Turing a Bletchley Park: attacco all'Enigma

Agostino Dovier

Dip di Matematica e Informatica, Univ. di Udine

Ottobre 2012

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;

Turing . . .

Alan Mathison Turing 23/06/1912–07/06/1954

ATHLETICS

MARATHON AND DECATHLON CHAMPIONSHIPS

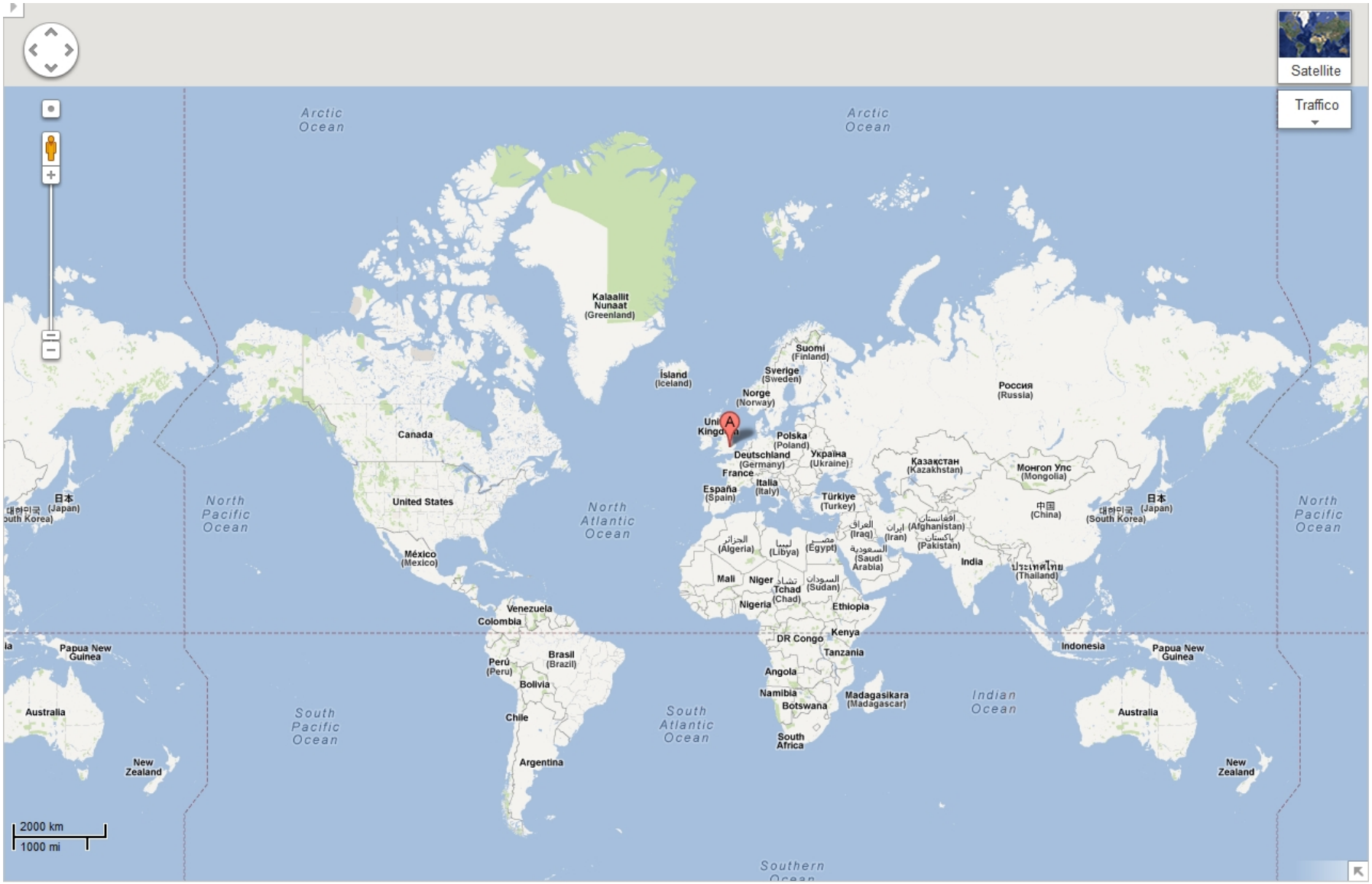
The Amateur Athletic Association championships for this year were concluded at Loughborough College Stadium, Leicestershire, on Saturday, with the second, and last, day of the Decathlon and the decision of the Marathon championship.

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.

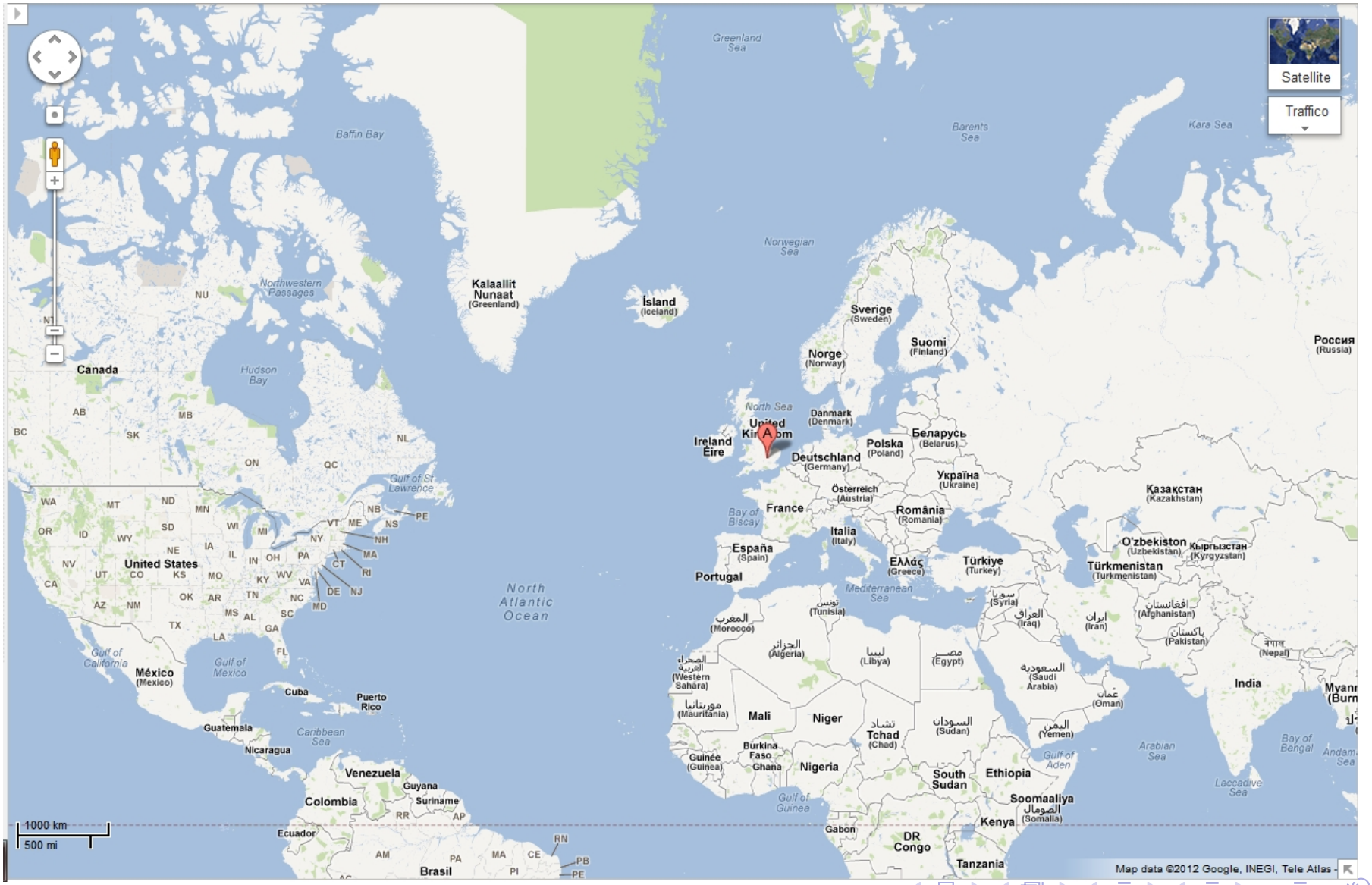
DECATHLON CHAMPIONSHIP.—H. J. Moesgaard-Kjeldsen (Polytechnic Harriers, London), 5,965 points, 1; Captain H. Whittle (Army and Reading A.C.), 5,650, 2;

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

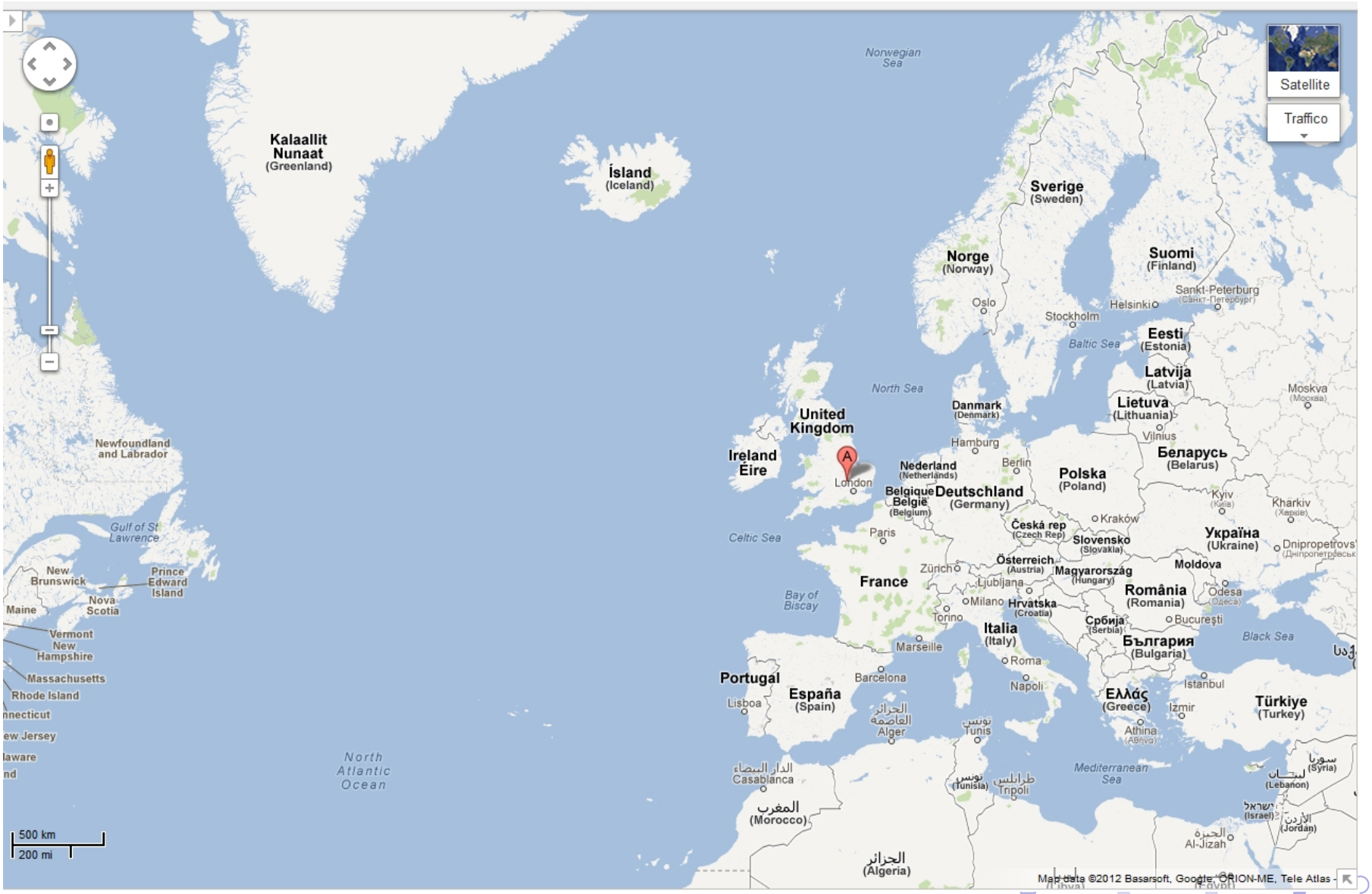
. . . a Bletchley Park



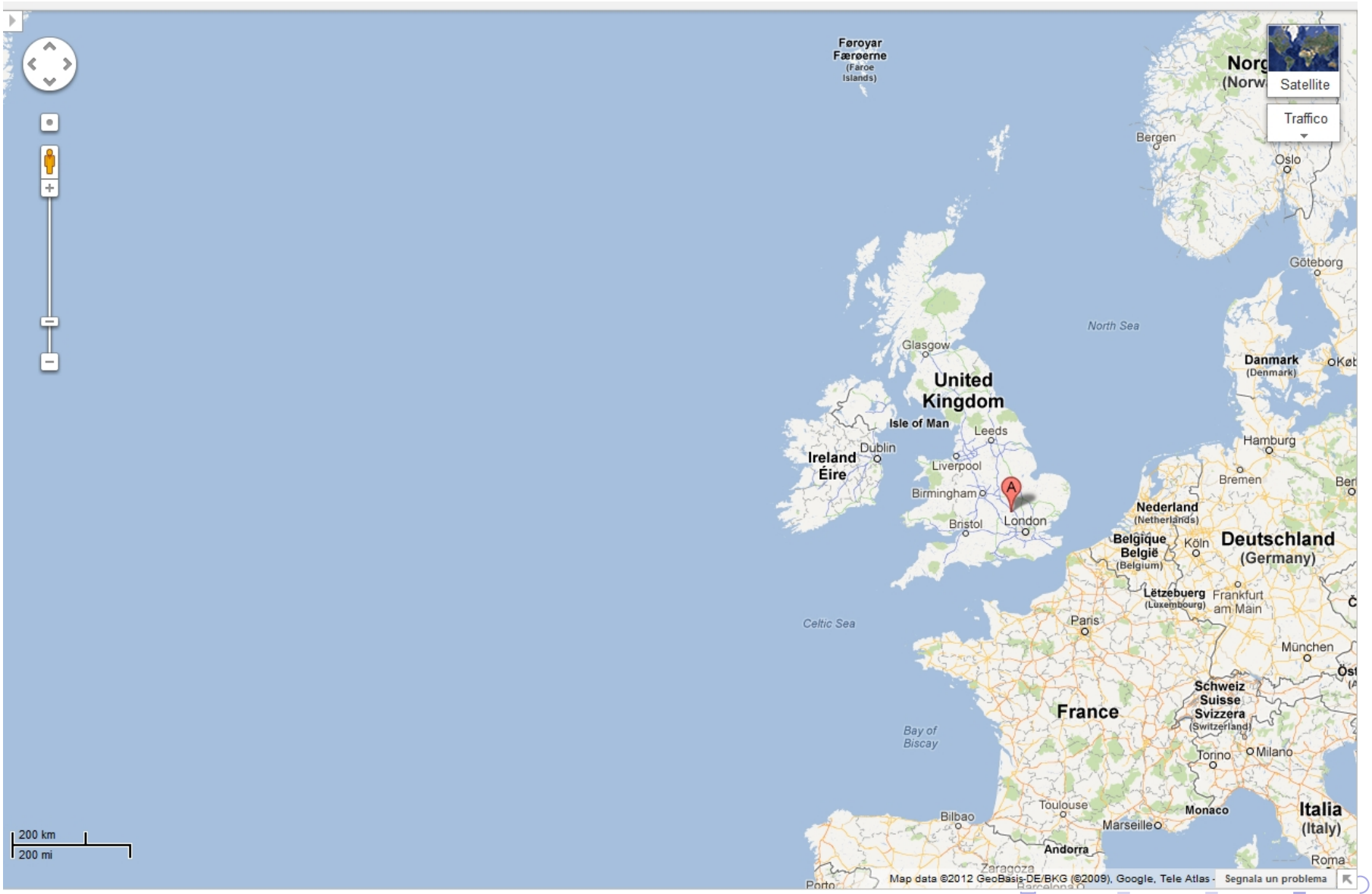
. . . a Bletchley Park



. . . a Bletchley Park



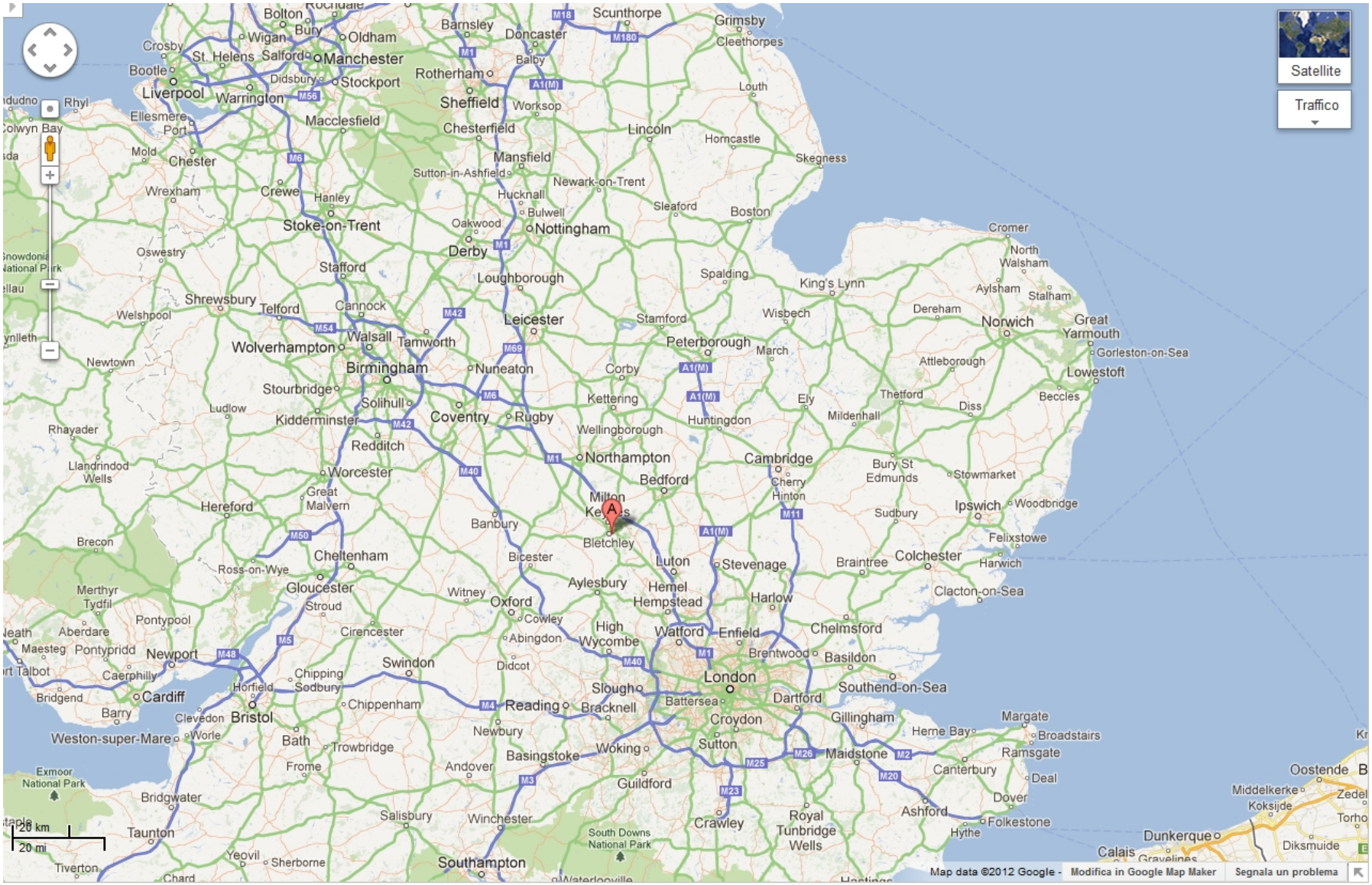
. . . a Bletchley Park



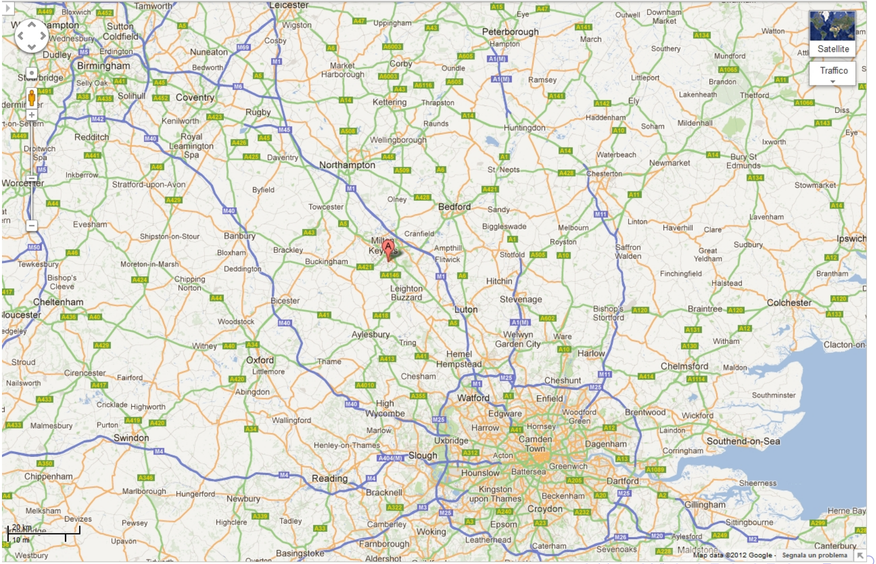
. . . a Bletchley Park

. . . a Bletchley Park

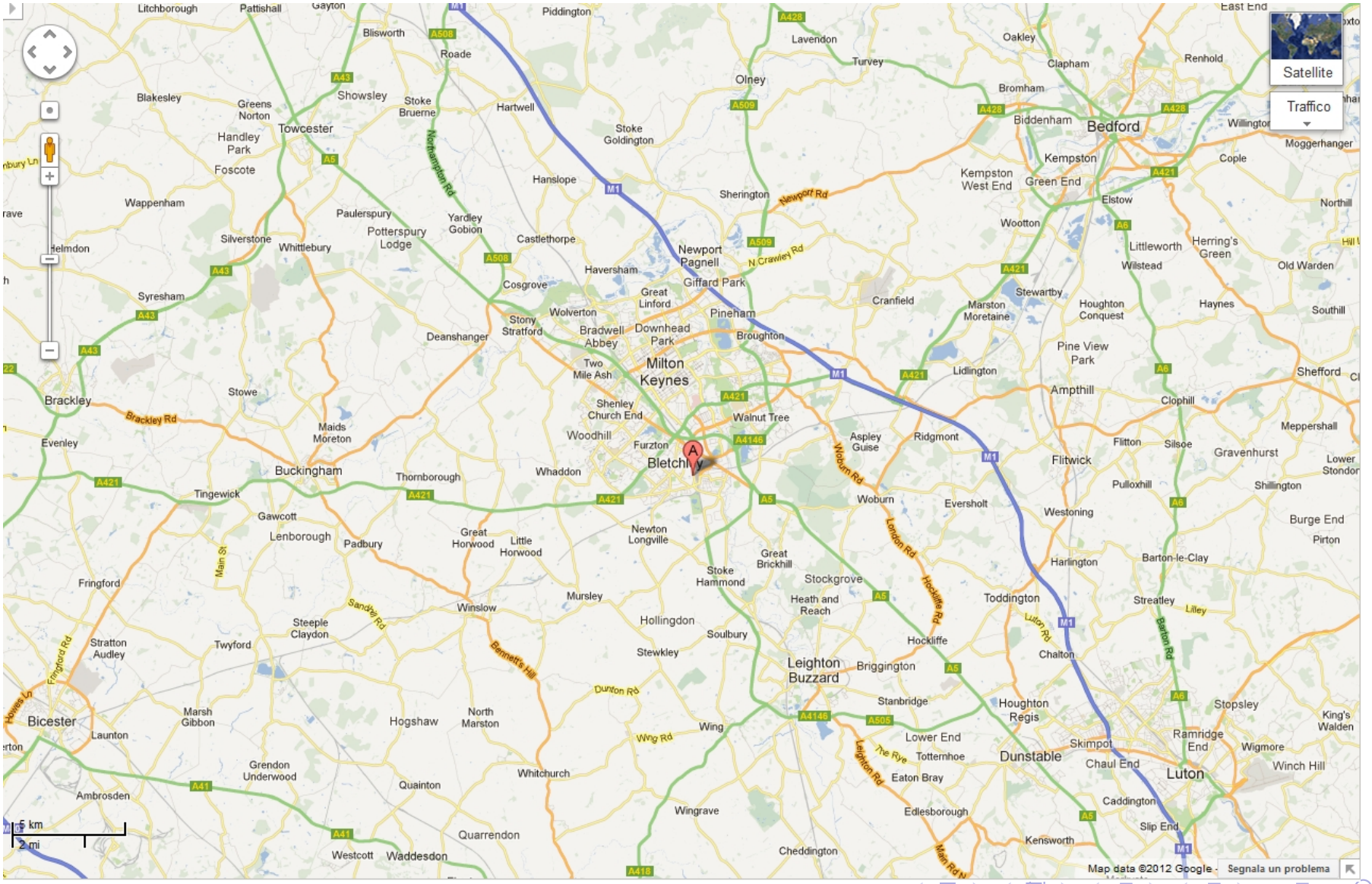
. . . a Bletchley Park



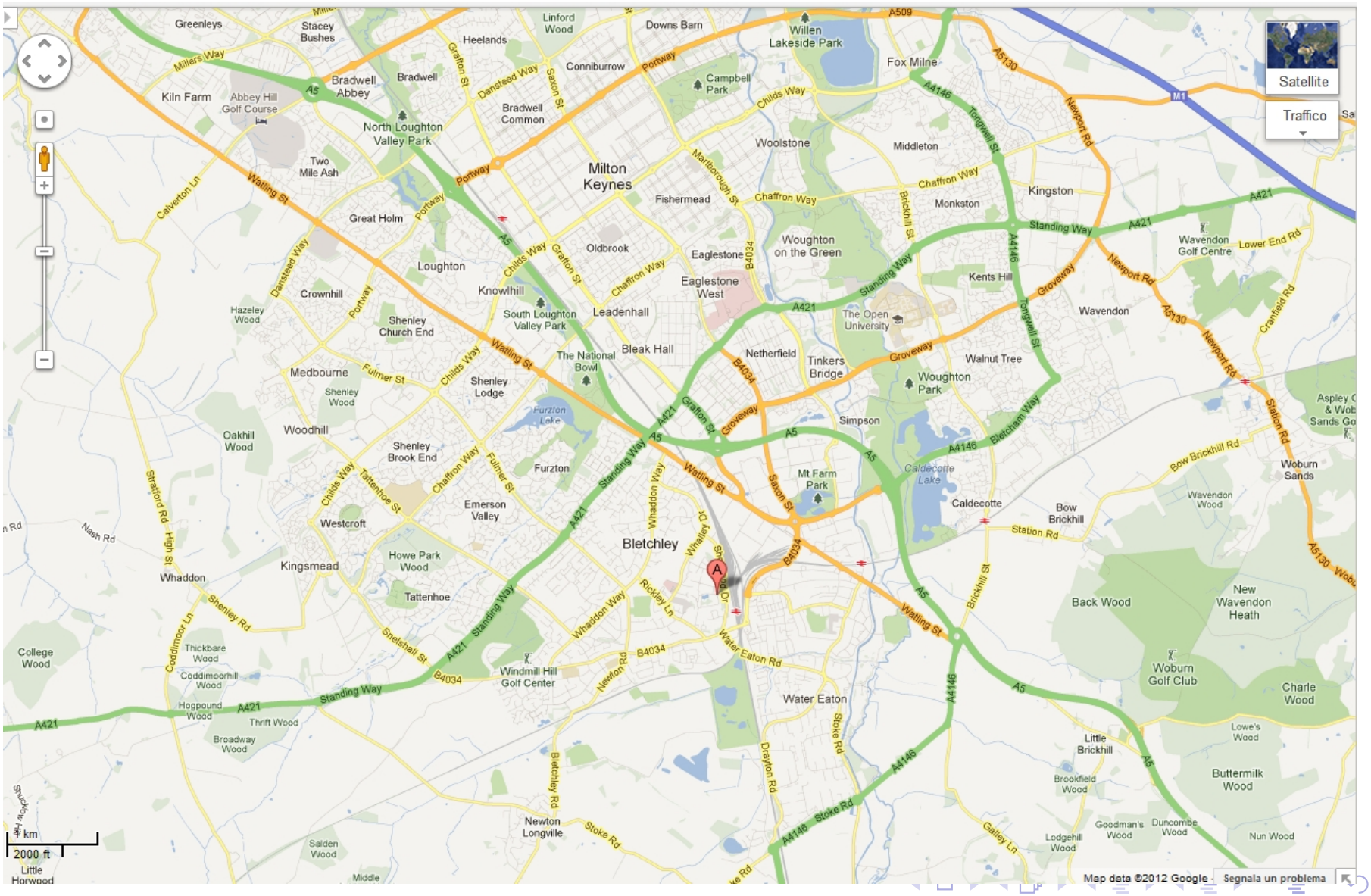
. . . a Bletchley Park



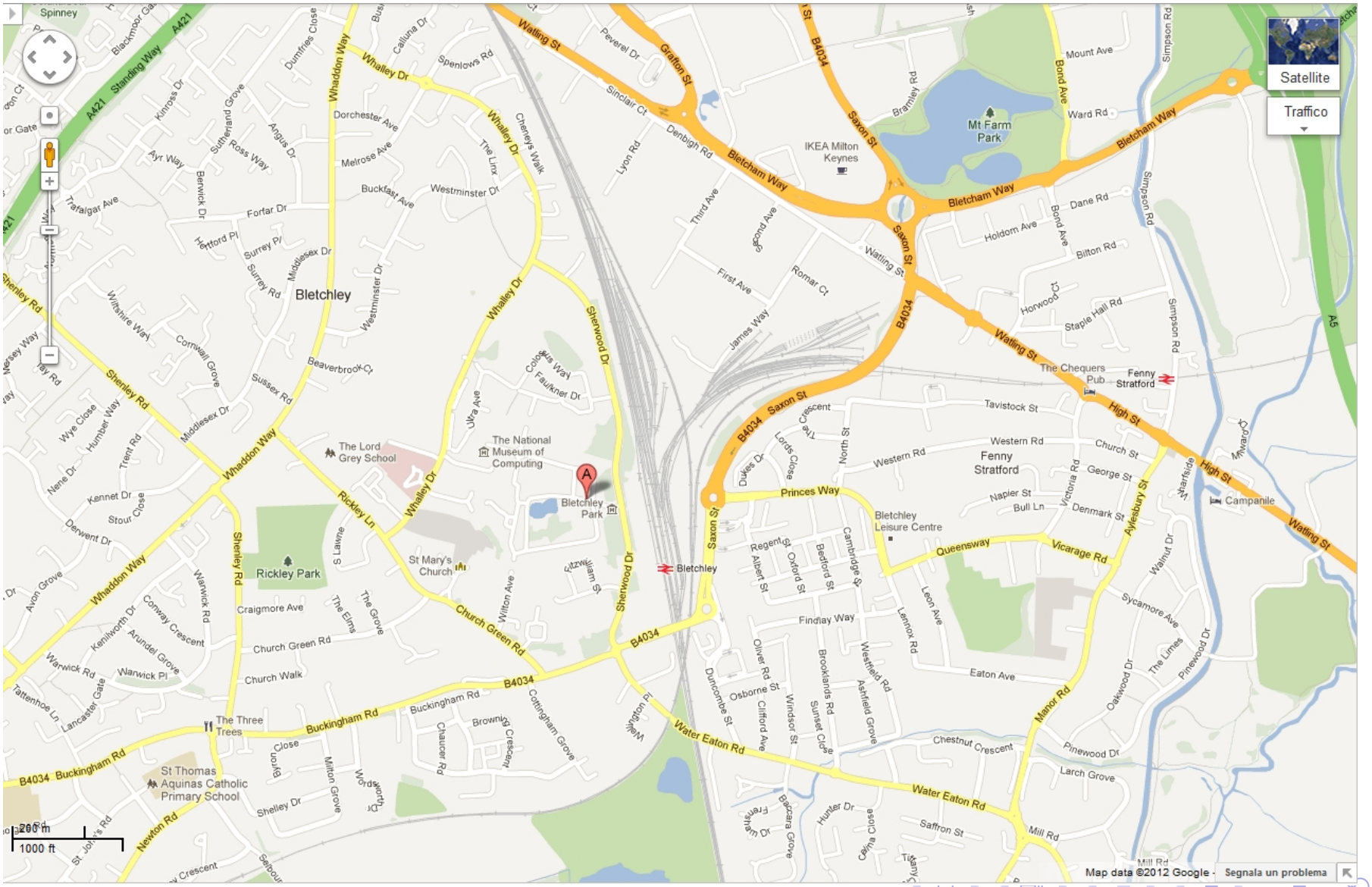
. . . a Bletchley Park



. . . a Bletchley Park



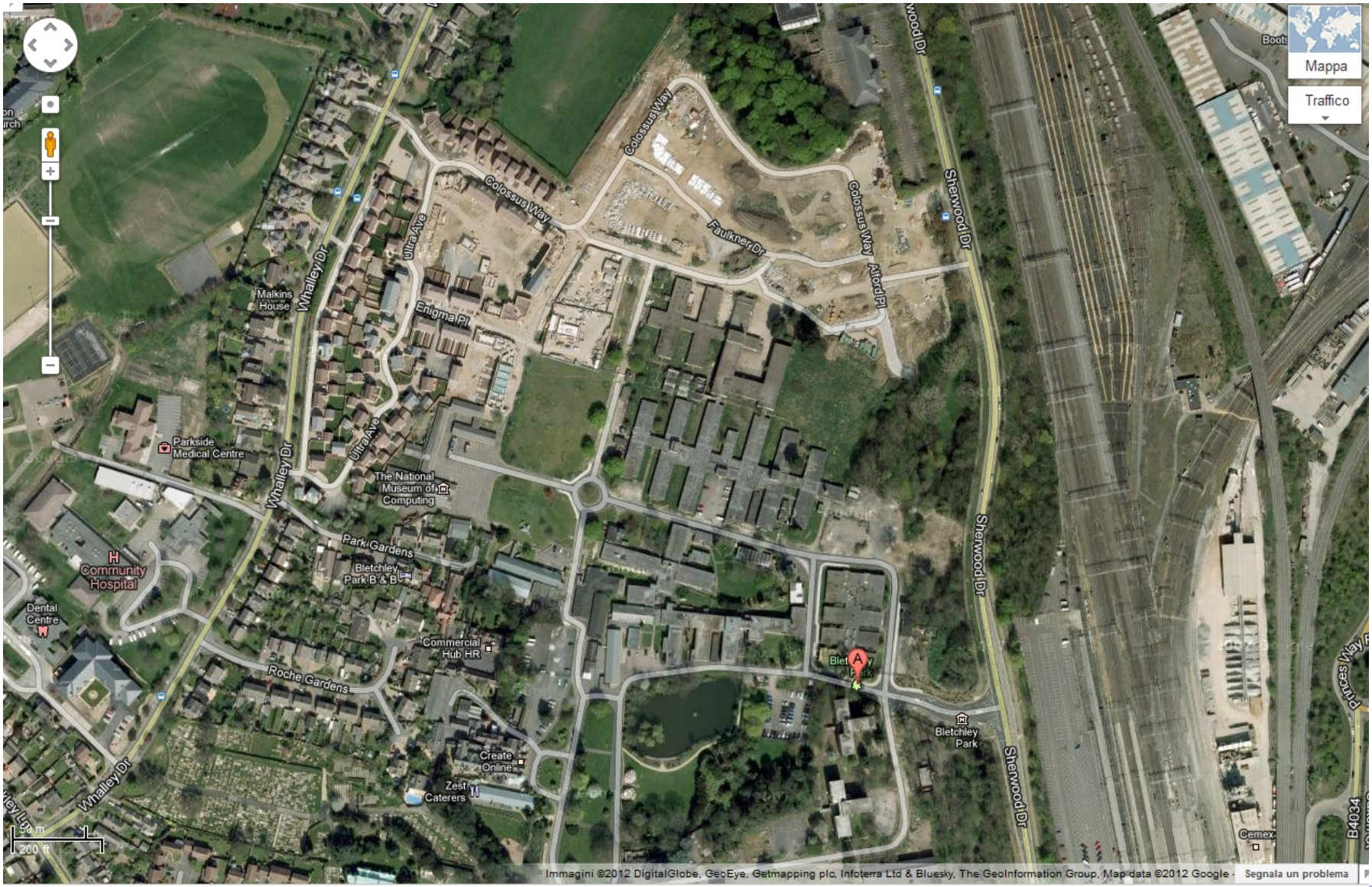
. . . a Bletchley Park



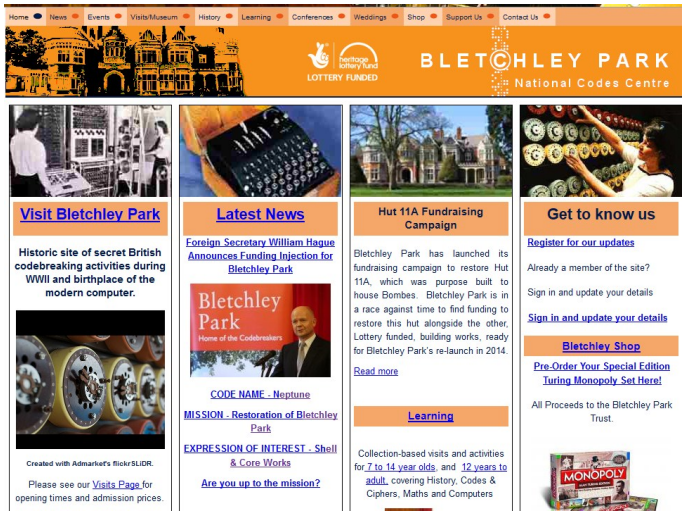
. . . a Bletchley Park

. . . a Bletchley Park

. . . a Bletchley Park

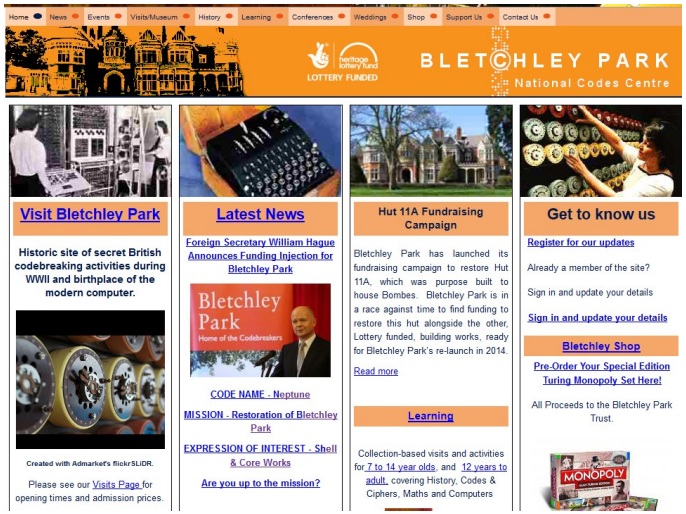


. . . a Bletchley Park



"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.

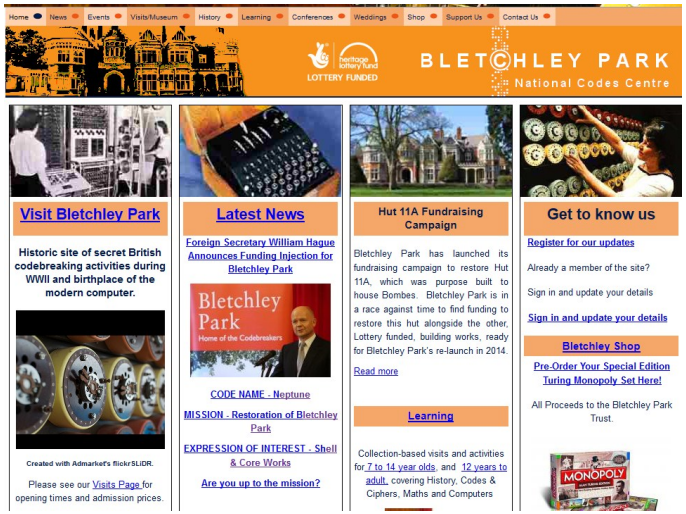
. . . a Bletchley Park



"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)

. . . 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.

Cifrari a sostituzione monoalfabetica

Giulio Cesare (100–44 AC)

M A L I G N A N I
P D O M K Q D Q M

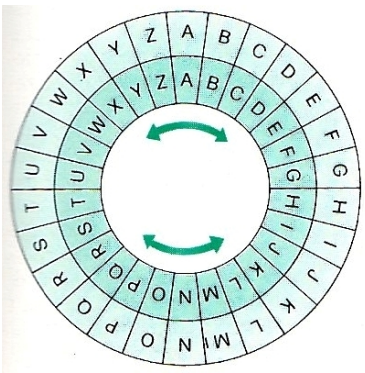
A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	A	B	C

Cifrari a sostituzione monoalfabetica

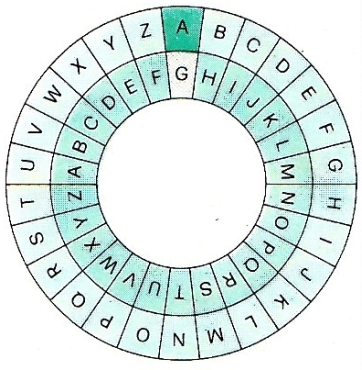
- La “chiave” segreta è la lettera iniziale (la D per Cesare).
- Sapendo il tipo di codifica usata (Principio di Kerchoofs), il crittanalista (la spia) deve indovinare la chiave.
- Ci sono una ventina di chiavi: il codice è troppo debole.

Cifrari a sostituzione monoalfabetica

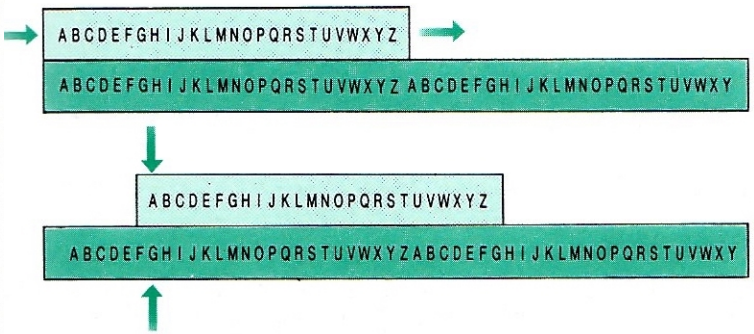
Macchine di cifra



L.B. Alberti
(1404–1472)



G.B. Della Porta
(1535–1615)



Regolo di Saint Cyr
(fine 800)

Cifrari a sostituzione monoalfabetica

Cifrari completi

- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
M	V	F	T	H	C	K	L	D	N	O	P	Q	R	A	G	E	X	S	B	I

- Le funzioni possibili diventano $21! \approx 5 \cdot 10^{19}$ (in realtà un po' meno ... non vogliamo troppe identità...) La chiave è l'intera sostituzione.

Cifrari a sostituzione monoalfabetica

Cifrari completi

- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
M	V	F	T	H	C	K	L	D	N	O	P	Q	R	A	G	E	X	S	B	I

- Le funzioni possibili diventano $21! \approx 5 \cdot 10^{19}$ (in realtà un po' meno ... non vogliamo troppe identità...) La chiave è l'intera sostituzione.
- Cominciano a diventare numeri pesanti per la forza bruta.

Cifrari a sostituzione monoalfabetica

Cifrari completi

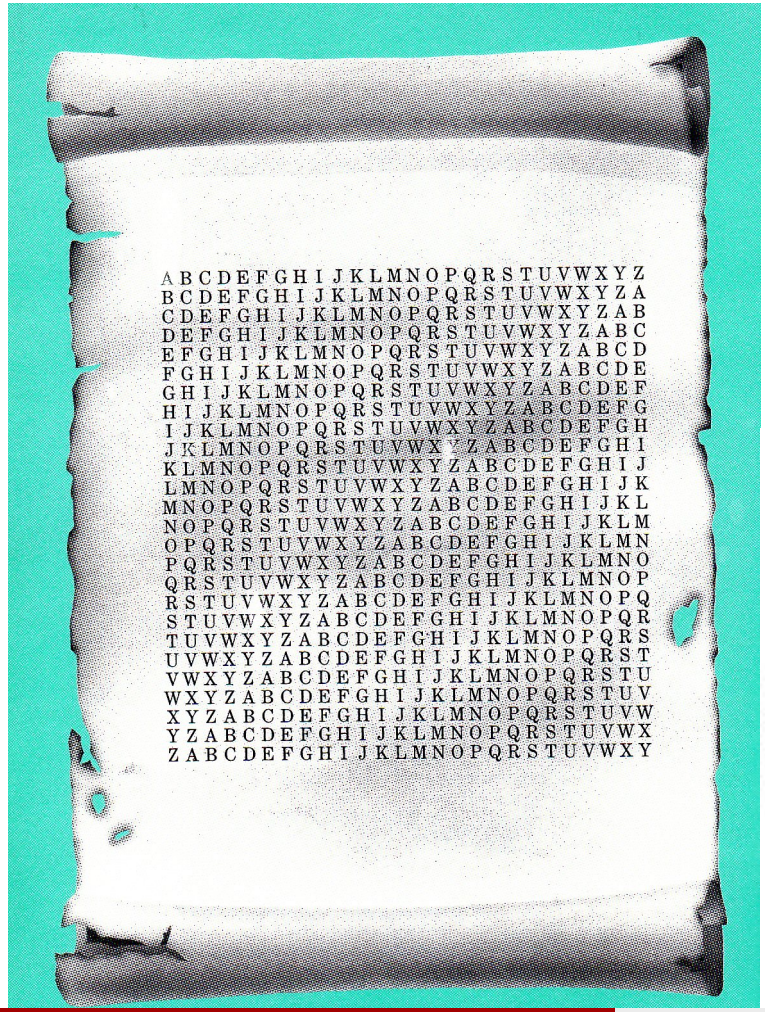
- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
M	V	F	T	H	C	K	L	D	N	O	P	Q	R	A	G	E	X	S	B	I

- Le funzioni possibili diventano $21! \approx 5 \cdot 10^{19}$ (in realtà un po' meno ... non vogliamo troppe identità...) La chiave è l'intera sostituzione.
- Cominciano a diventare numeri pesanti per la forza bruta.
- Viene usata la statistica. In una data lingua le lettere assumono una frequenza tipica. Il codice si forza a partire da questa informazione aggiuntiva.

Cifrari a sostituzione polialfabetica

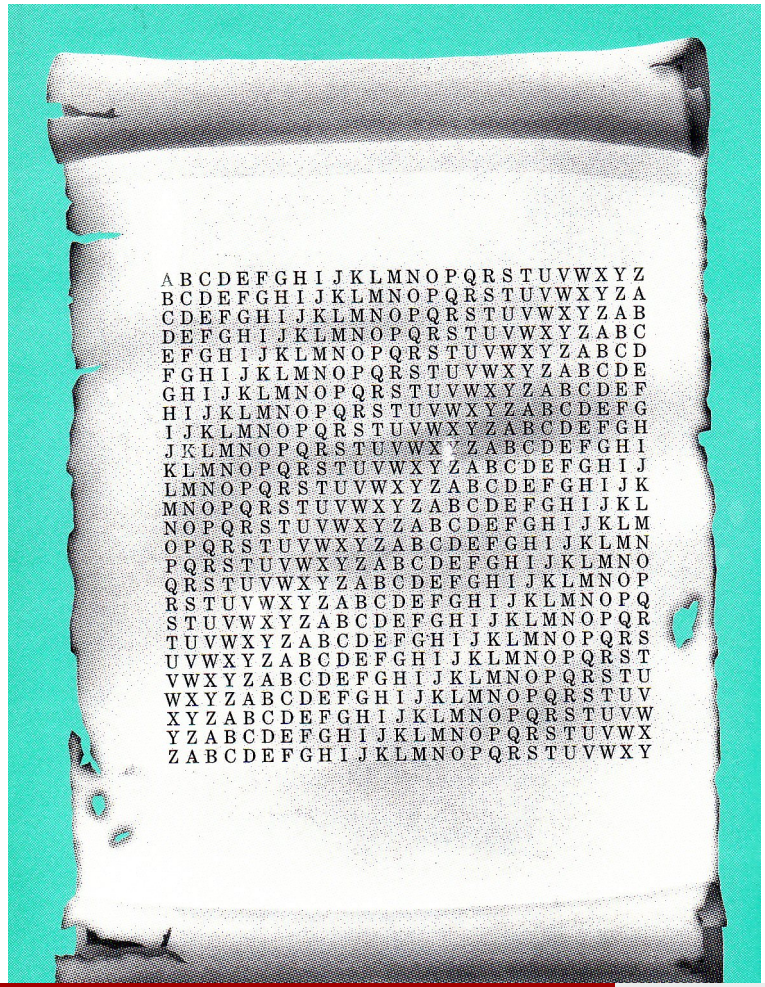
Blaise de Vigenère (1523–1596)



Cifrari a sostituzione polialfabetica

Cifrazione

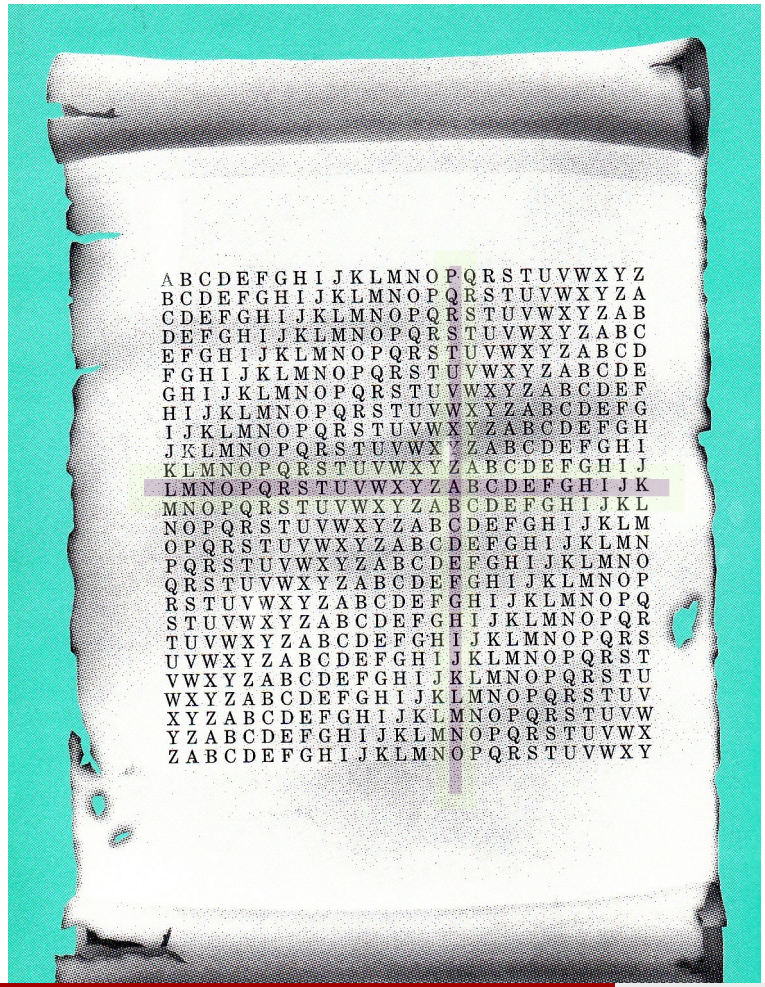
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

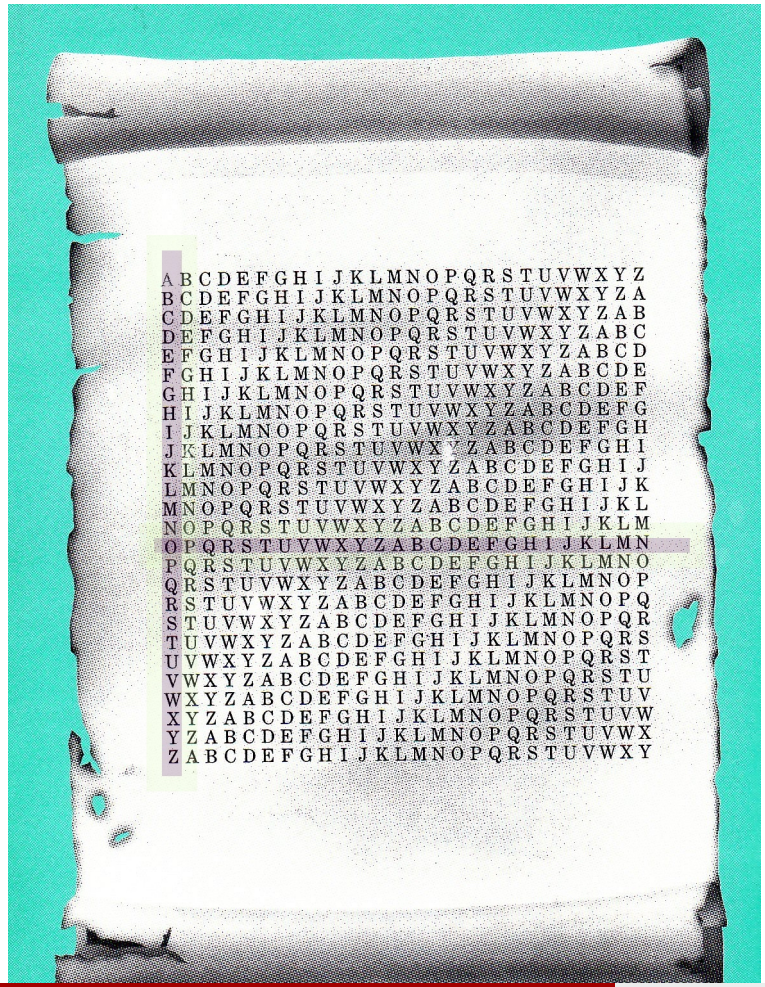
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

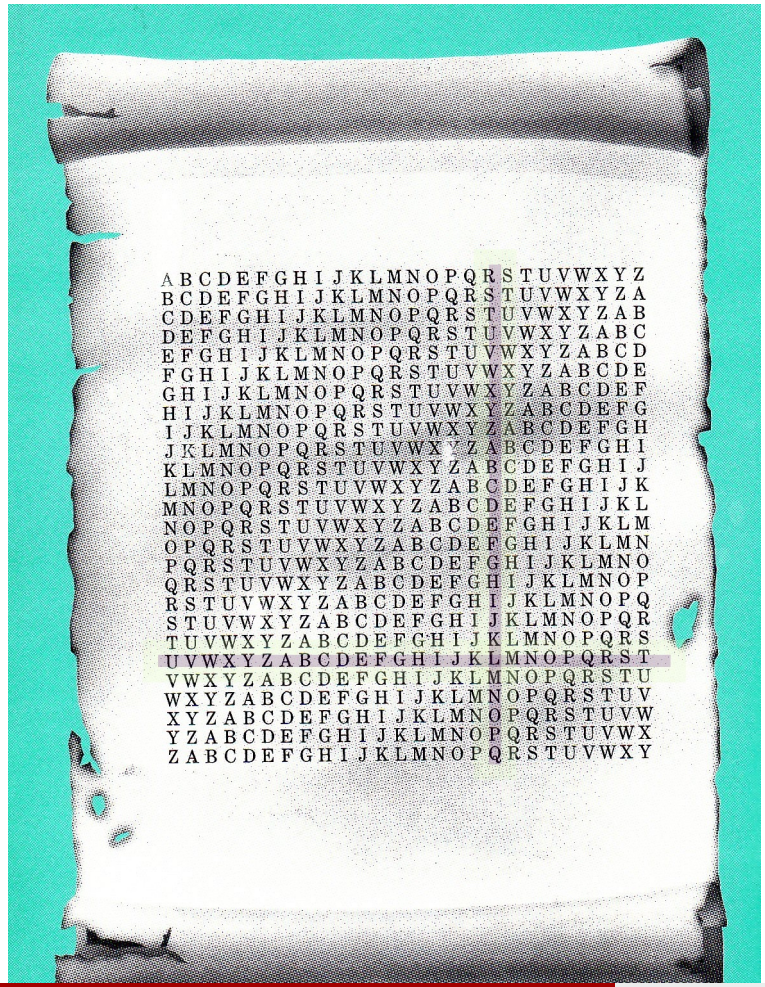
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

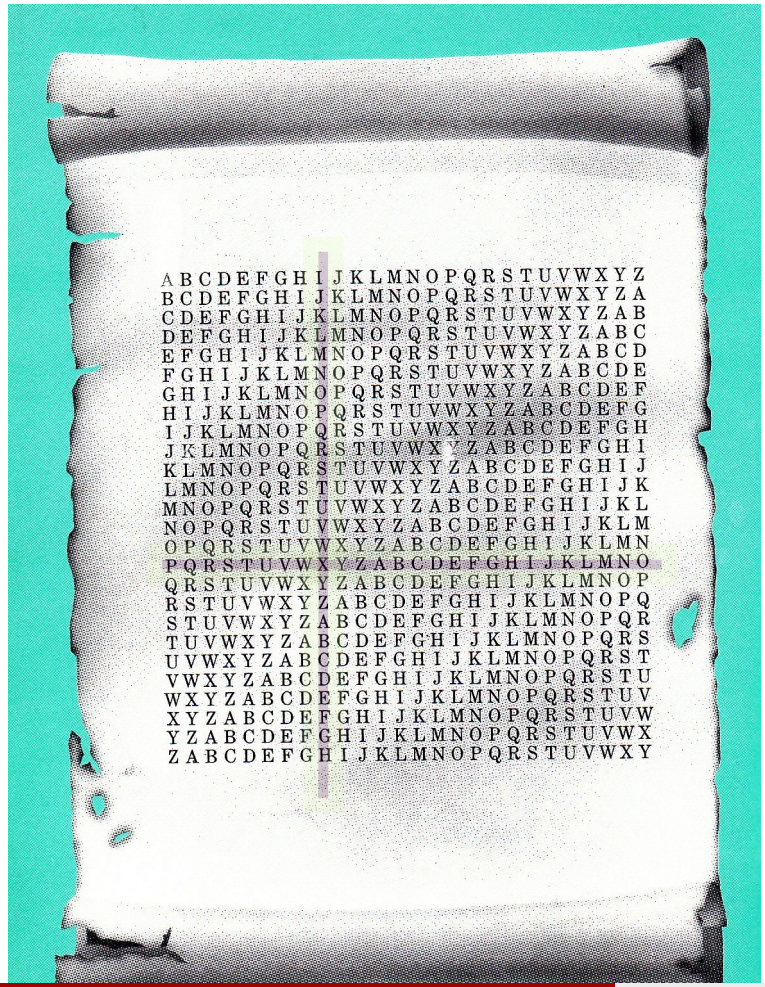
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

- È come se ci fossero più cifrari monoalfabetici del tipo di Cesare, tanti quanti la lunghezza della chiave.
- Se la chiave è lunga n, in fondo è come avere una funzione biiettiva

$$f : \{A, \ldots, Z\}^n \longrightarrow \{A, \ldots, Z\}^n$$

- Anche se su ogni lettera della chiave ci sono solo 21 scelte, in tutto ce ne sono ben 21^n.
- Inoltre la statistica sembra ingannata.
- E la spia non conosce nemmeno n.

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

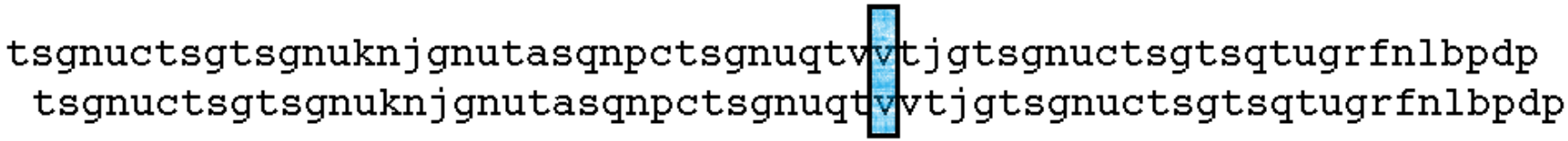
Cifrari a sostituzione polialfabetica

Decrittazione

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Cifrari a sostituzione polialfabetica

Decrittazione



Cifrari a sostituzione polialfabetica

Decrittazione

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
  tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

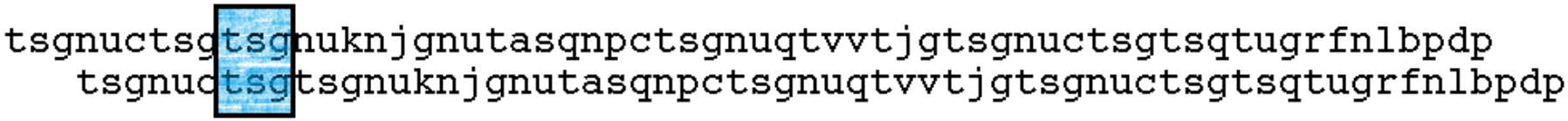
Cifrari a sostituzione polialfabetica

Decrittazione

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
   tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

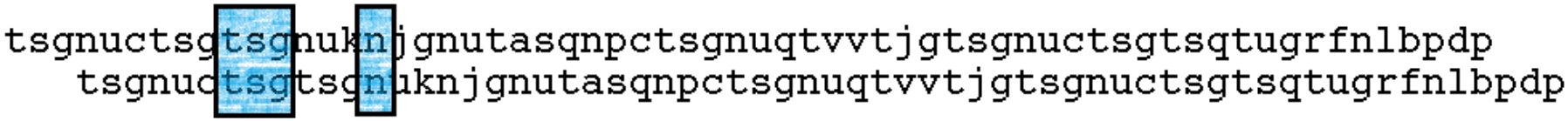
Cifrari a sostituzione polialfabetica

Decrittazione



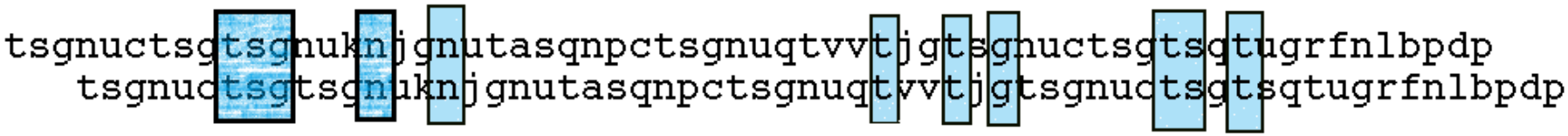
Cifrari a sostituzione polialfabetica

Decrittazione



Cifrari a sostituzione polialfabetica

Decrittazione



Cifrari a sostituzione polialfabetica

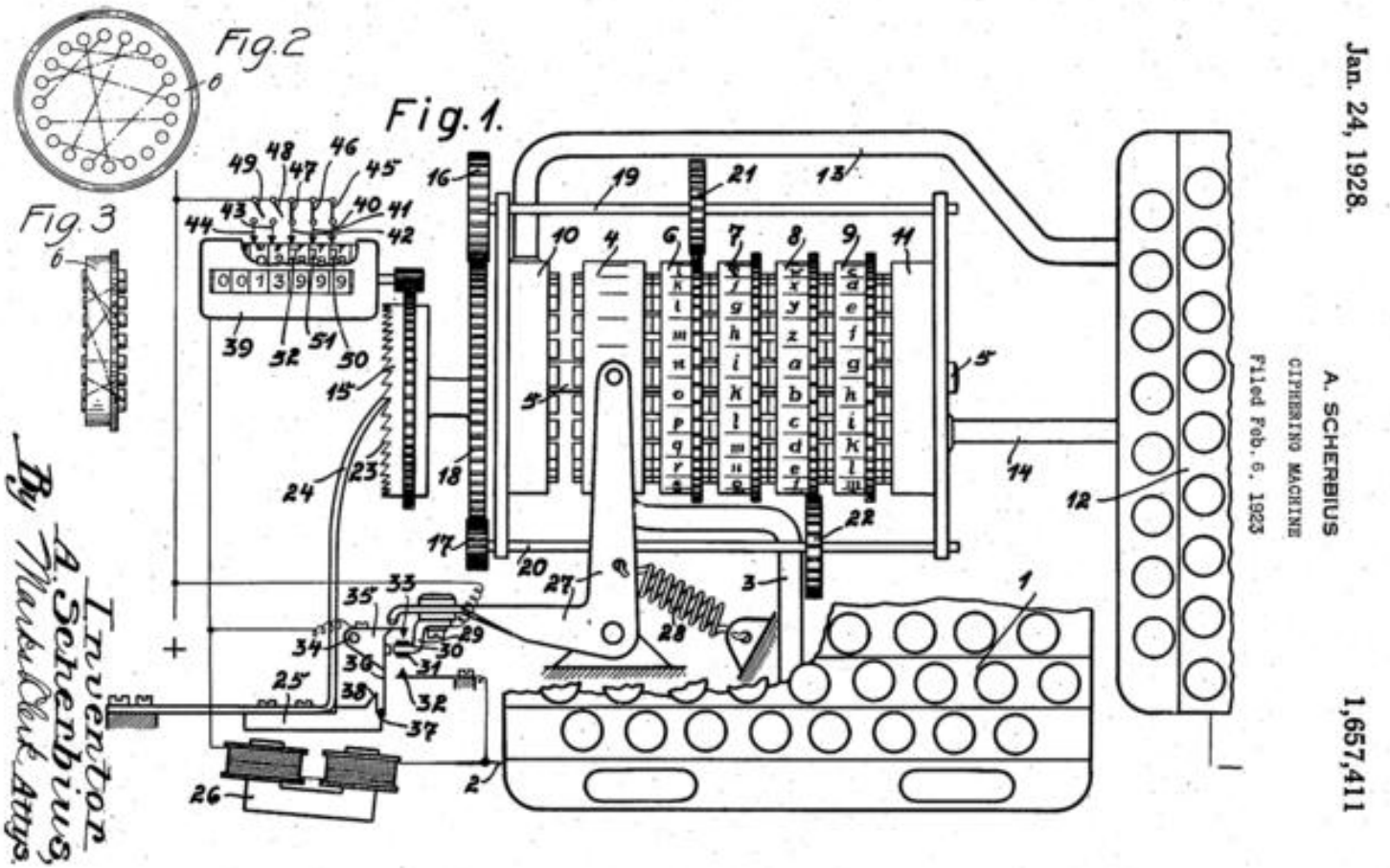
Decrittazione e limiti

1. Con l'allineamento visto, si determina la lunghezza della parola chiave.
2. Congetturata la lunghezza, si partiziona il testo in n sottotesti e si cercano le n chiavi con la la statistica.
3. La cifratura polialfabetica non è praticamente decifrabile se la parola chiave è lunga quanto il testo (e non viene più utilizzata per alti testi). Se inoltre non ha senso compiuto (è scelta lanciando una moneta) diventa dimostrabilmente indecifrabile (cifrario perfetto Vernam)
4. In generale, se la chiave (il periodo) è molto lungo rispetto al testo la decodifica statistica non è effettiva.

Enigma

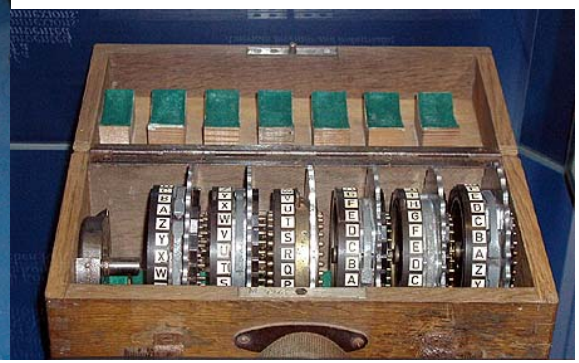
Arthur Scherbius (1878–1929)

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



Enigma

Nel 1923 Scherbius commercializza l'Enigma.

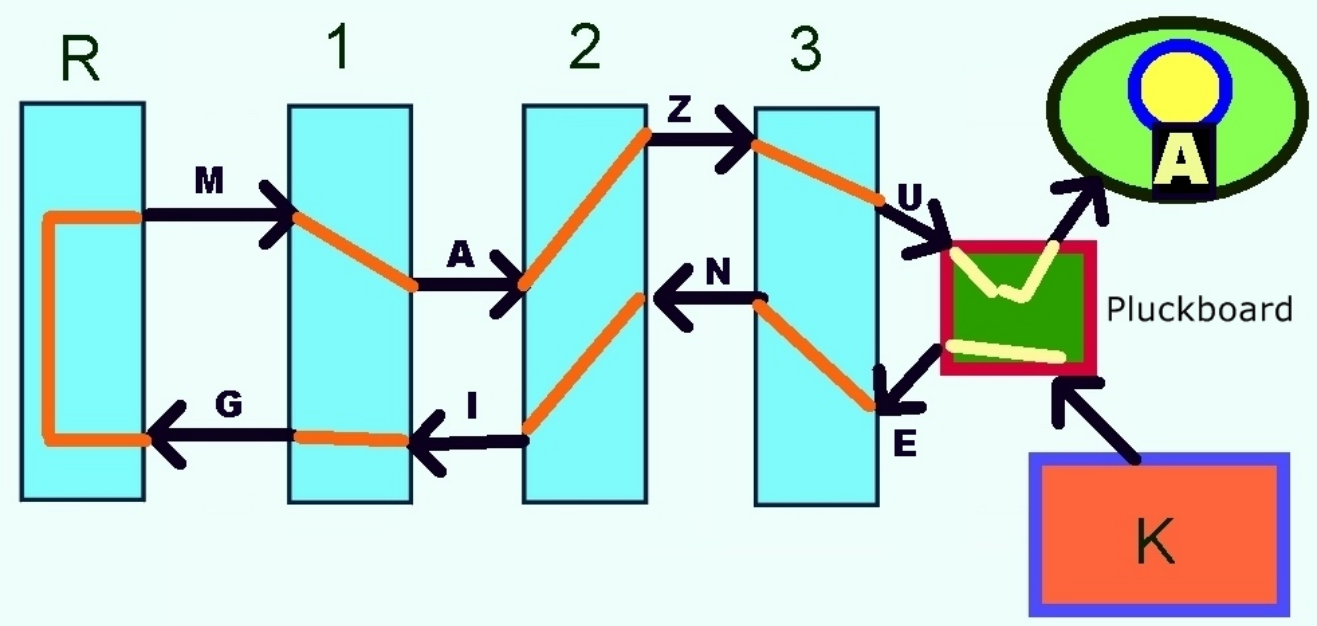


Enigma: funzionamento

- 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

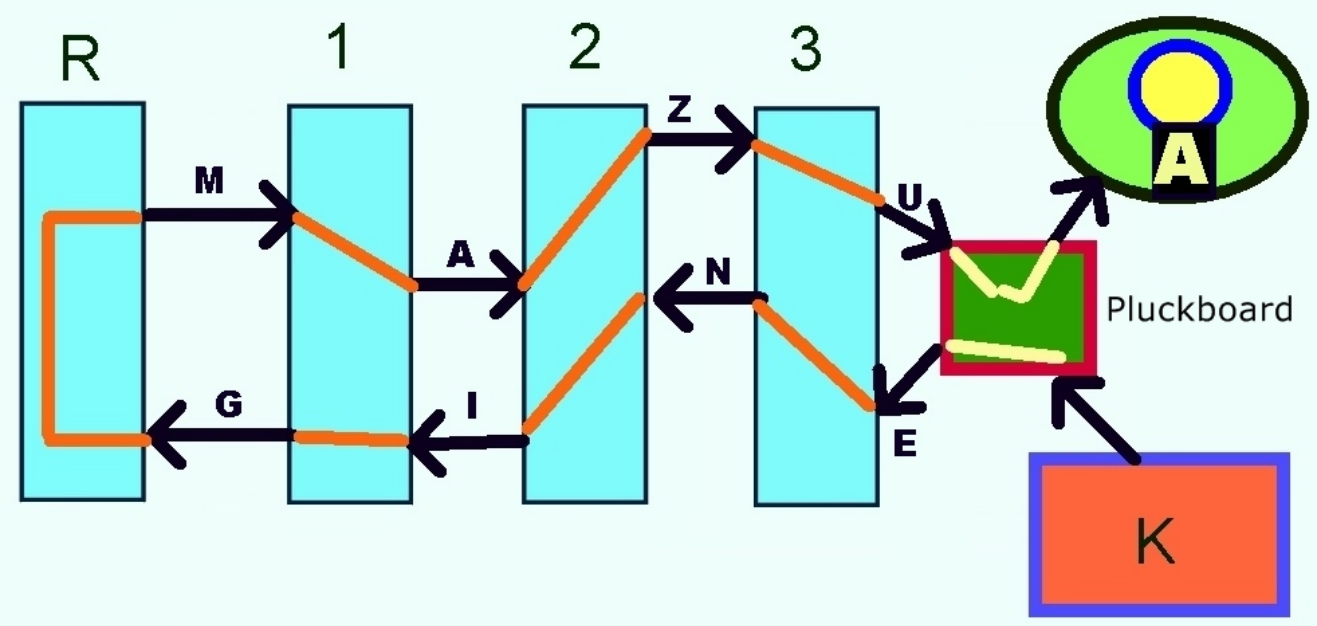
Si tratta di una macchina a rotori non fissi che si muovono con moto odometrico dopo ogni lettera codificata—stepping motion (come i vecchi contachilometri o i contatori dell'acqua o del gas).



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

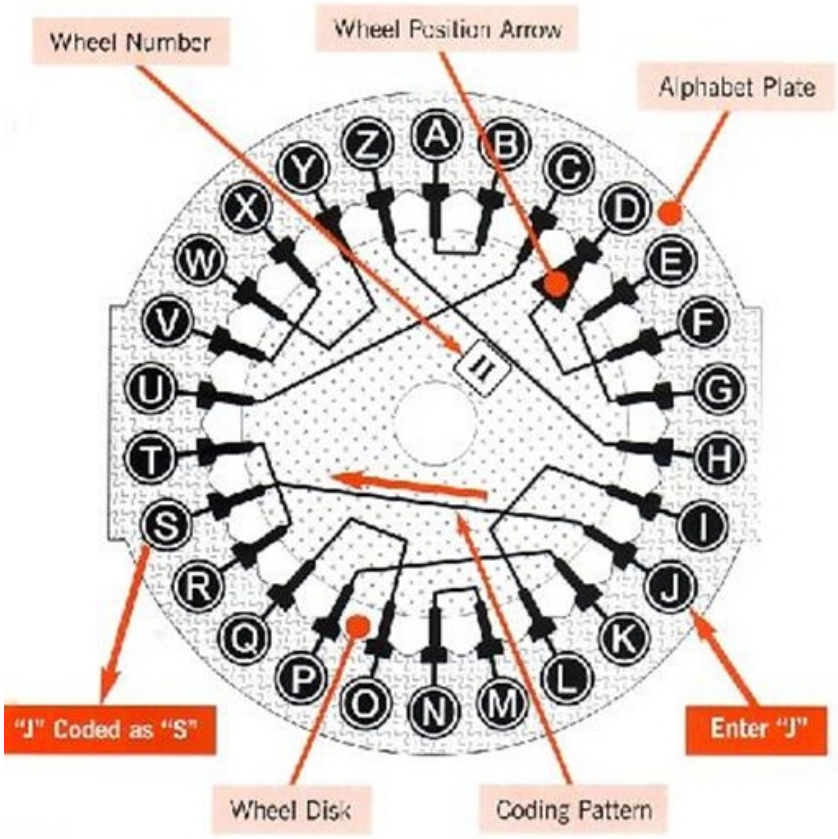
Enigma: funzionamento

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:

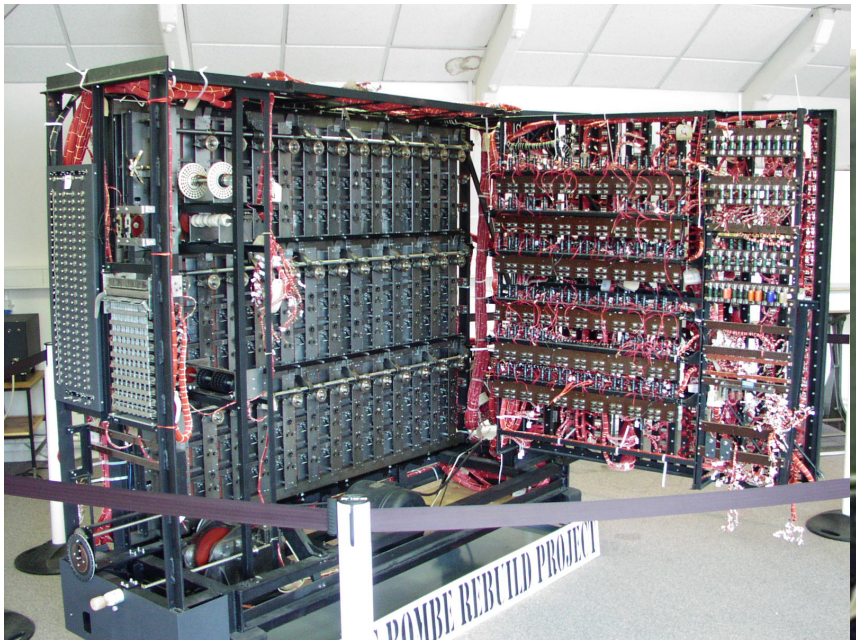
$$\binom{26}{2k} \frac{\binom{2k}{2}\binom{2k-2}{2}\cdots\binom{2}{2}}{k!}$$

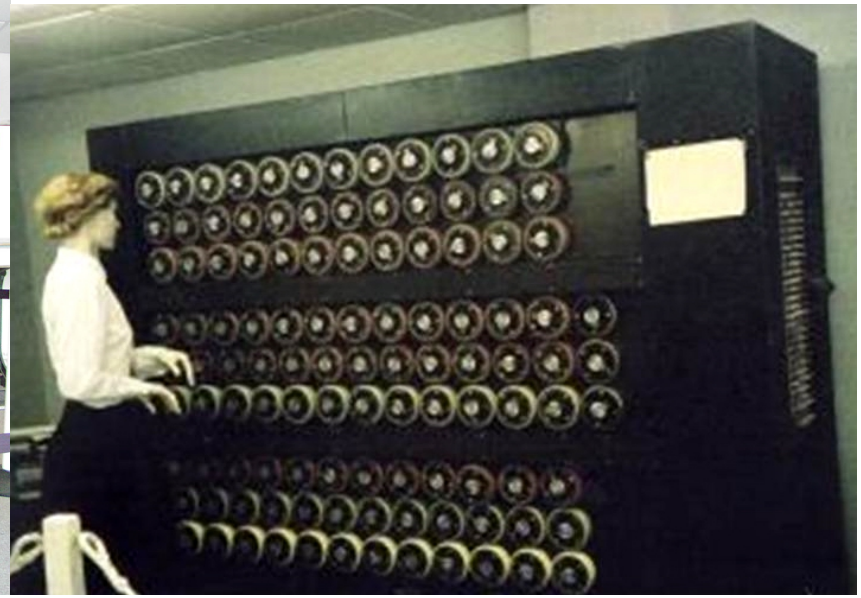
Enigma: attacco

- 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:

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

- 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.

Enigma: (poche) debolezze

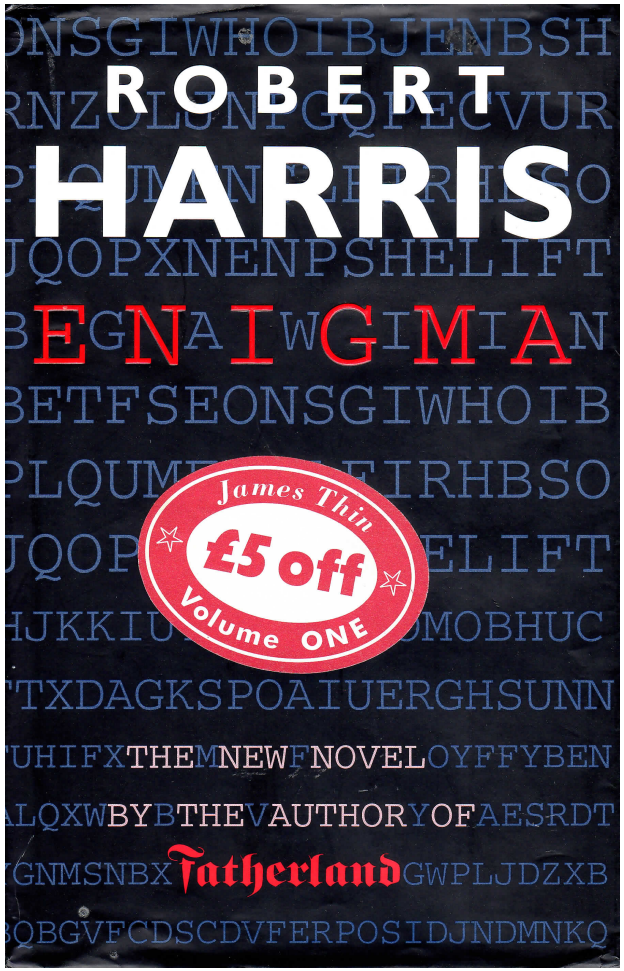
- Rejewski et al. realizzarono (a mano) un catalogo di 105456 settings iniziali e i corrispondenti parametri quali lunghezza ciclo di permutazioni.
- Alla fine degli anni '30 le comunicarono agli inglesi.

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.

Robert Harris

ENIGMA (1995)



Robert Harris

ENIGMA (1995)

The staircase was just as he remembered it, except that now this wing of the college was closed and the wind had blown dead leaves into the well of the steps. An old newspaper curled itself around his legs like a hungry cat. He tried the light switch. It clicked uselessly. There was no bulb. But he could still make out the name, one of three painted on a wooden board in elegant white capitals, now cracked and faded.

TURING, A.M.

How nervously he had climbed these stairs for the first time – when? in the summer of 1938? a world ago – to find a man barely five years older than himself, as shy as a freshman, with a hank of dark hair falling across his eyes: the great Alan Turing, the author of *On Computable Numbers*, the progenitor of the Universal Computing Machine …

Turing had asked him what he proposed to take as his subject for his first year's research.

'Riemann's theory of prime numbers.'

'But I am researching Riemann myself.'

10

Robert Harris

ENIGMA (1995)

The staircase was just as he remembered it, except that now this wing of the college was closed and the wind had blown dead leaves into the well of the steps. An old newspaper curled itself around his legs like a hungry cat. He tried the light switch. It clicked uselessly. There was no bulb. But he could still make out the name, one of three painted on a wooden board in elegant white capitals, now cracked and faded.

TURING, A.M.

How nervously he had climbed these stairs for the first time – when? in the summer of 1938? a world ago – to find a man barely five years older than himself, as shy as a freshman, with a hank of dark hair falling across his eyes: the great Alan Turing, the author of *On Computable Numbers*, the progenitor of the Universal Computing Machine …

Turing had asked him what he proposed to take as his subject for his first year's research.

'Riemann's theory of prime numbers.'

'But I am researching Riemann myself.'

10

Robert Harris

ENIGMA (1995)

'I know,' Jericho had blurted out, 'that's why I chose it.'

And Turing had laughed at this outrageous display of hero worship, and had agreed to supervise Jericho's research, even though he hated teaching.

Now Jericho stood on the landing and tried Turing's door. Locked, of course. The dust smeared his hand. He tried to remember how the room had looked. Squalor had been the overwhelming impression. Books, notes, letters, dirty clothes, empty bottles and tins of food had been strewn across the floor. There had been a teddy bear called Porgy on the mantelpiece above the gas fire, and a battered violin leaning in the corner, which Turing had picked up in a junk shop.

Robert Harris

ENIGMA (1995)

Turing had been too shy a man to get to know well. In any case, from the Christmas of 1938 he was hardly ever to be seen. He would cancel supervisions at the last minute saying he had to be in London. Or Jericho would climb these stairs and knock and there would be no reply, even though Jericho could sense he was behind the door. When, at last, around Easter 1939, not long after the Nazis had marched into Prague, the two men had finally met, Jericho had nerved himself to say: 'Look, sir, if you don't want to supervise me …'

'It's not that.'

'Or if you're making progress on the Riemann Hypothesis and you don't want to share it …'

Turing had smiled. 'Tom, I can assure you I am making no progress on Riemann whatsoever.'

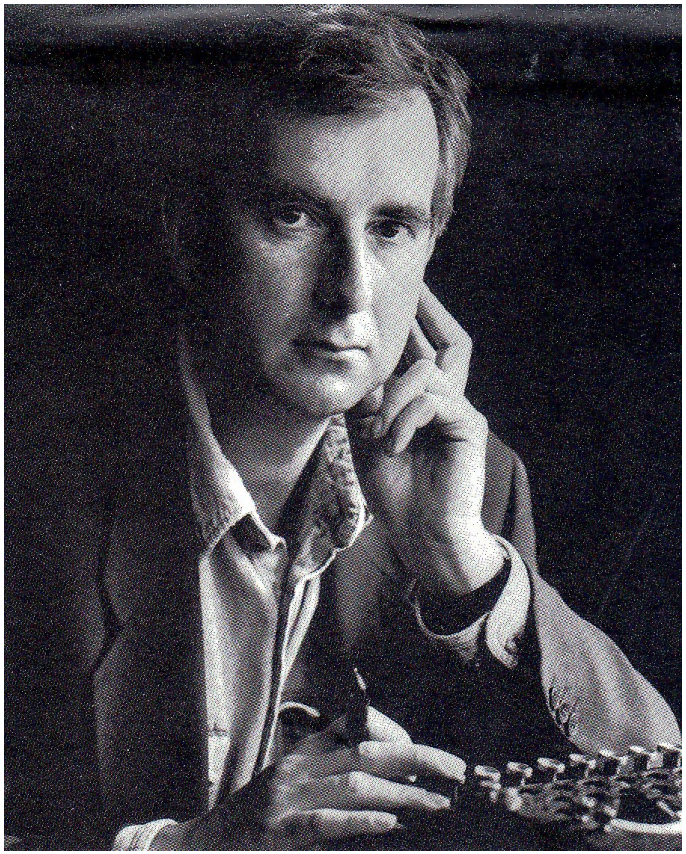
'Then what …?'

'It's not Riemann.' And then he had added, very quietly: 'There are other things now happening in the world, you know, apart from mathematics …'

Two days later Jericho had found a note in his pigeonhole.

Robert Harris

L'autore



- Nato a Nottingham nel 1957
- Studia a Cambridge
- Giornalista BBC, Observer, Sunday Times
- Fatherland (1992), Enigma (1995), Archangel (1999), Pompeii (2003), Imperium (2006), The Ghost (2007), Lustrum (Cospirata—2009)
- Saggi (tra cui Selling Hitler: Story of the Hitler Diaries (1986))
- Films: Fatherland, Enigma, The Ghost Writer, Archangel (BBC mini serie), . . .

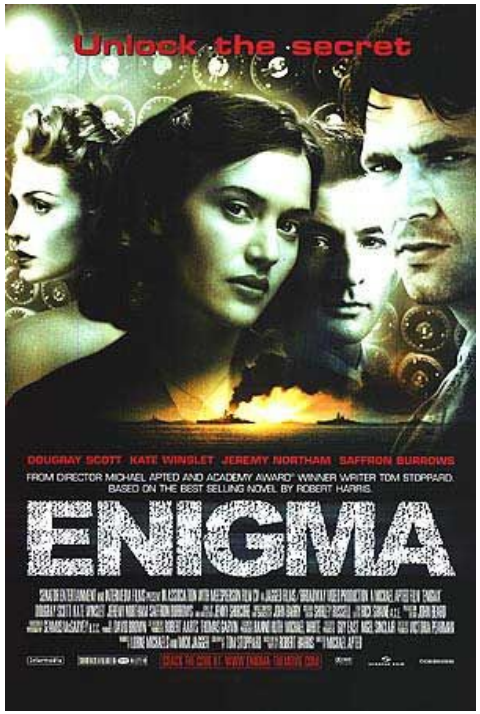
Michael Apted

Il regista

- Nato a Aylesbury il 10/02/1941
- Studia a Cambridge
- Dirige numerosi films, tra cui: Stardust (1974), Il segreto di Agatha Christie (1979), Gorky Park (1983), Gorilla nella nebbia (1988), Agente 007 - Il mondo non basta (1999) Enigma (2001), Le cronache di Narnia: il viaggio del veliero, . . .
- E documentari, ad esempio Bring on the night (Sting) La grande finale (documentario ufficiale dei mondiali FIFA di Germania).

Michael Apted

ENIGMA (2001)



Il film fu prodotto (in parte) da Mick Jagger che mise a disposizione il proprio ENIGMA.
Critiche principali: non menzionare mai (se non in una scena marginale sulla scelta del nome “squalo”) Alan Turing nè dare credito ai crittanalisti polacchi del Cipher Bureau.

Buona visione!