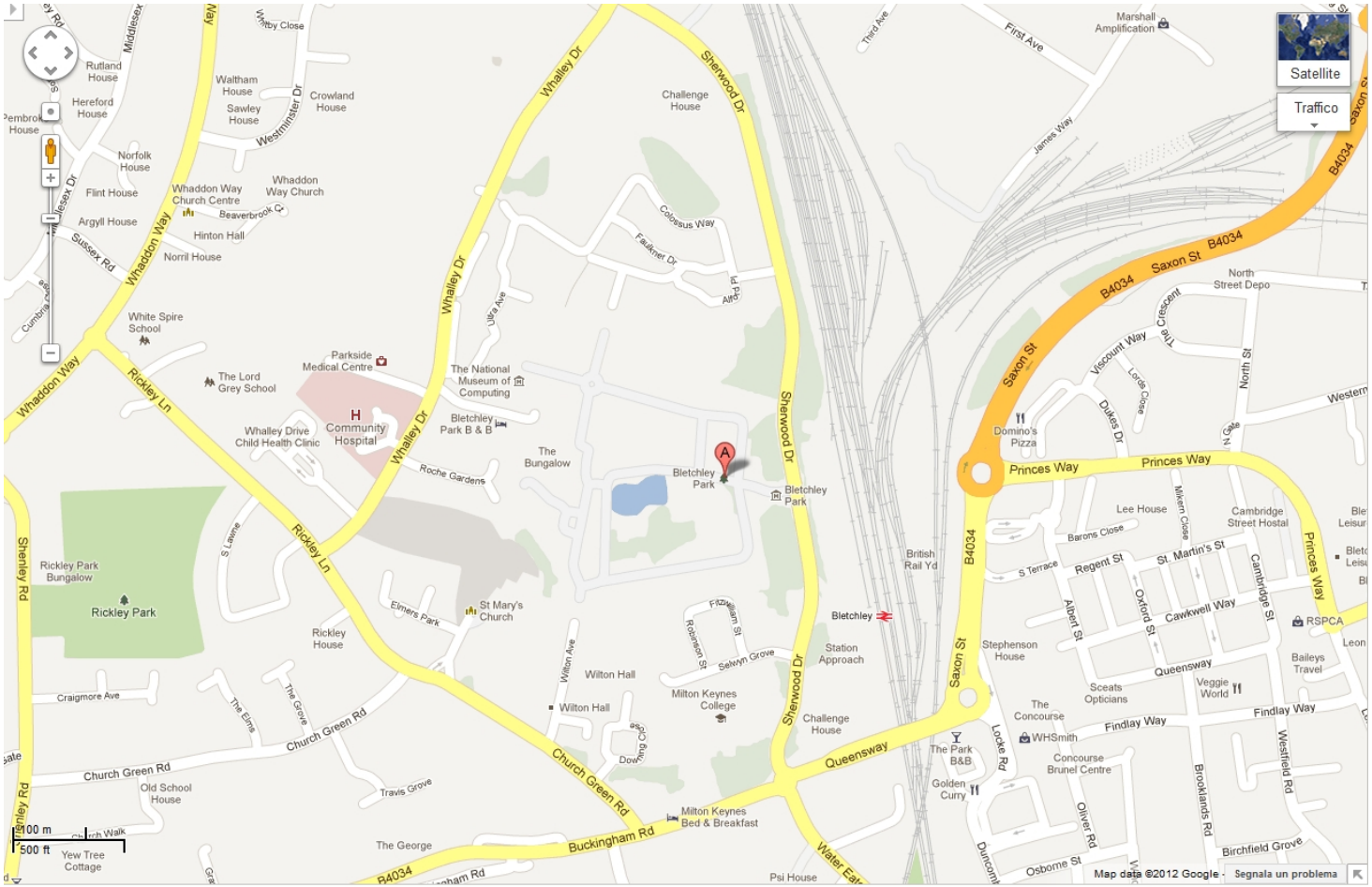
. . . a Bletchley Park



. . . a Bletchley Park

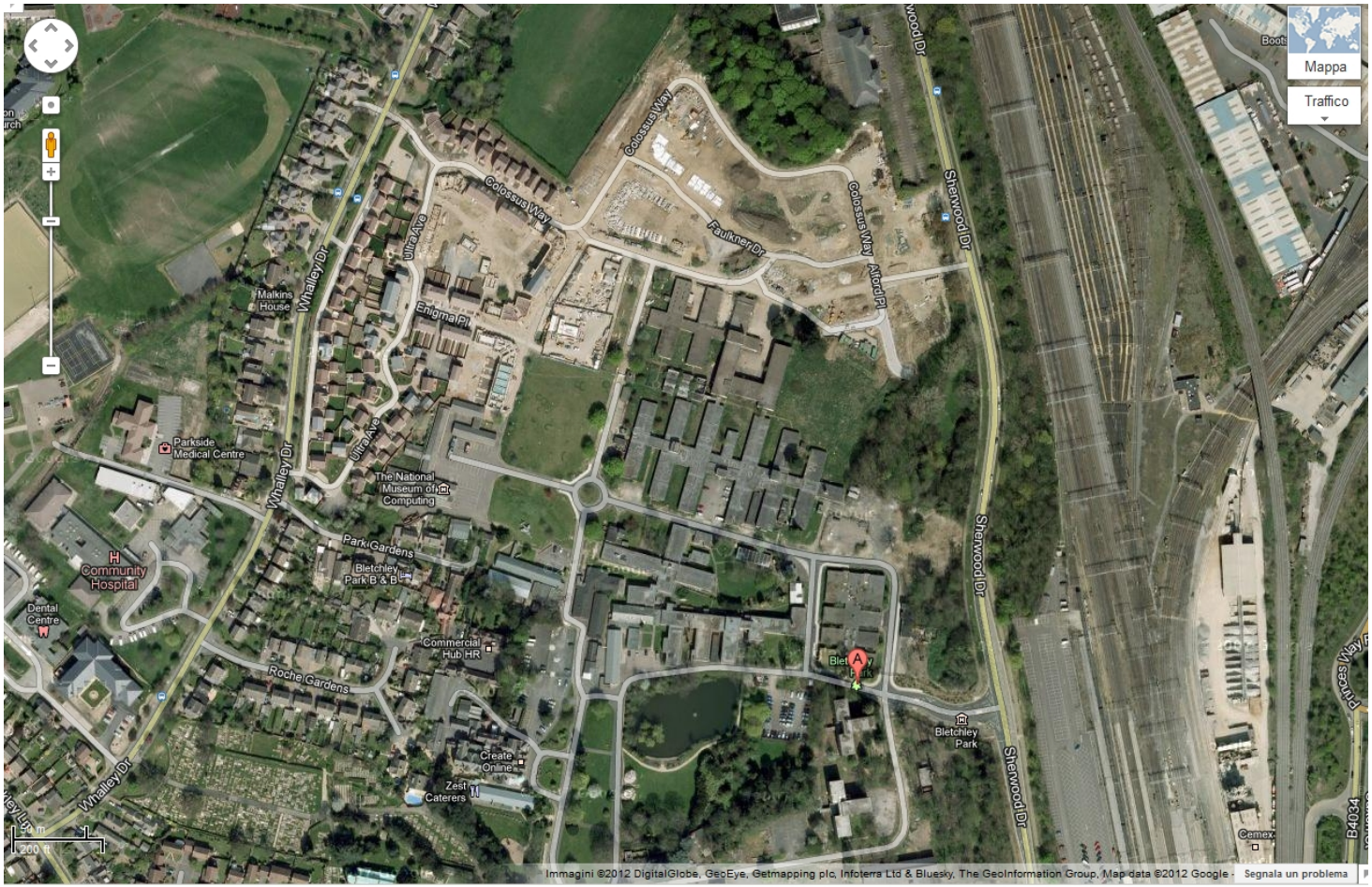


. . . a Bletchley Park

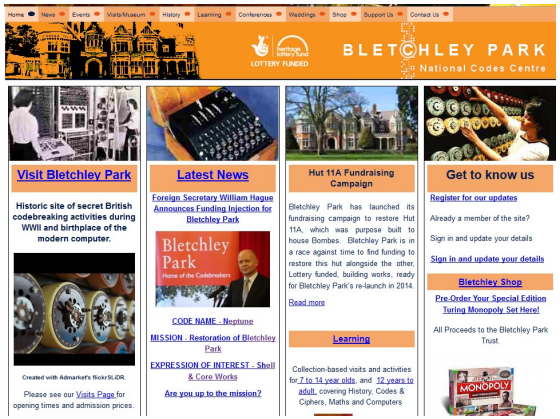


. . . a Bletchley Park

. . . a Bletchley Park



. . . a Bletchley Park

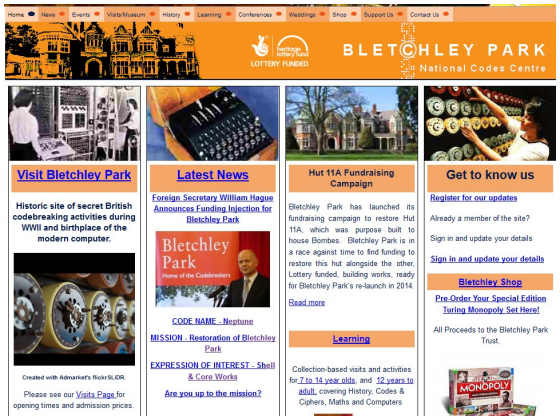


"The Government Code and Cypher School" originariamente di stanza a Londra aveva bisogno di un posto più sicuro dove lavorare e nel 1938 decise di installarsi a Bletchley Park. Nell'agosto 1939 divenne il centro operativo del controspionaggio inglese.

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.

. . . a Bletchley Park

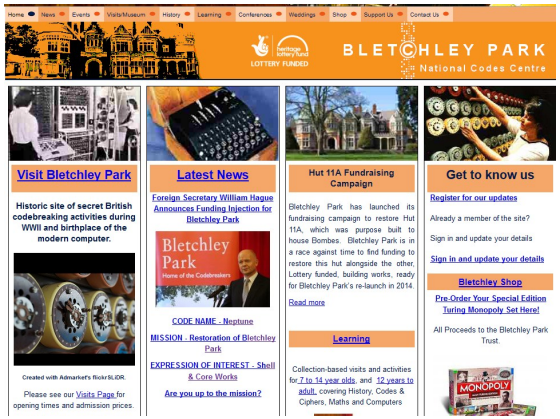


"The Government Code and Cypher School" originariamente di stanza a Londra aveva bisogno di un posto più sicuro dove lavorare e nel 1938 decise di installarsi a Bletchley Park. Nell'agosto 1939 divenne il centro operativo del controspionaggio inglese.

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.

. . . 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)

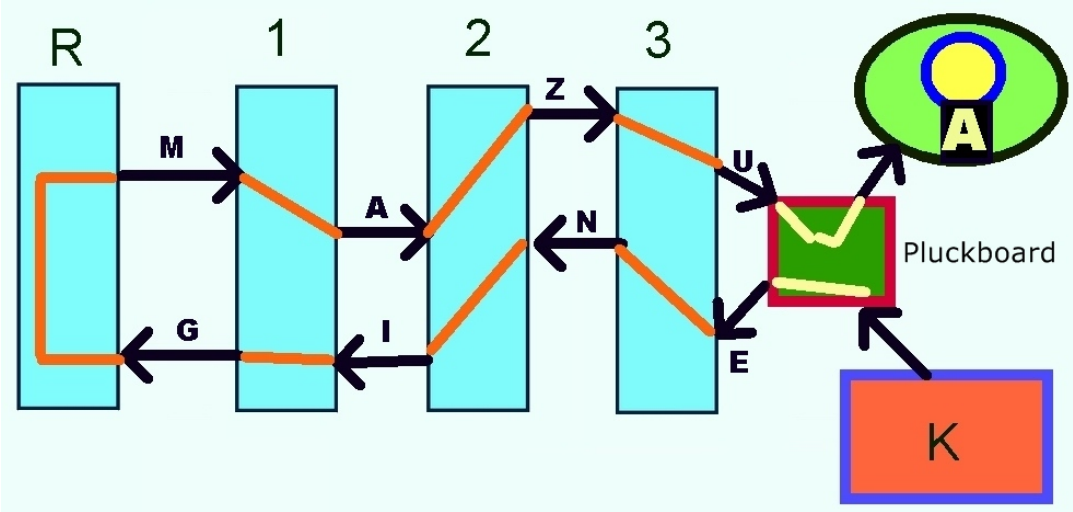
Alan Turing ebbe un ruolo cruciale nel team per la decrittazione dell'Enigma, la "macchina da cifra" impiegata dall'esercito e dalla marina tedesca.

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).

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).

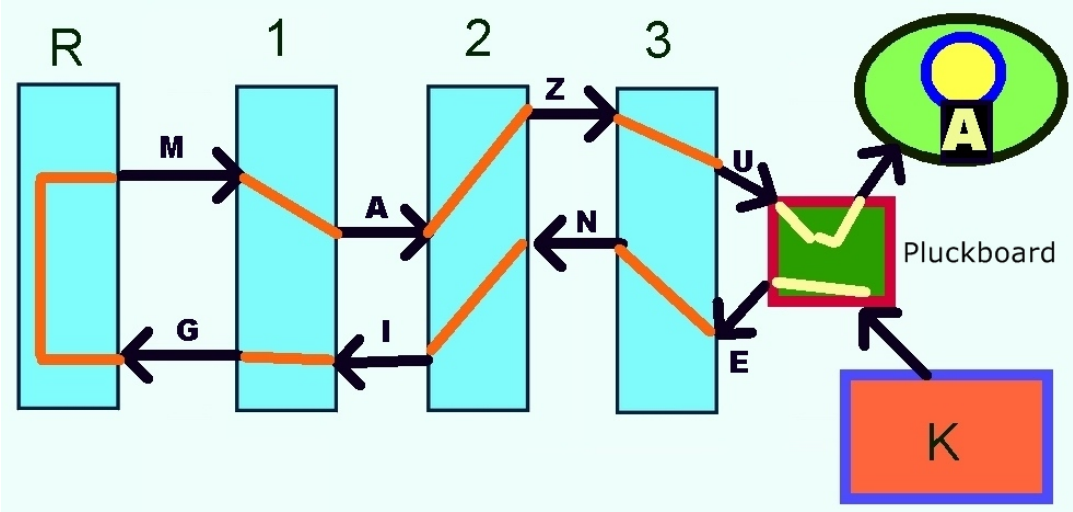


Ogni rotore ha 26 contatti su una faccia e 26 sull'altra e implementa una sostituzione monoalfabetica (completa).

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

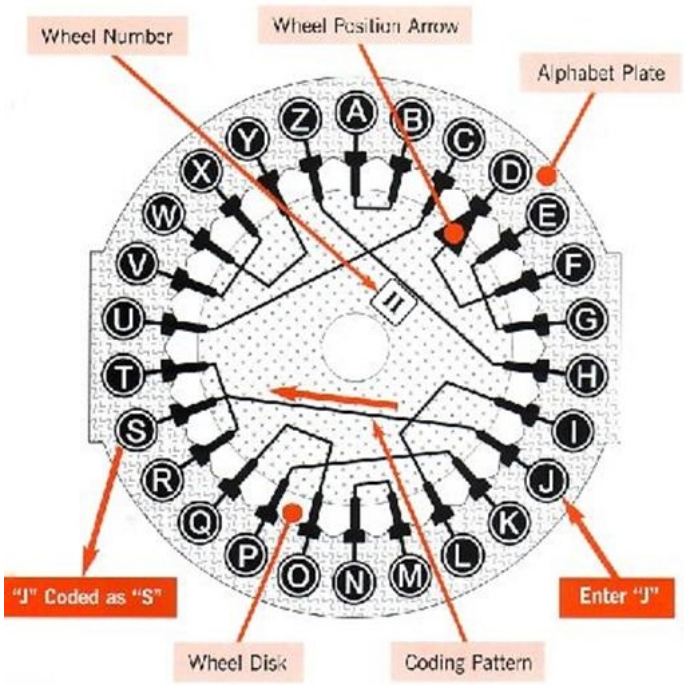
Enigma: funzionamento

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).



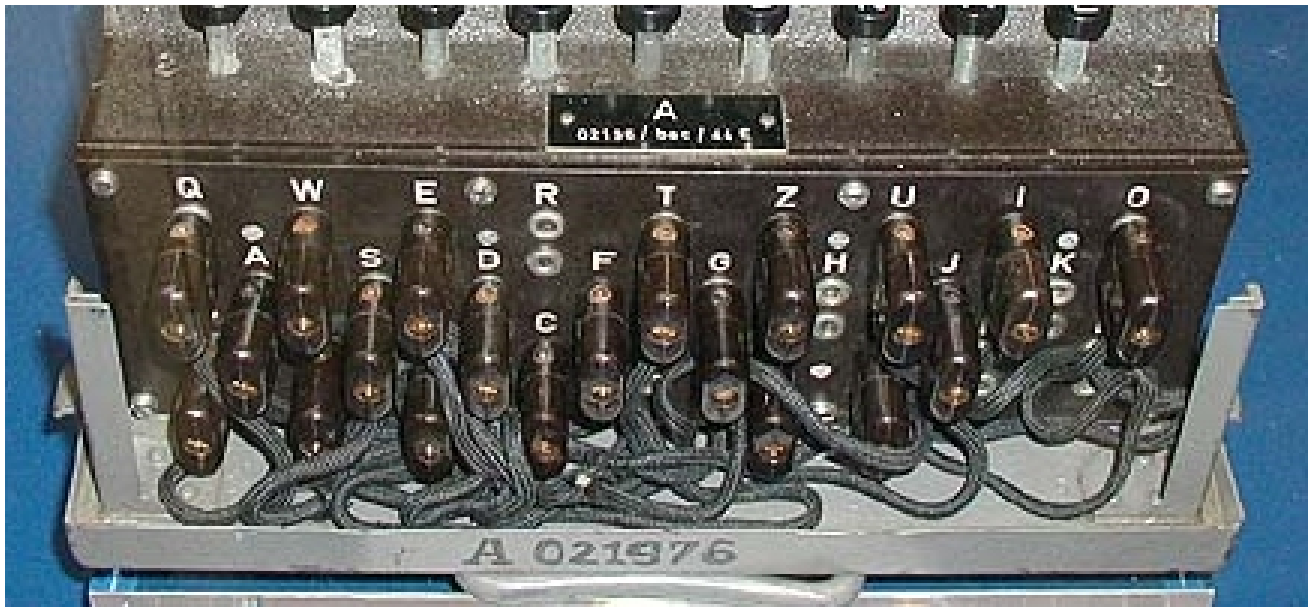
Ogni rotore ha 26 contatti su una faccia e 26 sull'altra e implementa una sostituzione monoalfabetica (completa). Il reflector garantisce simmetria. Inoltre (brevetto) mai una lettera era codificata in sè stessa.

Enigma: funzionamento



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).

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:

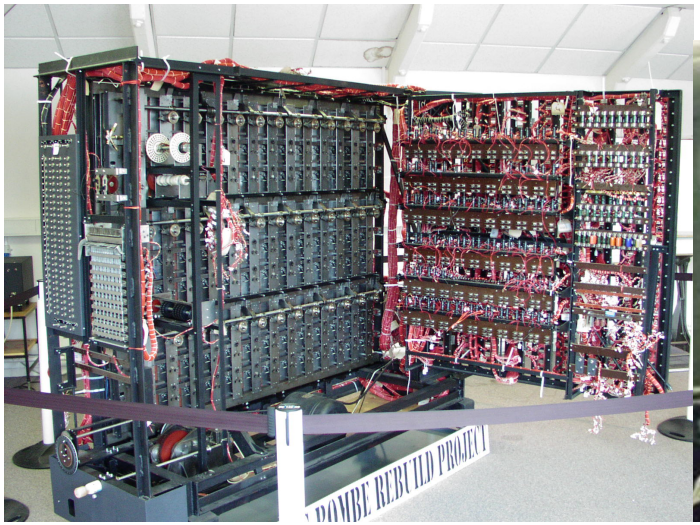
$$\binom{26}{2k} \frac{\binom{2k}{2}\binom{2k-2}{2}\cdots\binom{2}{2}}{k!}$$

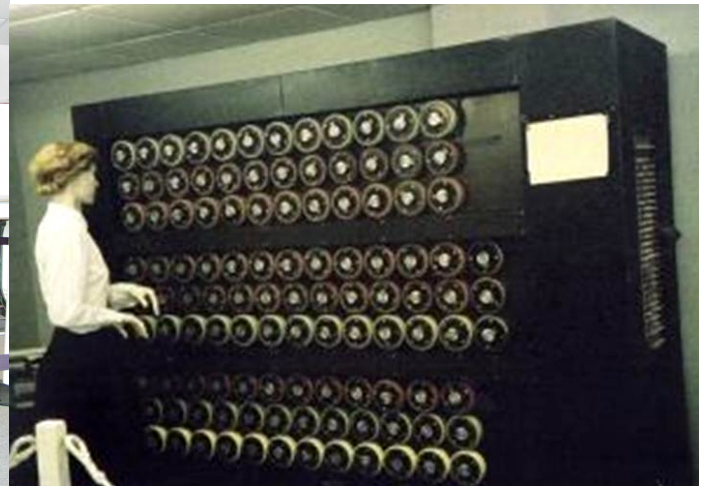
Enigma: attacco

- 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.

ENIGMA: ATTACCO

Nel 1940 fu costruita la prima Bombe





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

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).

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.

Enigma: (poche) debolezze

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

A	B	C	D	E	F	$\ldots$
Q	W	E	R	T	Y	$\ldots$
E	N	I	G	M	A	$\ldots$
M	A	L	I	G	N	$\ldots$

- 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.

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.

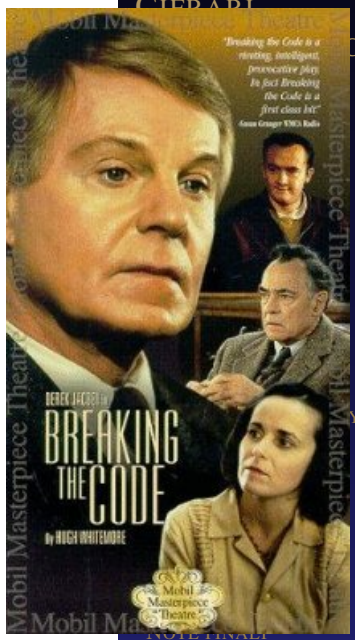
Enigma: (poche) debolezze

- 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.

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:**

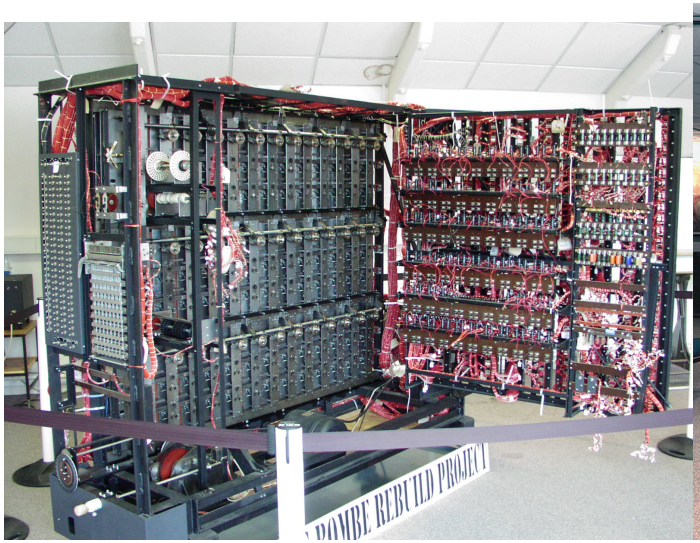
- M. Davis. *Il calcolatore universale*
- A. Hodges. *The Enigma* (da cui è tratto “The imitation game”)

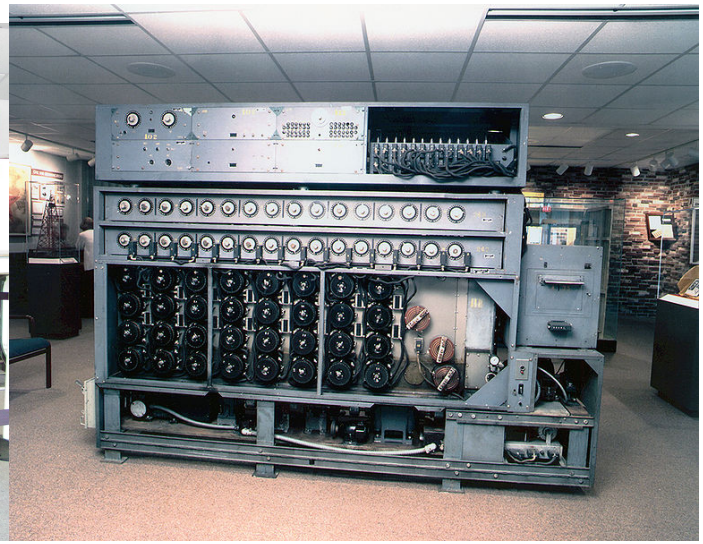
Romanzi:

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

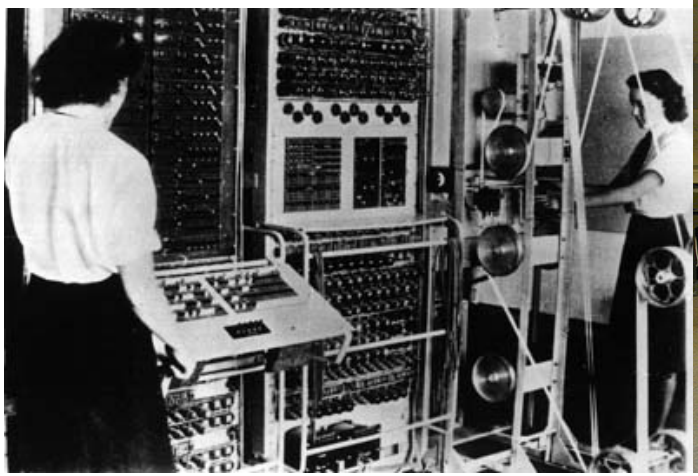
Oltre ovviamente ai contributi scientifici scritti da Turing reperibili da:
`http://www.turingarchive.org/`

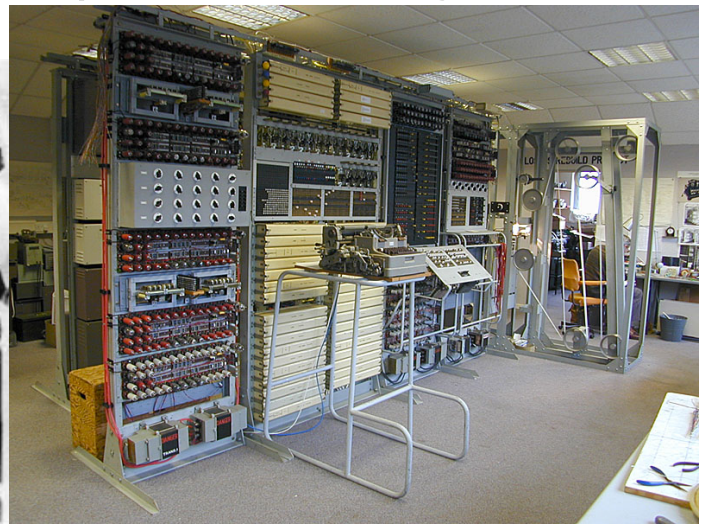
Nel 1940 fu costruita la prima Bombe





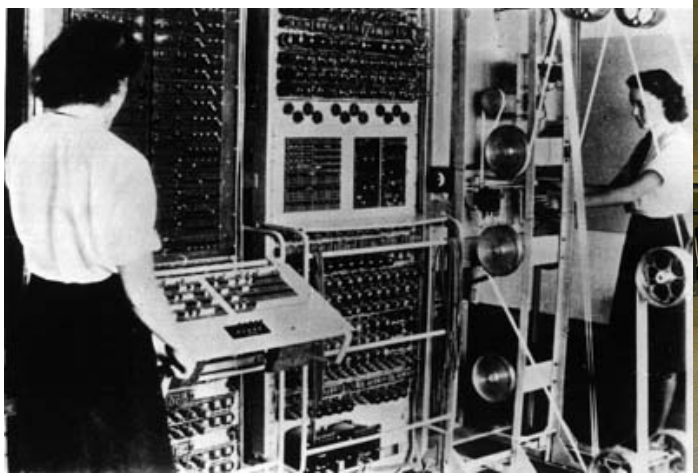
I tedeschi cambiarono metodologia di codifica con Enigma (e.g., uso di 4 rotori per i sommergibili).

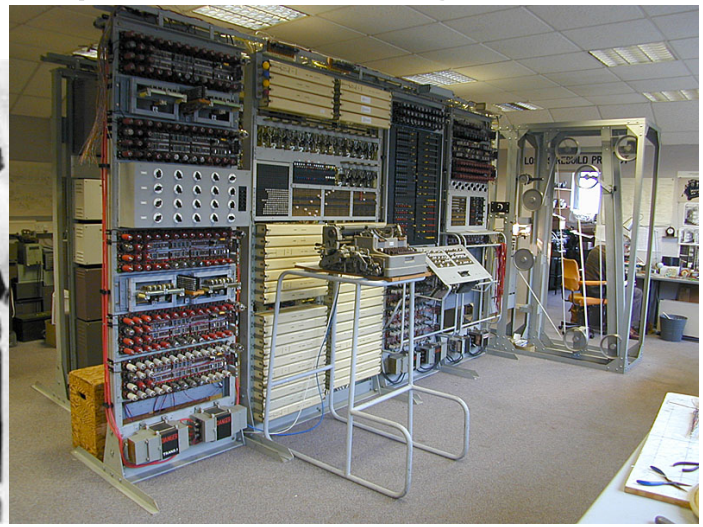




Furono costruiti i colossi.

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





Furono costruiti i colossi.

- 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.

- 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.