Attacco a Enigma: dal codice di Giulio Cesare alla moderna Crittografia

Agostino Dovier

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

23 MARZO 2016

Introduzione

- Inizieremo con una breve introduzione alla crittografia (incompleta . . . servirebbe una settimana)

- Approfittando della diffusione recente film The imitation game ci soffermeremo sull'Enigma e sulla figura di Alan Mathison Turing (23/06/1912–07/06/1954)

- Concluderemo poi con qualche accenno sulla crittografia *post-Enigma* e sul ruolo (anche se nascosto) nella società di oggi.

Introduzione

- Inizieremo con una breve introduzione alla crittografia (incompleta . . . servirebbe una settimana)

- Approfittando della diffusione recente film The imitation game ci soffermeremo sull'Enigma e sulla figura di Alan Mathison Turing (23/06/1912–07/06/1954)

- Concluderemo poi con qualche accenno sulla crittografia *post-Enigma* e sul ruolo (anche se nascosto) nella società di oggi.

Per ogni dubbio, domanda, interrompetemi in qualunque momento!

Codici Segreti

La nostra storia è da sempre piena di esempi di utilizzo di *codici* per nascondere l'informazione a tutti tranne che al desiderato destinatario.

La profezia di Daniele
MENE TEKEL PERES
(V Libro del profeta Daniele)
⇐ Rembrand: il festino di Baldassarre

ATBASH (Ebraico)

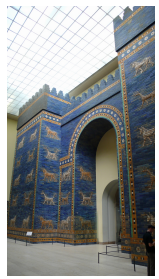
aleph	beth	gimel	daleth	he	waw	zayin	heth	teth	yod	kaph
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ
taw	sin shin	resh	qoph	sadhe	pe	ayin	samkeh	nun	mem	lamed
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל

ב ב ל

Babel/Babilonia

ש ש כ

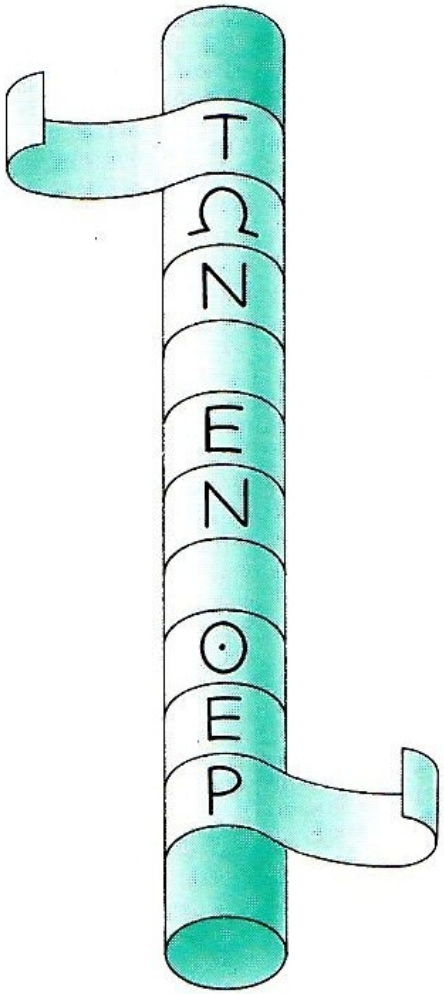
Sheschach

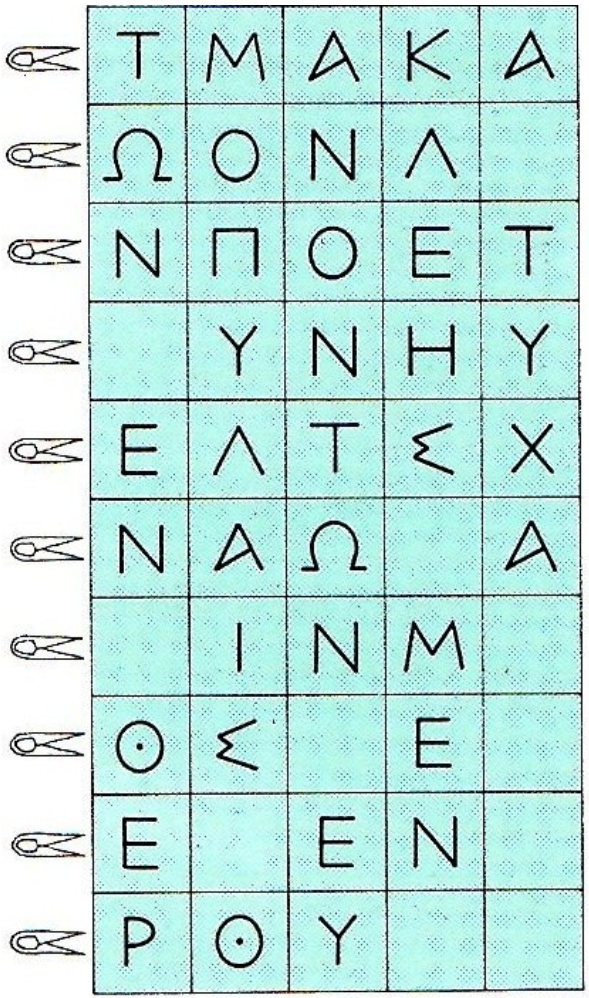


Il messaggio in chiaro viene trasformato in un messaggio in cifra (o crittogramma) mediante una operazione di cifratura usando un codice segreto (un algoritmo).

Codici Segreti

Scitala spartana (≈ 400 AC) — trasposizione





Codici Segreti

Steganografia (nascondere l'informazione)

- Scrivere in messaggio sotto la cera nuova delle tavolette di cera (block notes/tablet dell'epoca)
- Se non c'è fretta: radere i capelli, scrivere sul cuoio capelluto, attendere che ricrescano e inviare il messaggero col messaggio (Istiéo ad Aristagona di Mileto)
- Usare una miscela di allume e aceto per scrivere sul guscio d'uovo (sodo). Il messaggio si vedrà solo a uovo pelato (G.B. Della Porta)
- Inchiostri simpatici di vario tipo . . .

Codici Segreti

Steganografia (nascondere l'informazione)

- Scrivere in messaggio sotto la cera nuova delle tavolette di cera (block notes/tablet dell'epoca)
- Se non c'è fretta: radere i capelli, scrivere sul cuoio capelluto, attendere che ricrescano e inviare il messaggero col messaggio (Istiéo ad Aristagona di Mileto)
- Usare una miscela di allume e aceto per scrivere sul guscio d'uovo (sodo). Il messaggio si vedrà solo a uovo pelato (G.B. Della Porta)
- Inchiostri simpatici di vario tipo . . .
  Il messaggio non è cifrato, è solo nascosto. Se cade in mano del nemico viene compreso in poco tempo: non approfondiremo la steganografia!

Cifrari a sostituzione monoalfabetica

Giulio Cesare (100–44 AC)

P I G R E C O

S M K V H F R

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

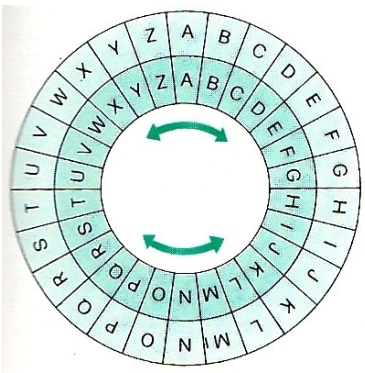
Cifrari a sostituzione monoalfabetica

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

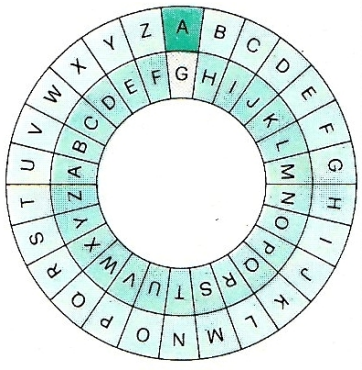
- La “chiave” segreta è la lettera iniziale (la D per Cesare).
- Anche ammettendo che la spia conosca il tipo di codifica usata (Principio di Kerckhoffs 1835–1903)
  deve essere difficile per lei/lui identificare tale la chiave.
- Ci sono una ventina di chiavi: il codice è troppo debole.

Cifrari a sostituzione monoalfabetica

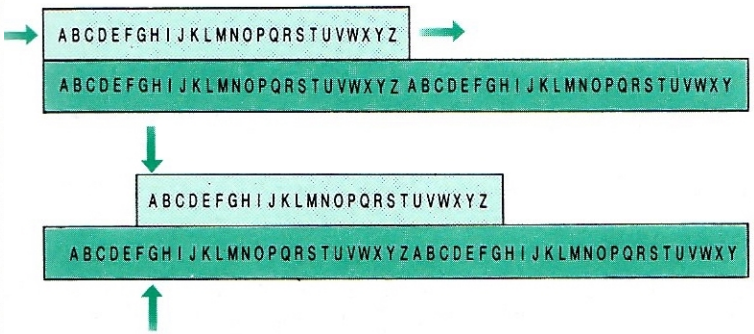
Macchine di cifra



L.B. Alberti
(1404–1472)



G.B. Della Porta
(1535–1615)



Regolo di Saint Cyr
(fine 800)

Cifrari a sostituzione monoalfabetica

Cifrari completi

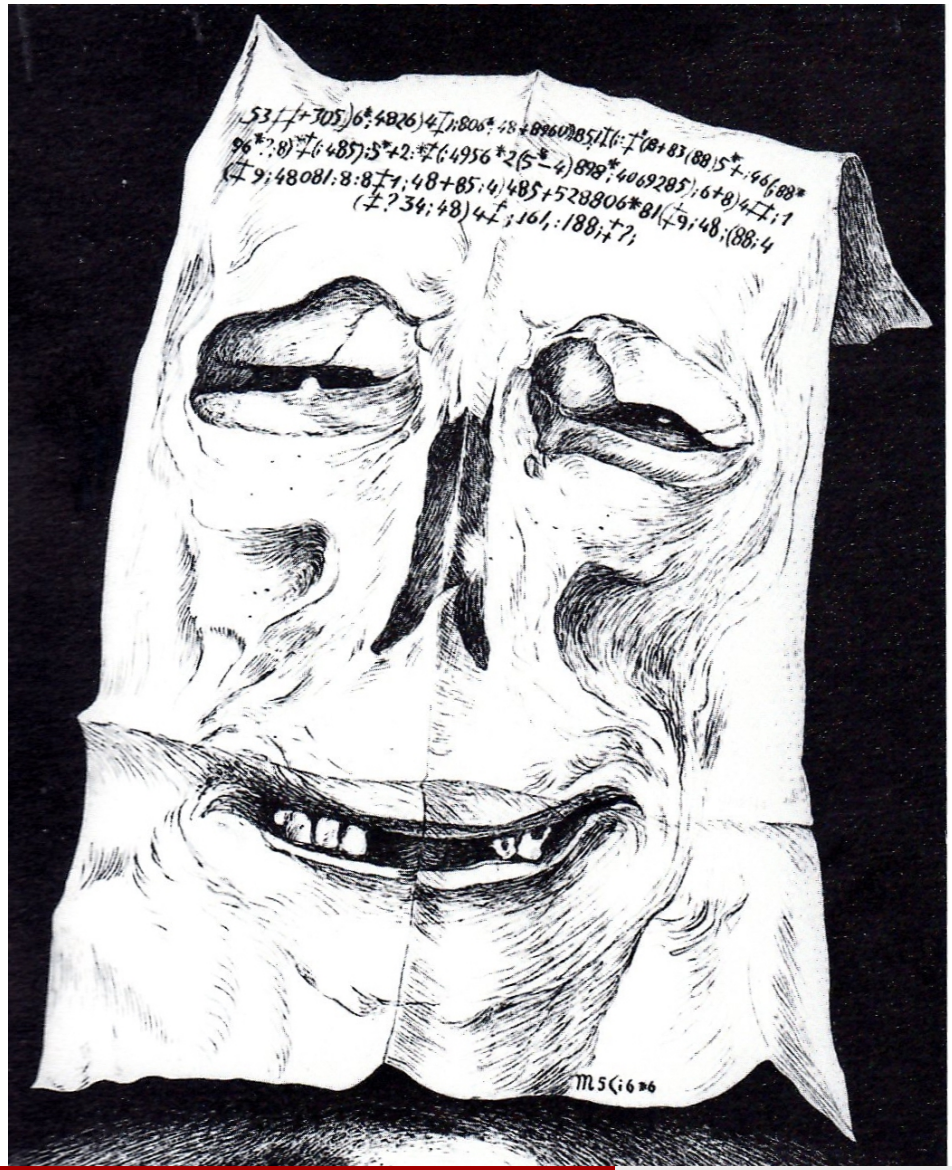
- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.

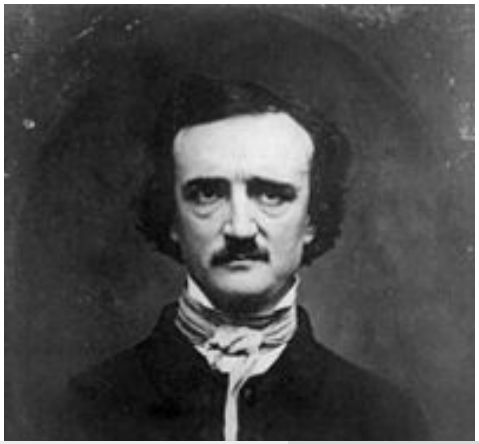
A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
M	V	F	T	H	C	K	L	D	N	O	P	Q	R	A	G	E	X	S	B	I

- Le chiavi possibili diventano $21! = 21 \cdot 20 \cdot 19 \cdots 2 \cdot 1 \approx 5 \cdot 10^{19}$ (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 monoalfabetica

Decrittazione





Cifrari a sostituzione monoalfabetica

Decrittazione

Viene usata la statistica linguistica.

Il carattere 8 si trova 33 volte
= " ; " " 26 "
= " 4 " " 19 "
= ") " " 16 "
= " ‡ " " 16 "
= " * " " 13 "
= " 5 " " 12 "
= " 6 " " 11 "
= " † " " 8 "
= " 1 " " 8 "
= " 0 " " 6 "
= " 9 " " 5 "
= " 2 " " 5 "
= " : " " 4 "
" " 3 " " 4 "
" " ? " " 3 "
" " ¶ " " 2 "
" " - " " 1 "
" " . " " 1 "

Confondere la statistica

Testo ausiliario

C'era una volta, tanto tempo fa, una principessa che non voleva uscire di casa per far le compere ma ordinare tutto senza alzarsi dalla scrivania utilizzando la connessione wifi a bassa protezione in hotel.

Confondere la statistica

Testo ausiliario

C'era una volta, tanto tempo fa, una principessa che non voleva uscire di casa per far le compere ma ordinare tutto senza alzarsi dalla scrivania utilizzando la connessione wifi a bassa protezione in hotel.

Allora, il testo "attacchiamo" può essere cifrato con:

24 6 5 31 19 1 35 34 24 20 21

Confondere la statistica

Testo ausiliario

C'era una volta, tanto tempo fa, una principessa che non voleva uscire di casa per far le compere ma ordinare tutto senza alzarsi dalla scrivania utilizzando la connessione wifi a bassa protezione in hotel.

Allora, il testo "attacchiamo" può essere cifrato con:

24 6 5 31 19 1 35 34 24 20 21

n indica l'iniziale della parola *n*-esima del testo.
Se non si conosce il testo chiave, e si evitano le ripetizioni, è un buon sistema.

Confondere la statistica

Testo ausiliario

C'era una volta, tanto tempo fa, una principessa che non voleva uscire di casa per far le compere ma ordinare tutto senza alzarsi dalla scrivania utilizzando la connessione wifi a bassa protezione in hotel.

Allora, il testo "attacchiamo" può essere cifrato con:

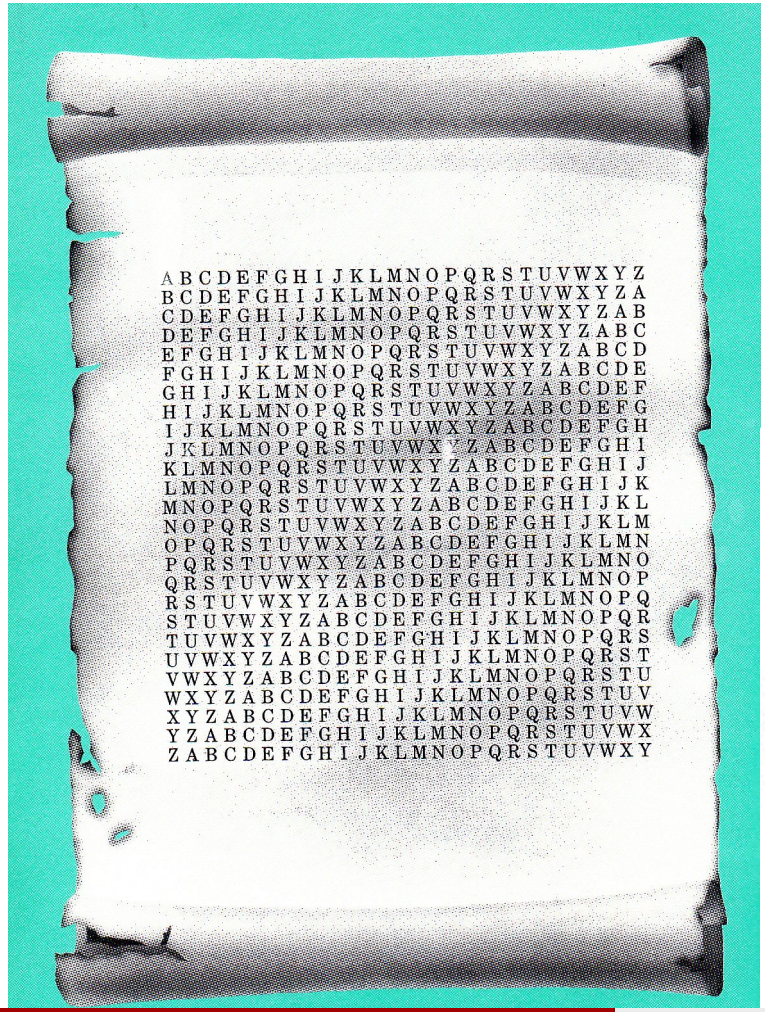
24 6 5 31 19 1 35 34 24 20 21

n indica l'iniziale della parola *n*-esima del testo.
Se non si conosce il testo chiave, e si evitano le ripetizioni, è un buon sistema.

Il secondo crittogramma di Beale è stato cifrato con questa tecnica, usando la dichiarazione d'indipendenza degli stati uniti (parole numerate da 1 a 1322).

Cifrari a sostituzione polialfabetica

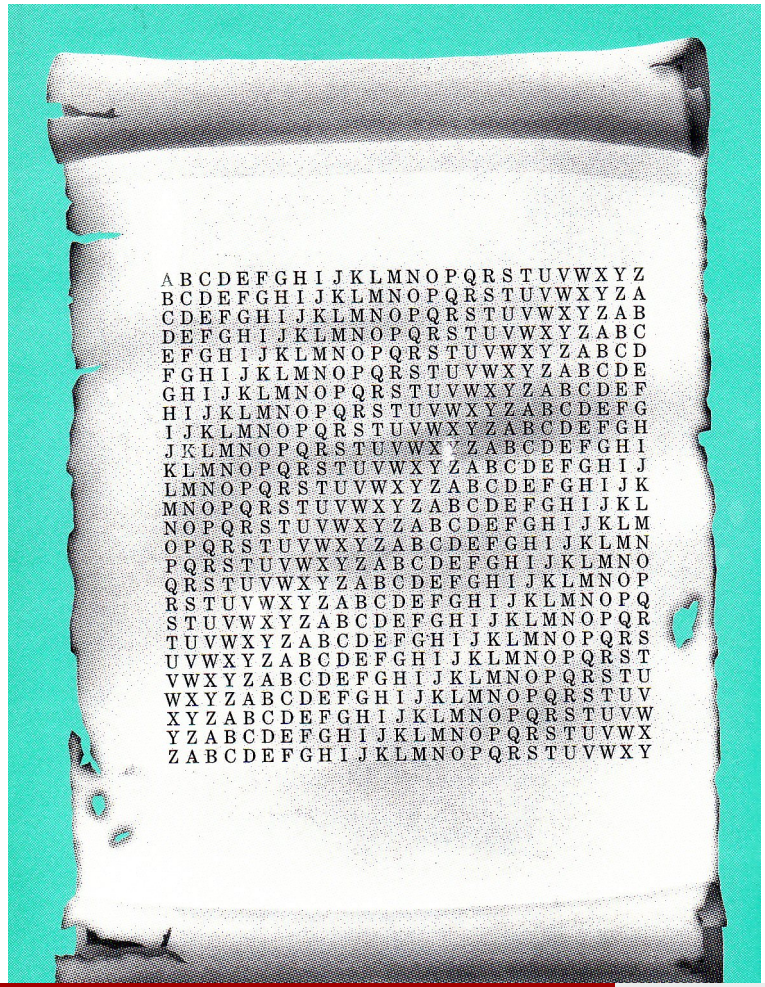
Blaise de Vigenère (1523–1596)



Cifrari a sostituzione polialfabetica

Cifrazione

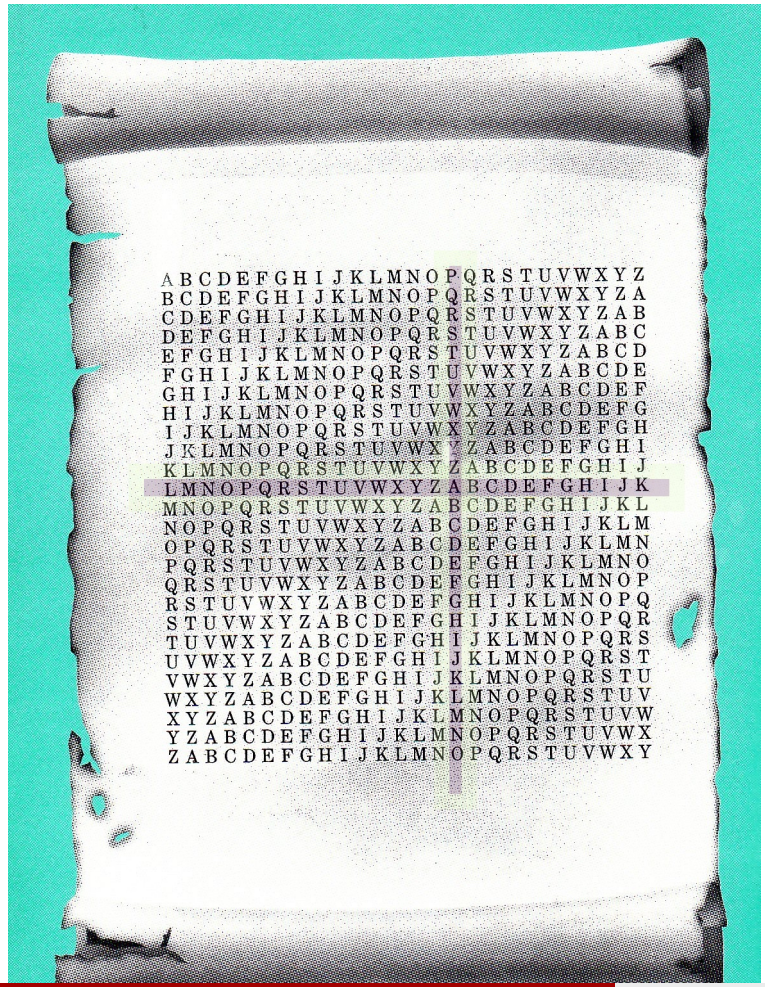
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

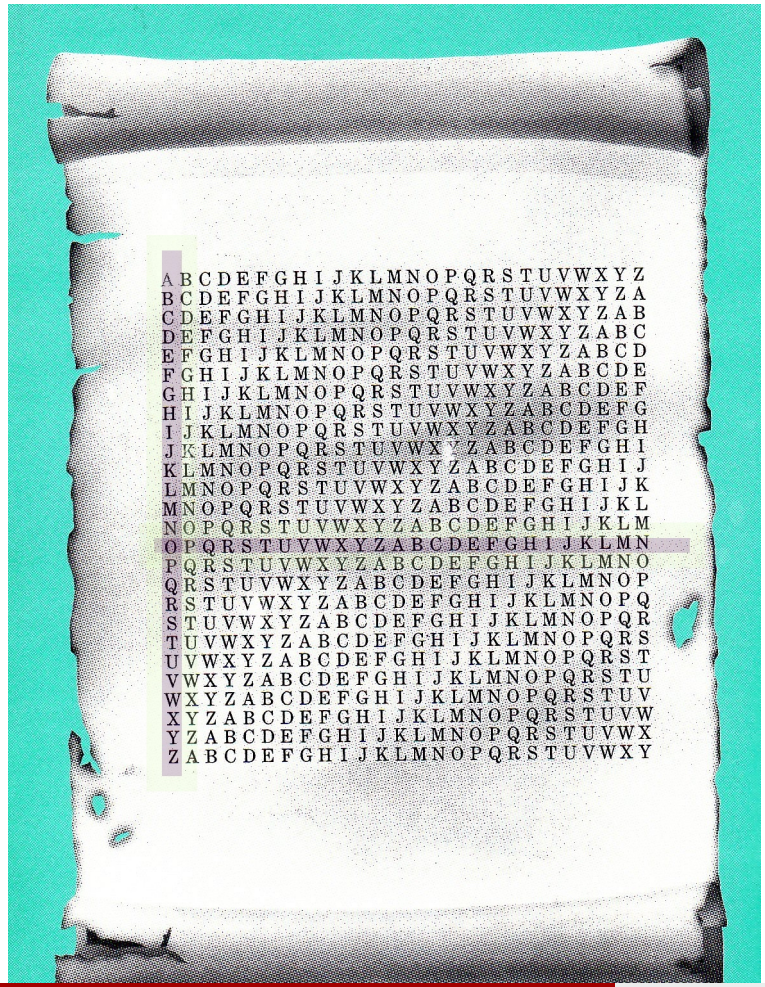
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

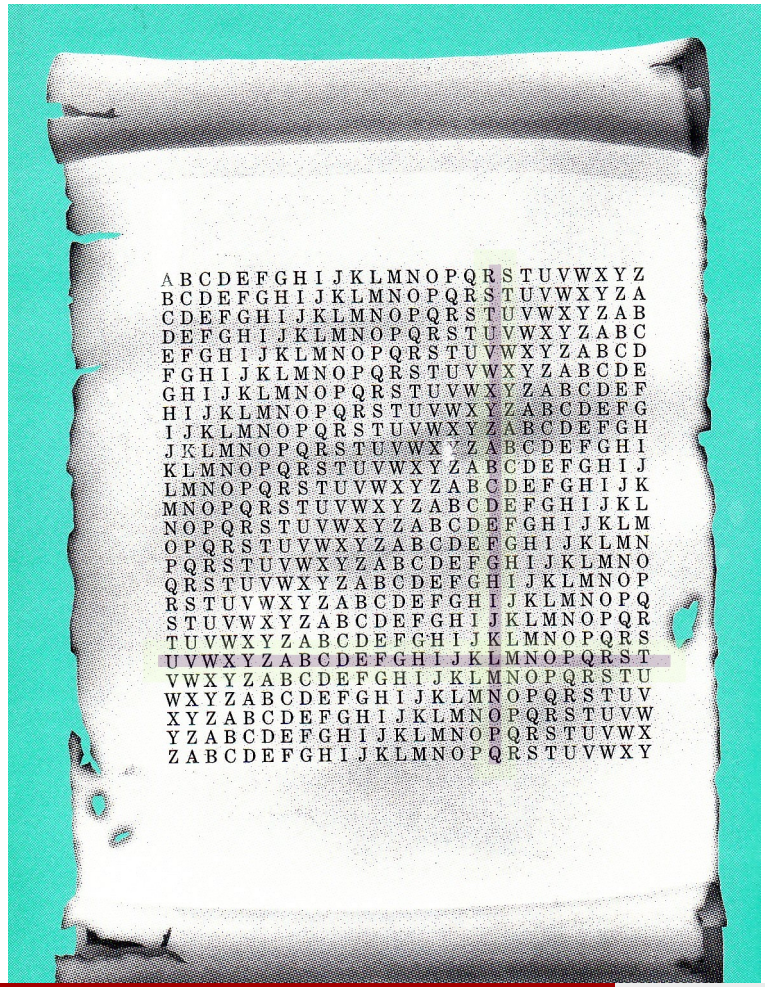
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

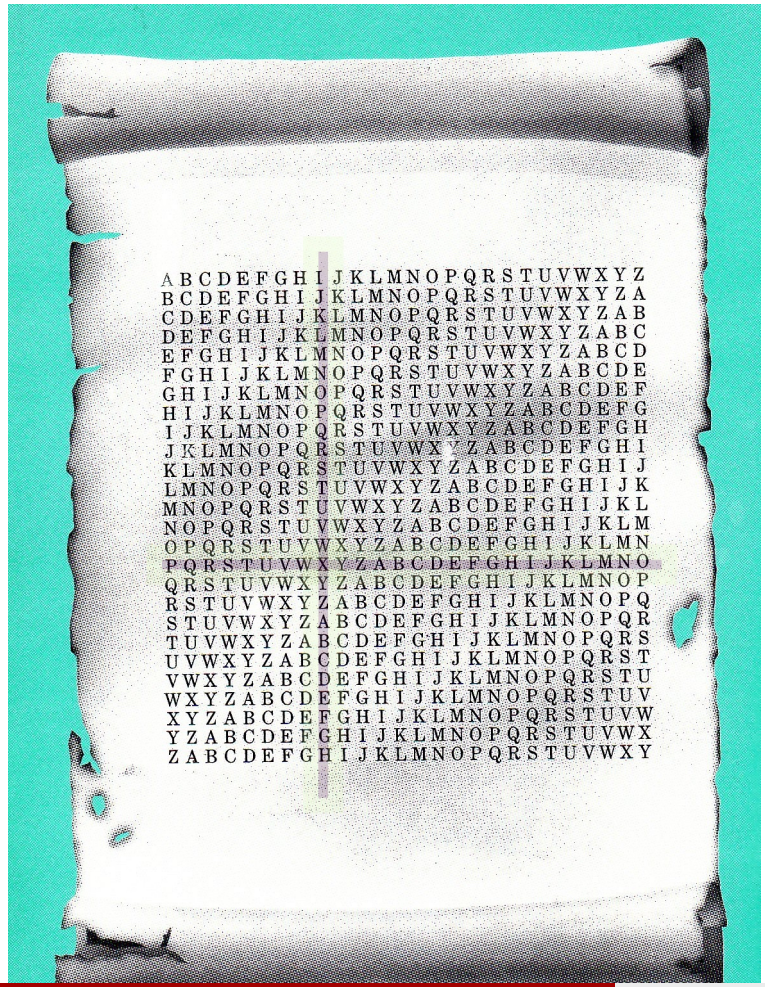
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



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 $21^n = \underbrace{21 \cdot 21 \cdot \cdots \cdot 21}_{n}$.
- Inoltre la statistica sembra ingannata.
- E la spia non conosce nemmeno n.

Andrew Swanston. Il codice del traditore (The King's Spy). 2012

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

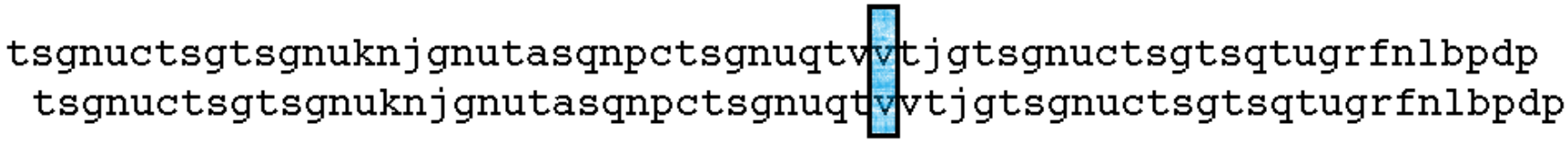
Cifrari a sostituzione polialfabetica

Decrittazione

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Cifrari a sostituzione polialfabetica

Decrittazione



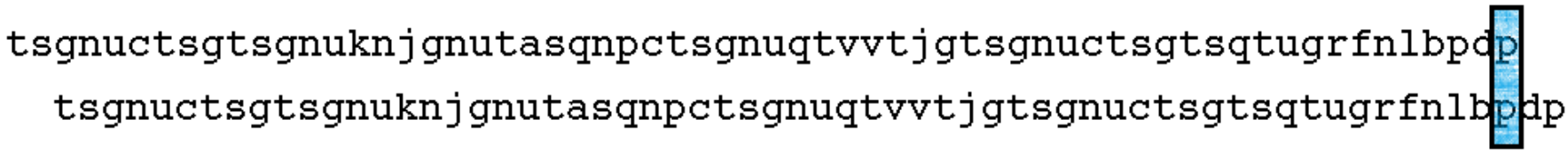
Cifrari a sostituzione polialfabetica

Decrittazione

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
  tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Cifrari a sostituzione polialfabetica

Decrittazione



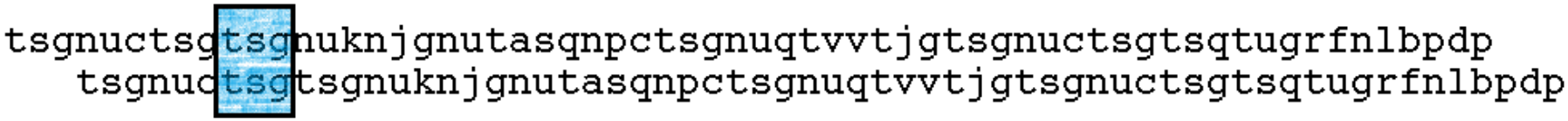
Cifrari a sostituzione polialfabetica

Decrittazione

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
   tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

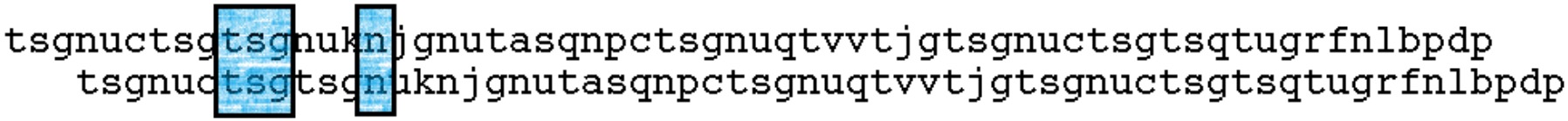
Cifrari a sostituzione polialfabetica

Decrittazione



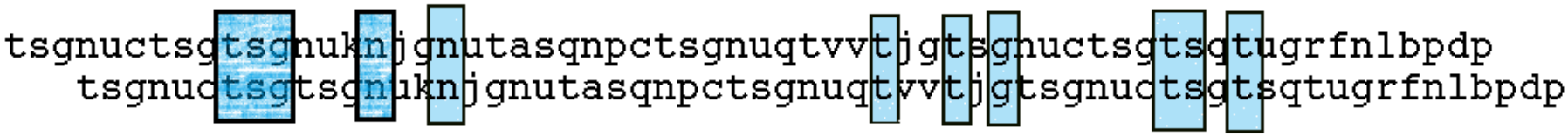
Cifrari a sostituzione polialfabetica

Decrittazione



Cifrari a sostituzione polialfabetica

Decrittazione



Cifrari a sostituzione polialfabetica

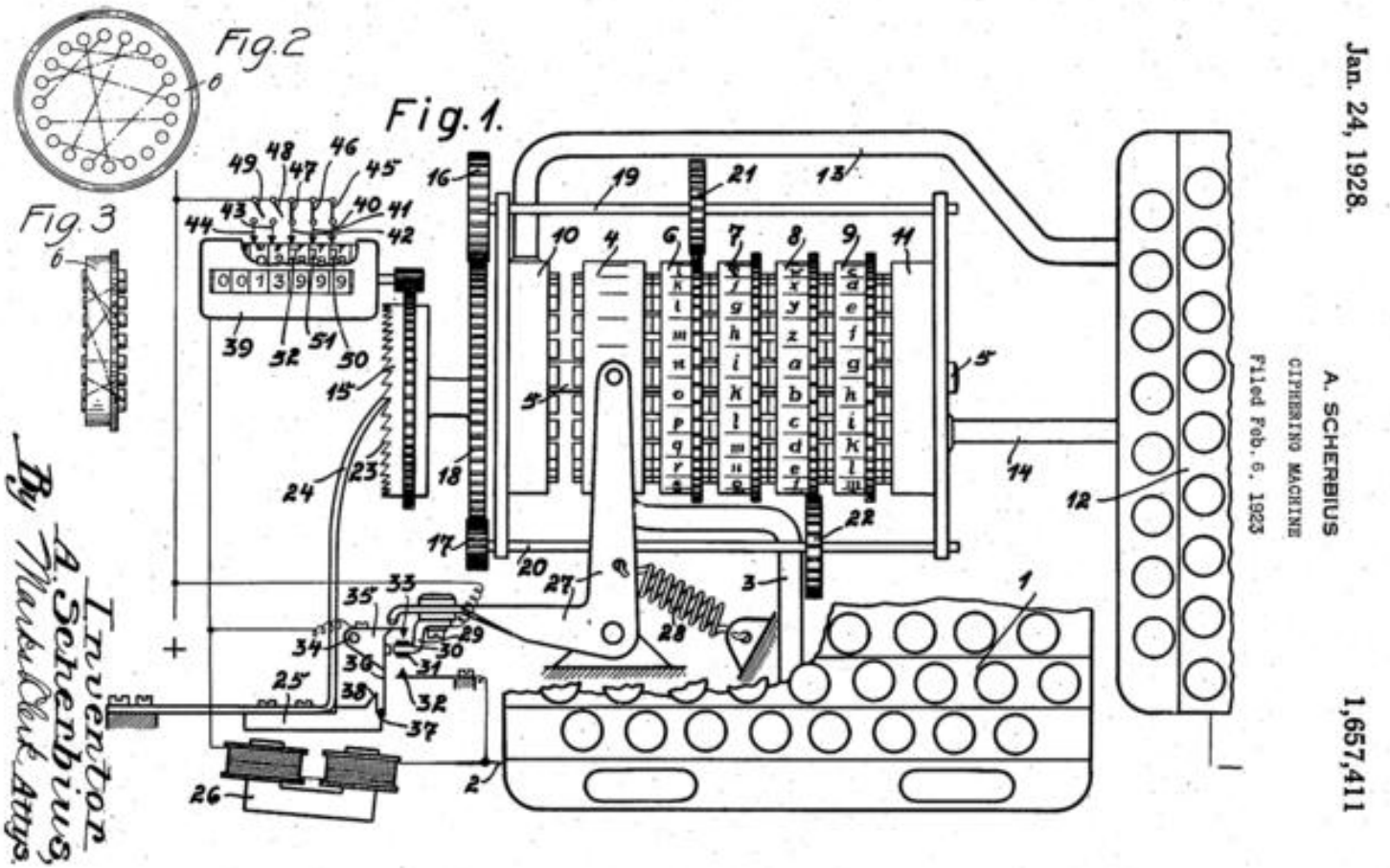
Decrittazione e limiti

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/one time pad—Vernam)
4. In generale, se la chiave (il periodo) è molto lungo rispetto al testo la decodifica statistica non è effettiva.

Enigma

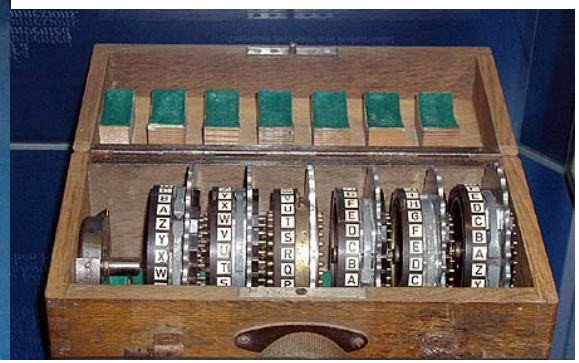
Arthur Scherbius (1878–1929)

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



Enigma

Nel 1923 Scherbius commercializza l'Enigma.

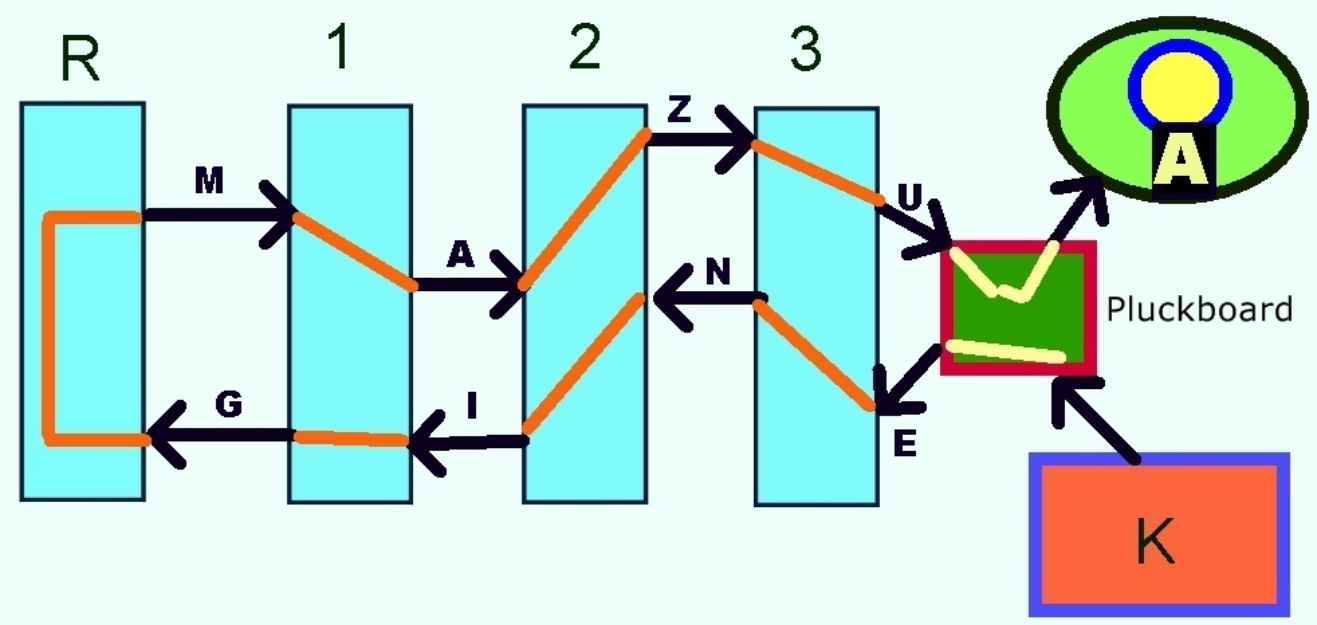


Enigma: funzionamento

- 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).
- Ci sono simulatori di Enigma per tutte le piattaforme (Windows, Linux, Mac, I-phone, Android). Quella forse più realistica e corredata di diverso materiale sulla crittografia si trova qui: `http://users.telenet.be/d.rijmenants/`

Enigma: funzionamento

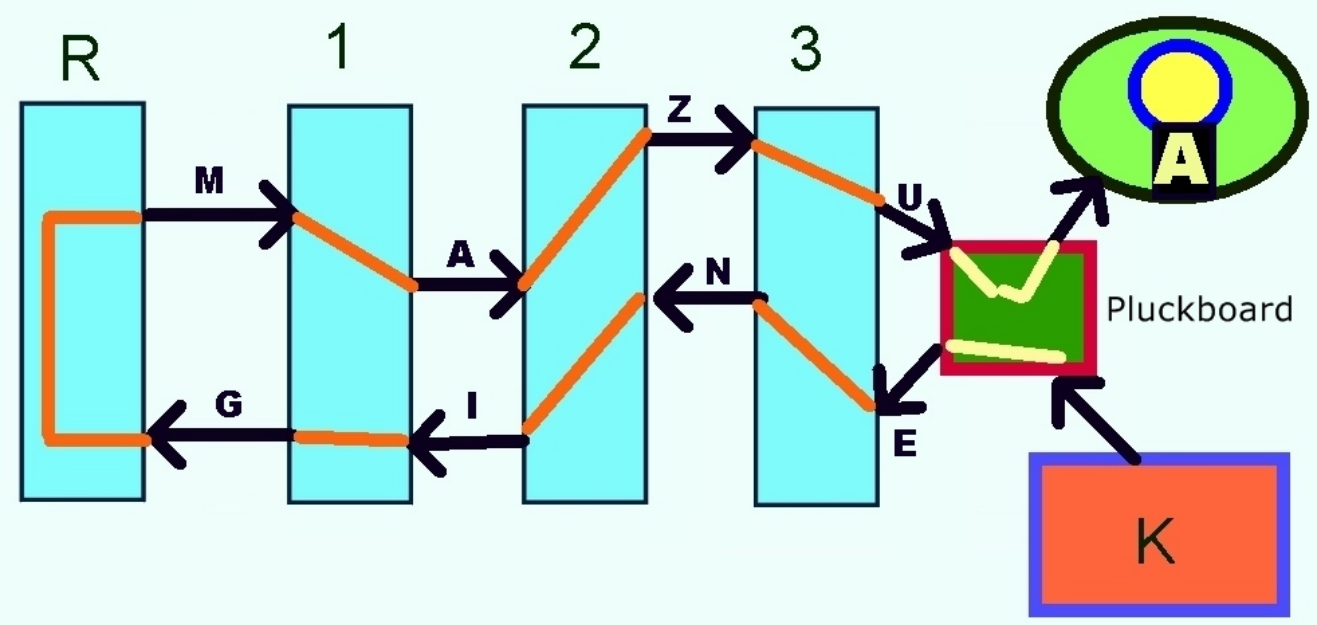
È una macchina a rotori non fissi che si muovono con moto odometrico dopo ogni lettera codificata—stepping motion (come i vecchi contachilometri o i contatori dell'acqua o del gas).



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

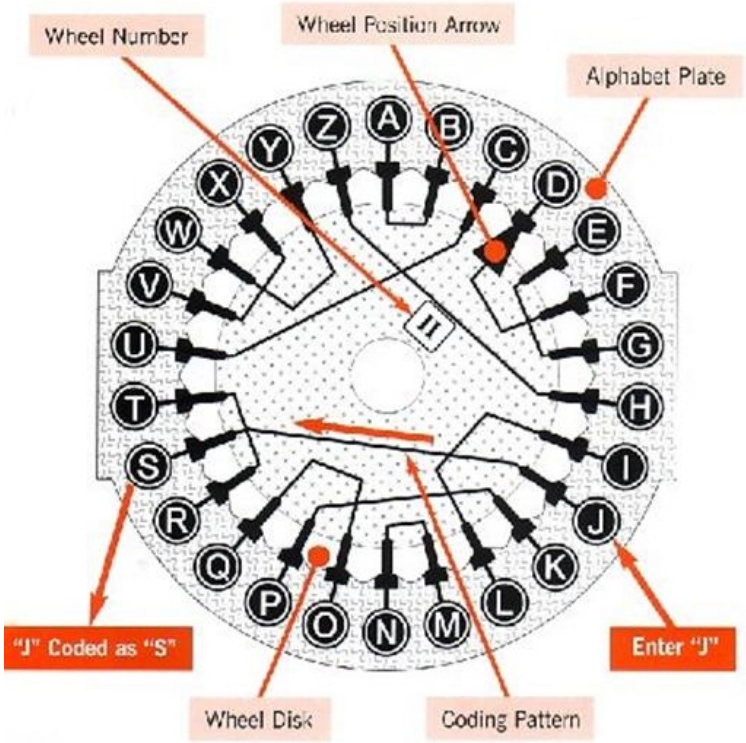
Enigma: funzionamento

È 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).
Mai una lettera sarà codificata in sè stessa.

Enigma: funzionamento



(DEMO)

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:

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

Alan M. Turing . . . e π

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. Turing.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

In §§ 9, 10 I give some arguments with the intention of showing that the computable numbers include all numbers which could naturally be regarded as computable. In particular, I show that certain large classes of numbers are computable. They include, for instance, the real parts of all algebraic numbers, the real parts of the zeros of the Bessel functions, the numbers π, e, etc. The computable numbers do not, however, include all definable numbers, and an example is given of a definable number which is not computable.

Alan M. Turing . . . e la corsa del $(2\pi)^2 + \frac{\pi}{2}$

23/06/1912–07/06/1954

ATHLETICS

MARATHON AND DECATHLON CHAMPIONSHIPS

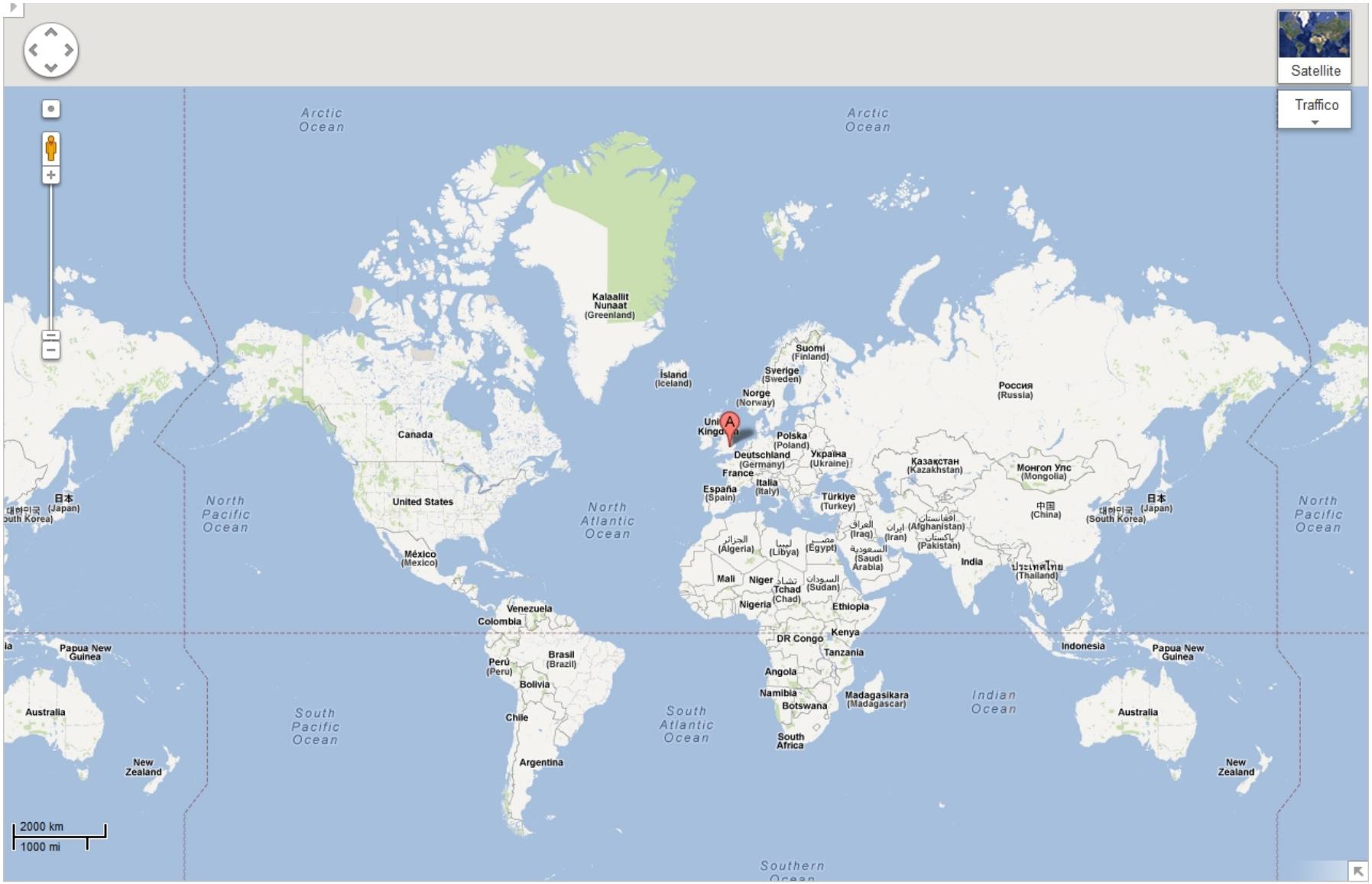
The Amateur Athletic Association championships for this year were concluded at Loughborough College Stadium, Leicestershire, on Saturday, with the second, and last, day of the Decathlon and the decision of the Marathon championship.

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.

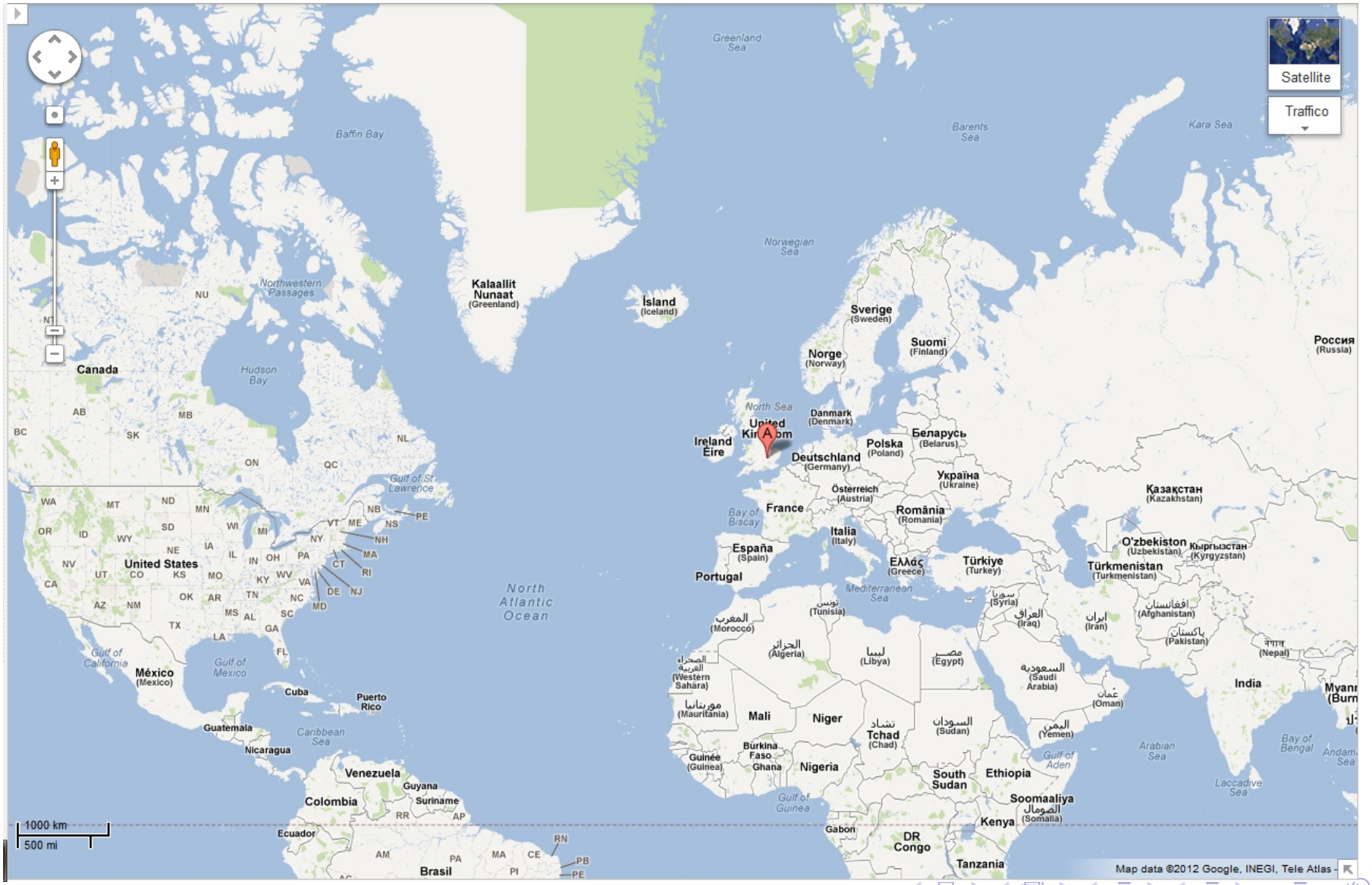
DECATHLON CHAMPIONSHIP.—H. J. Moesgaard-Kjeldsen (Polytechnic Harriers, London), 5,965 points, 1; Captain H. Whittle (Army and Reading A.C.), 5,650, 2;

(1947) Nel 1948 (Olimpiadi di Londra) Delfo Cabrera vinse in 2h34'51"

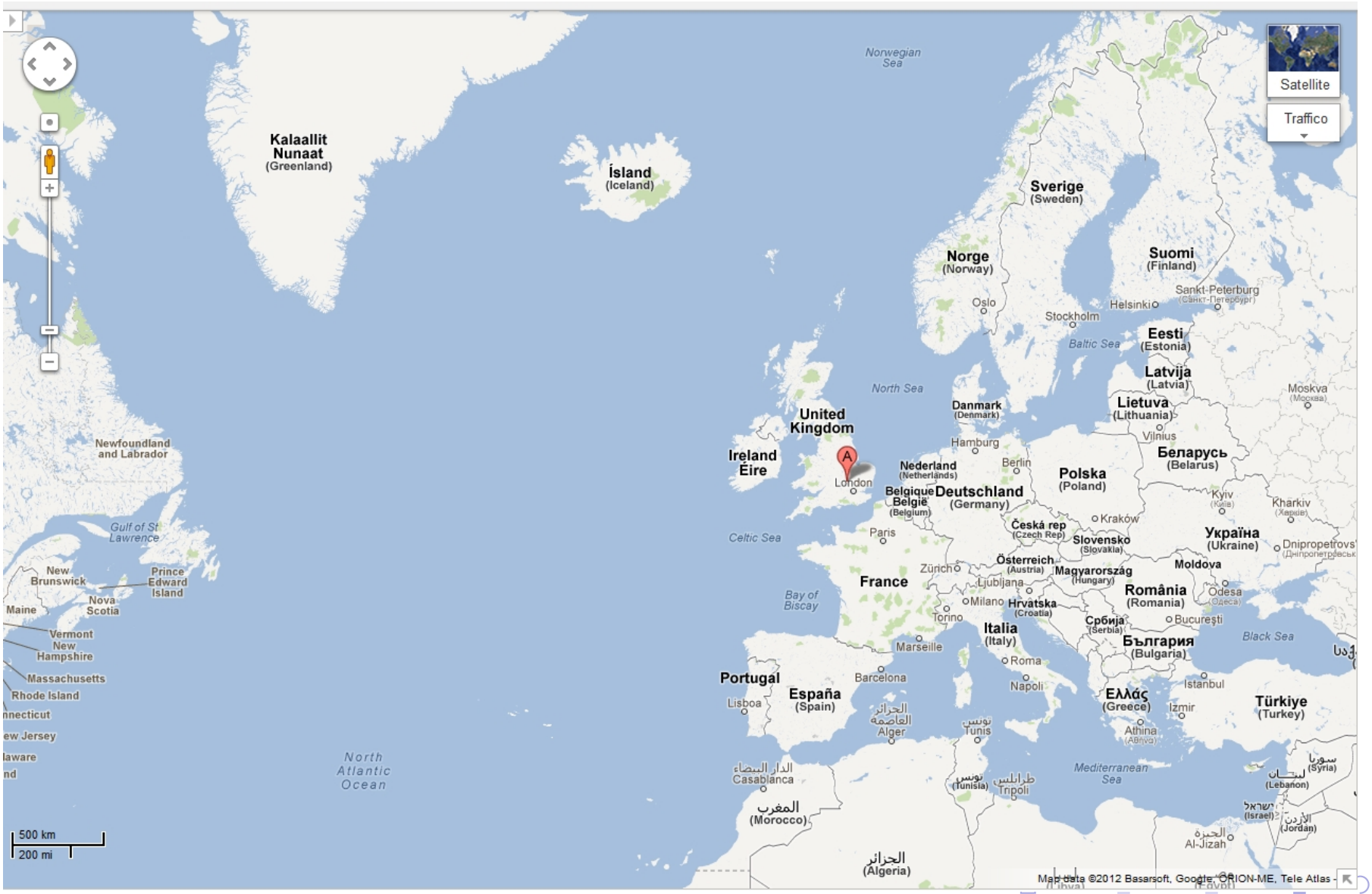
. . . a Bletchley Park



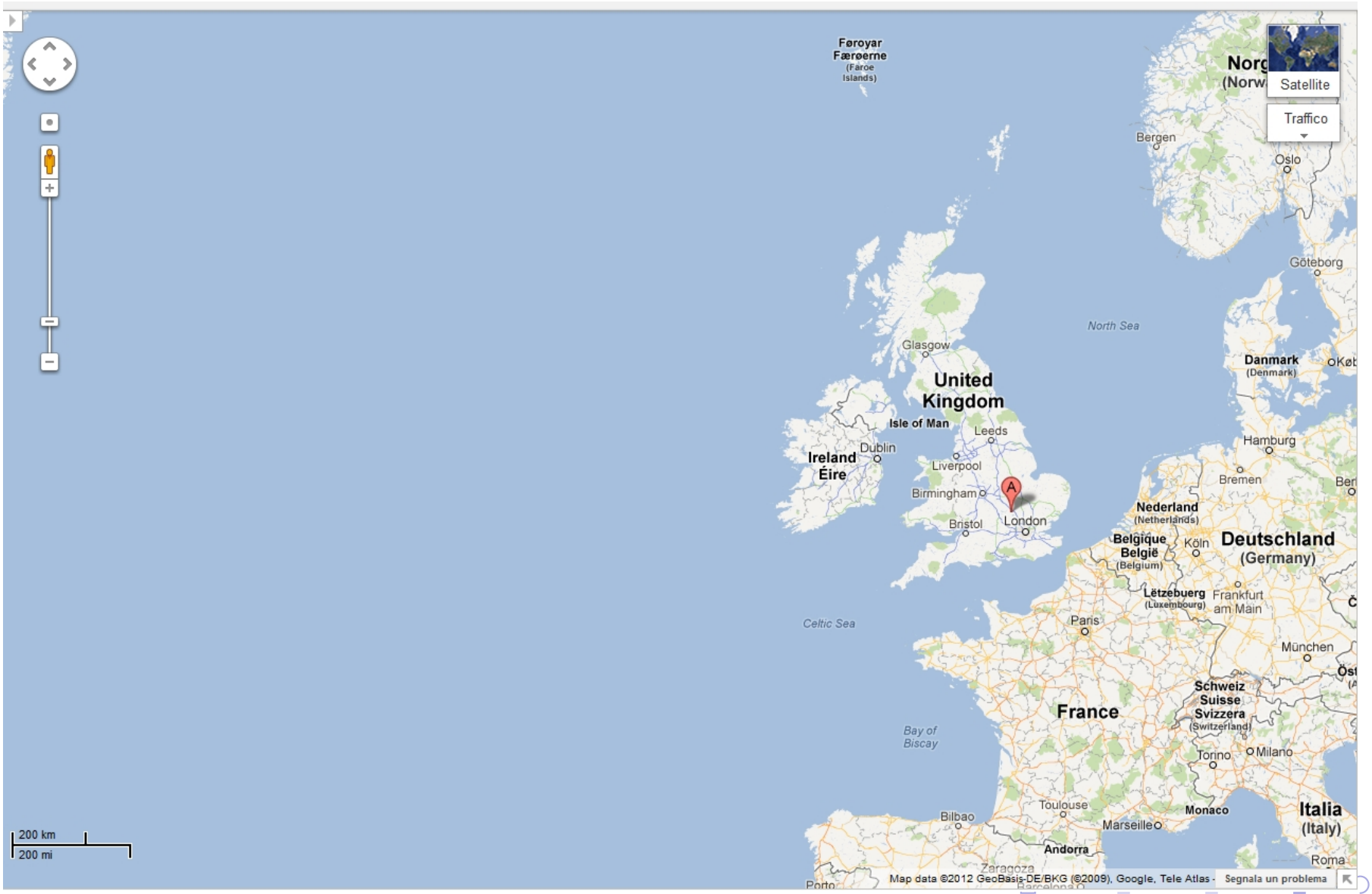
. . . a Bletchley Park



. . . a Bletchley Park



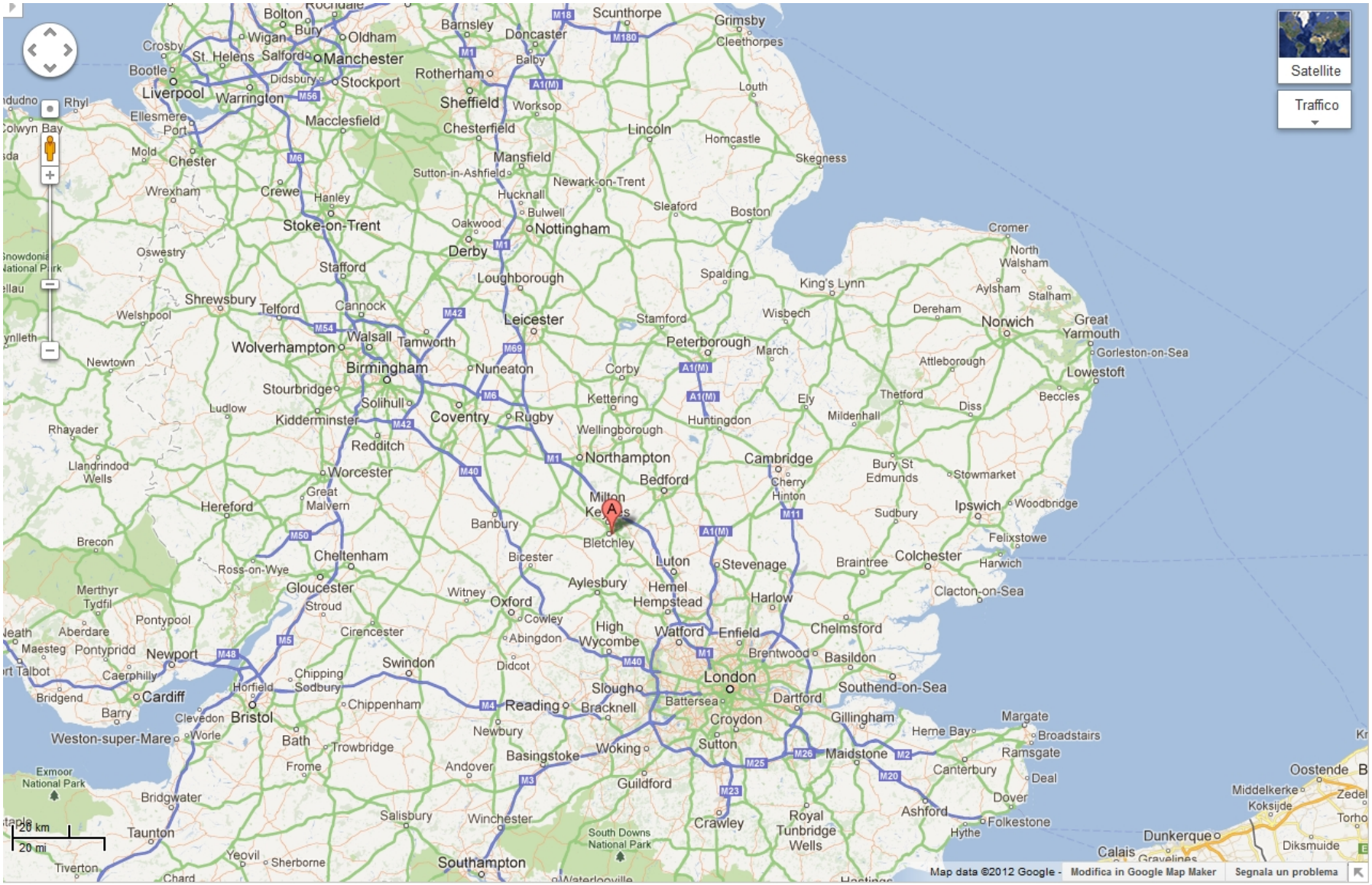
. . . a Bletchley Park



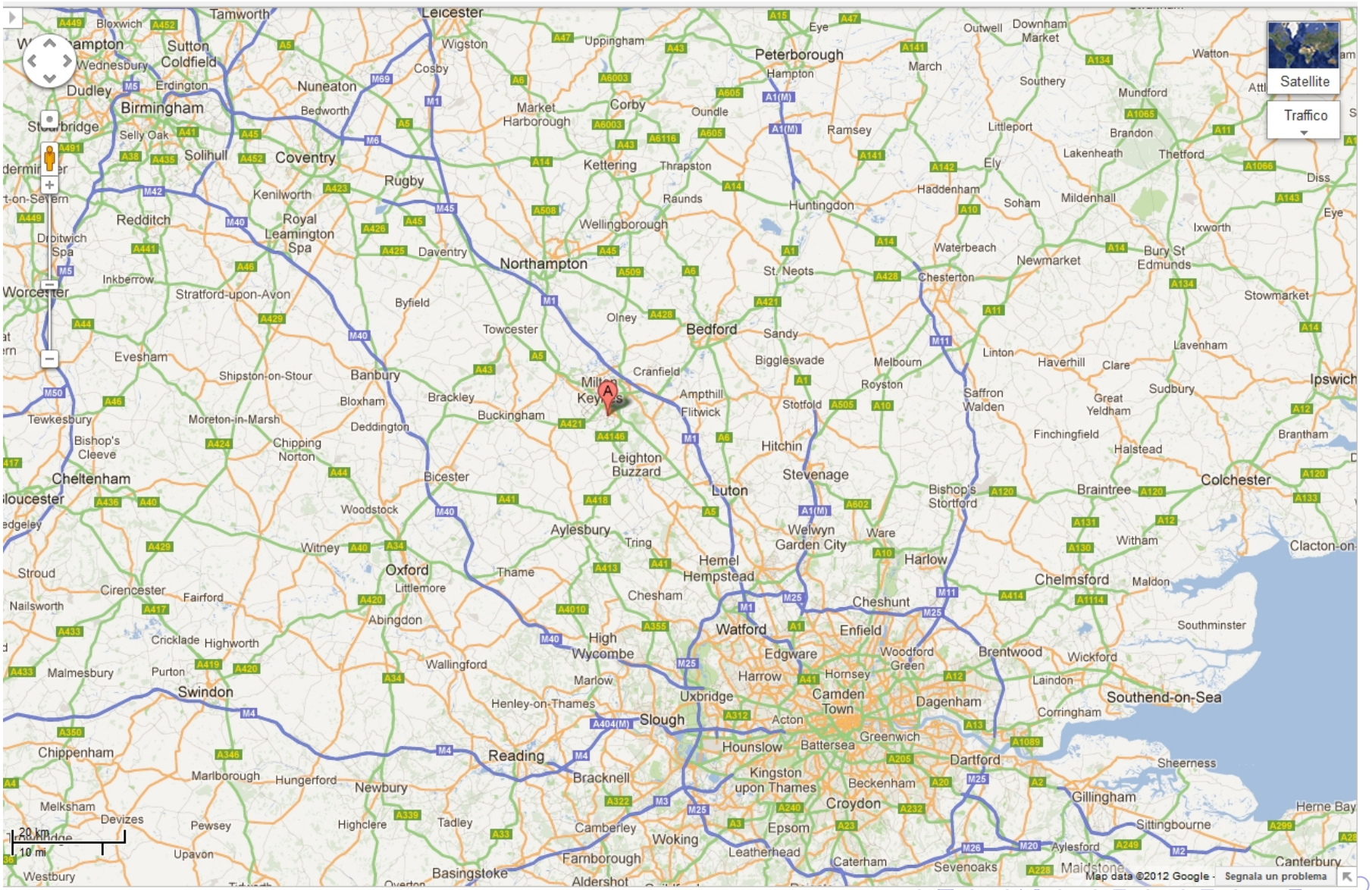
. . . a Bletchley Park

. . . a Bletchley Park

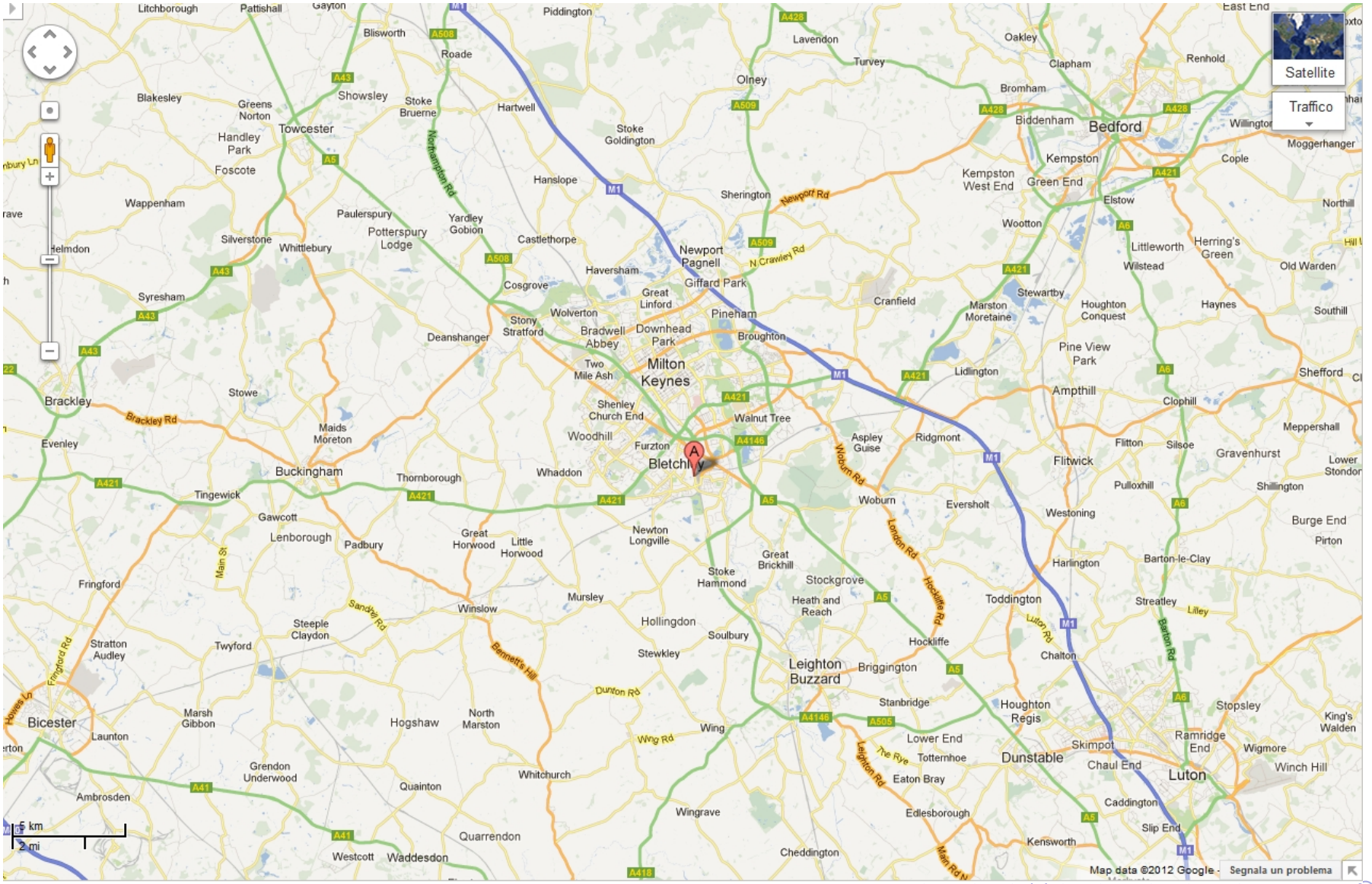
. . . a Bletchley Park



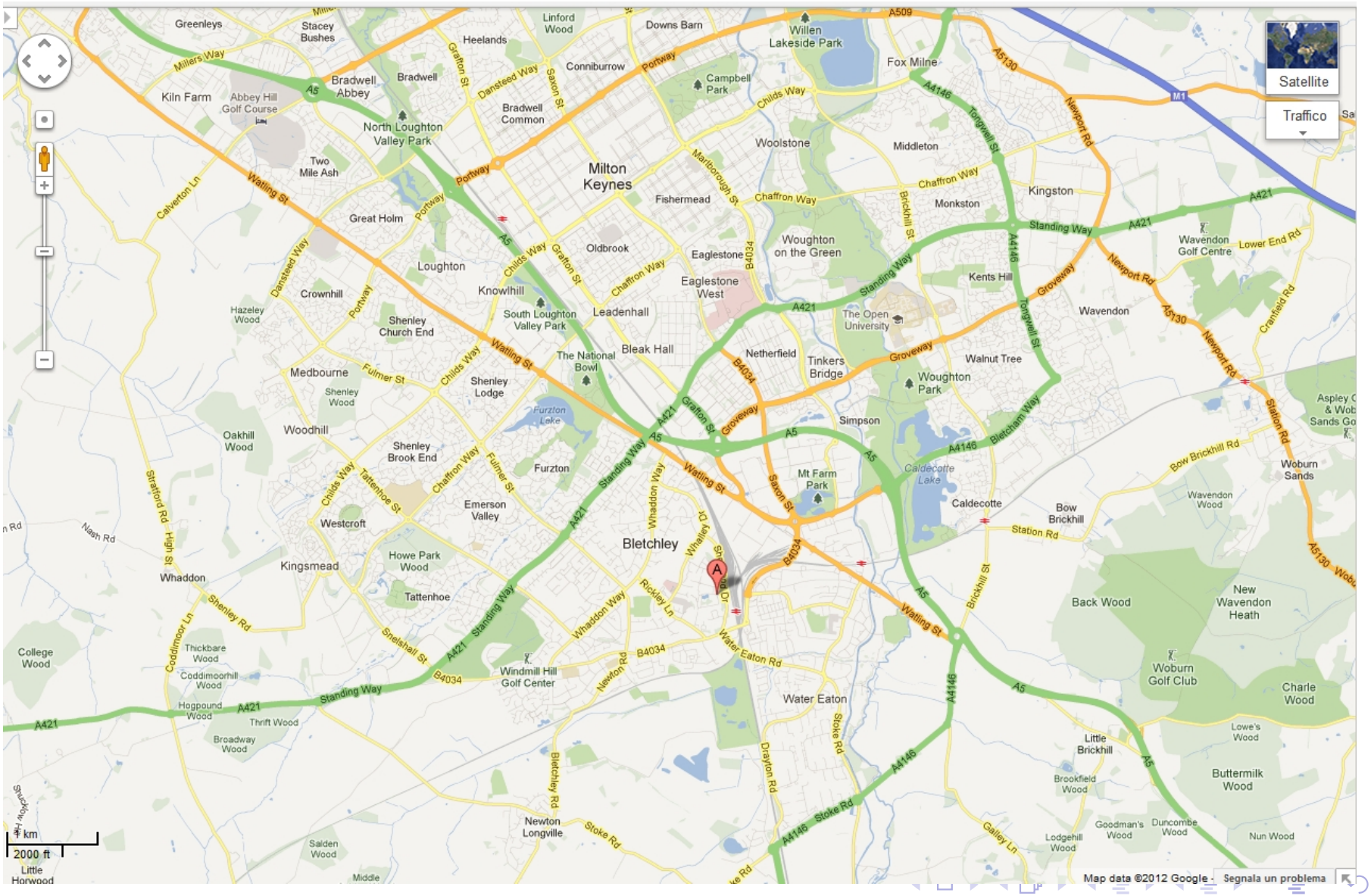
. . . a Bletchley Park



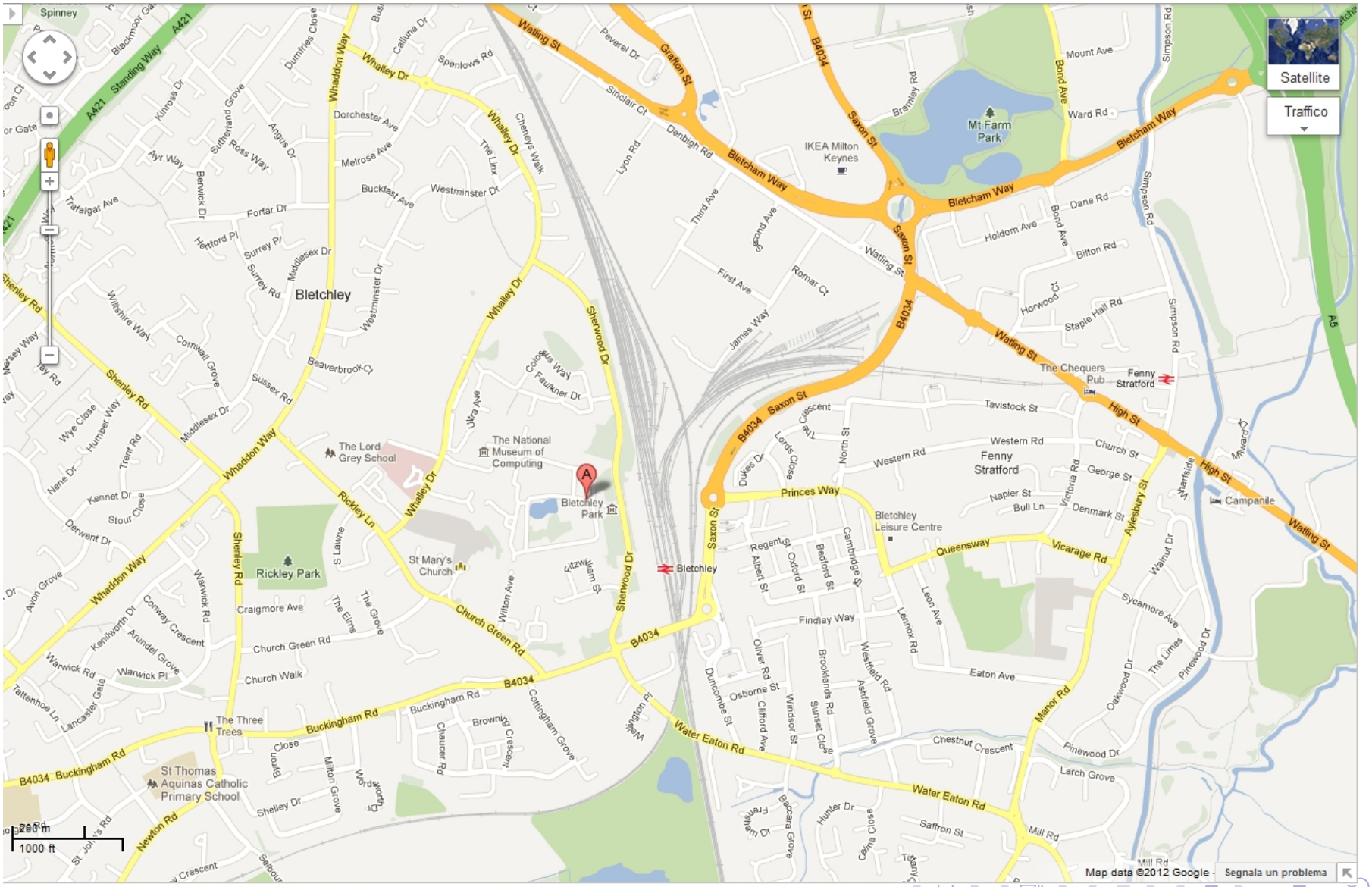
. . . a Bletchley Park



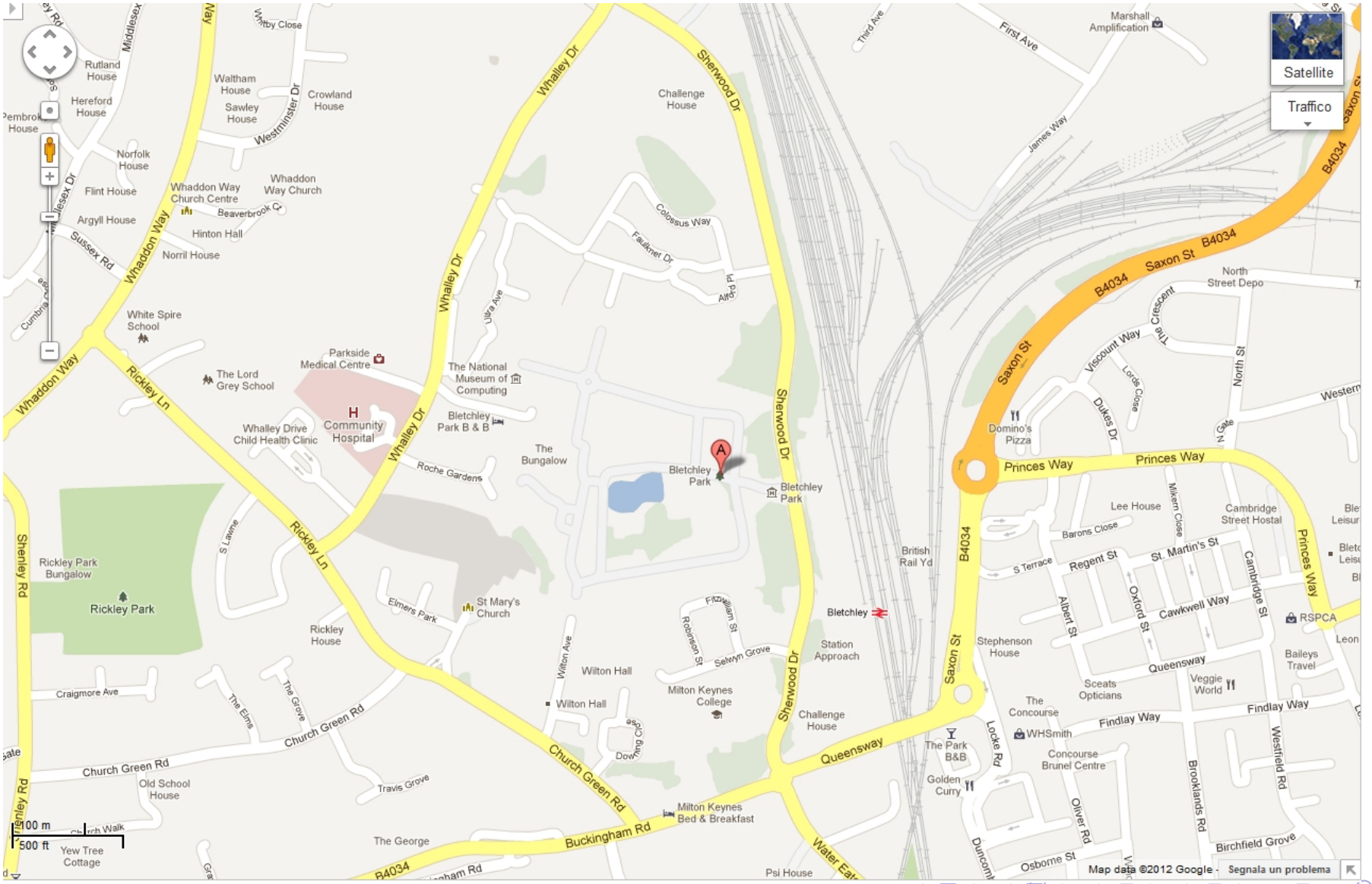
. . . a Bletchley Park



. . . a Bletchley Park

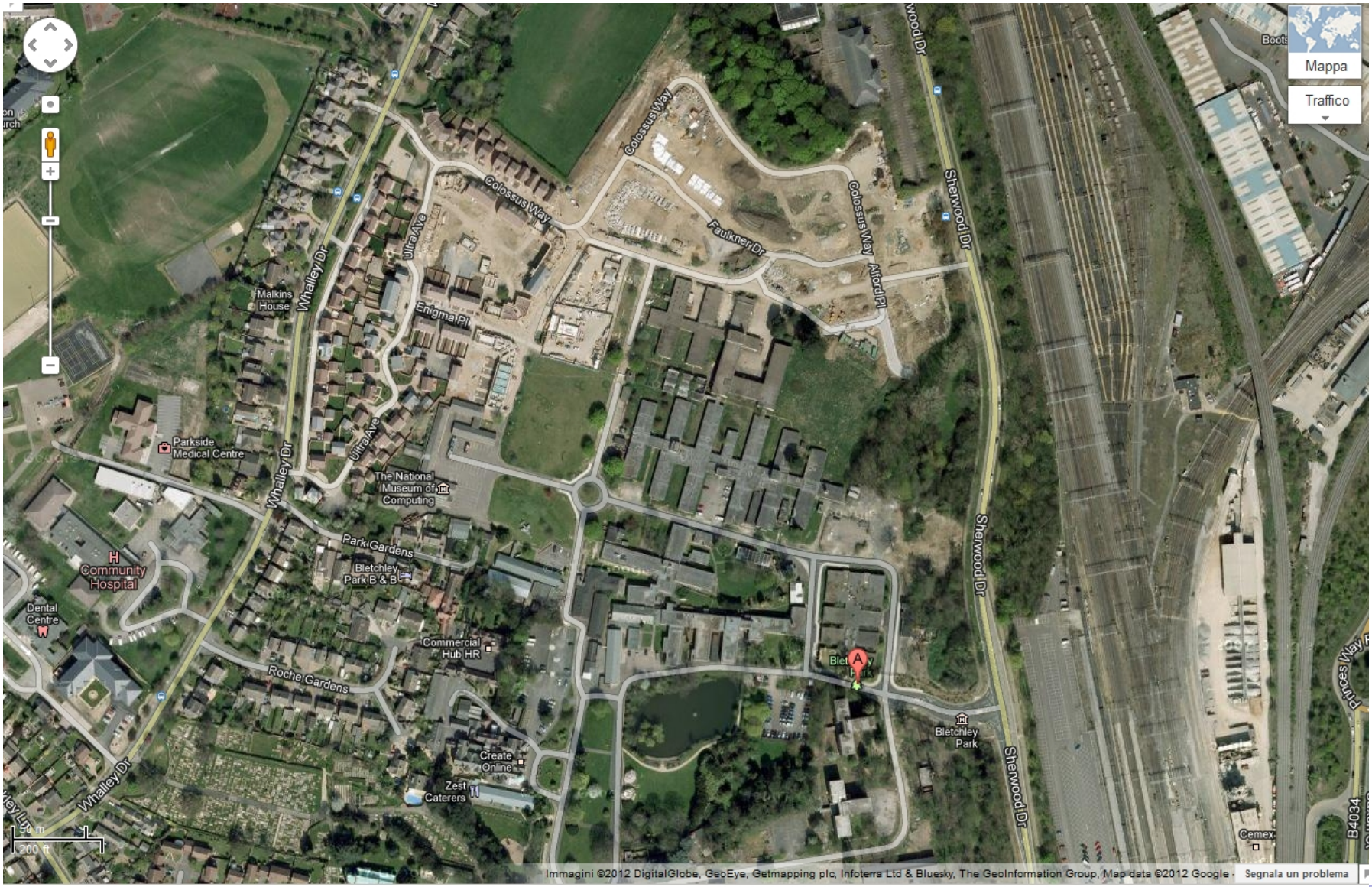


. . . a Bletchley Park

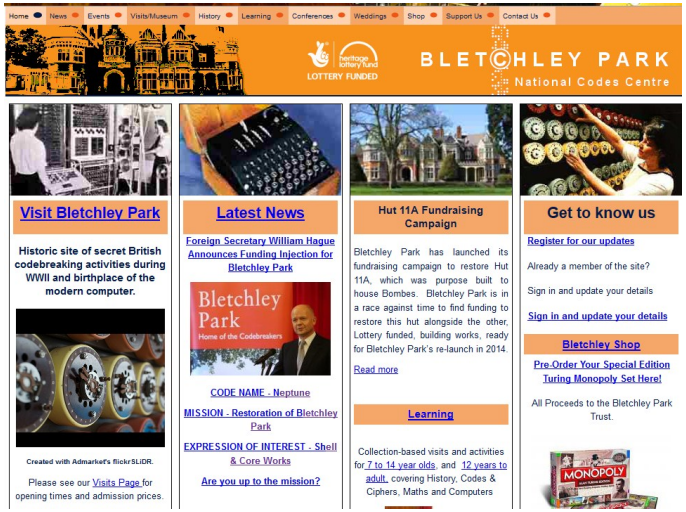


. . . a Bletchley Park

. . . a Bletchley Park

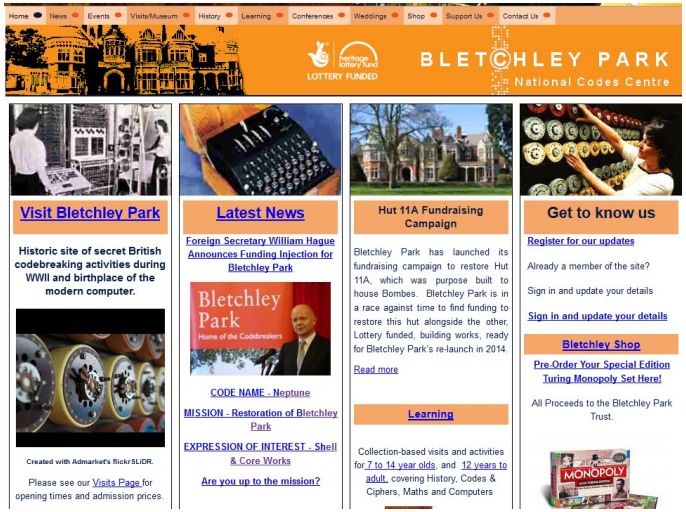


. . . a Bletchley Park



"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.

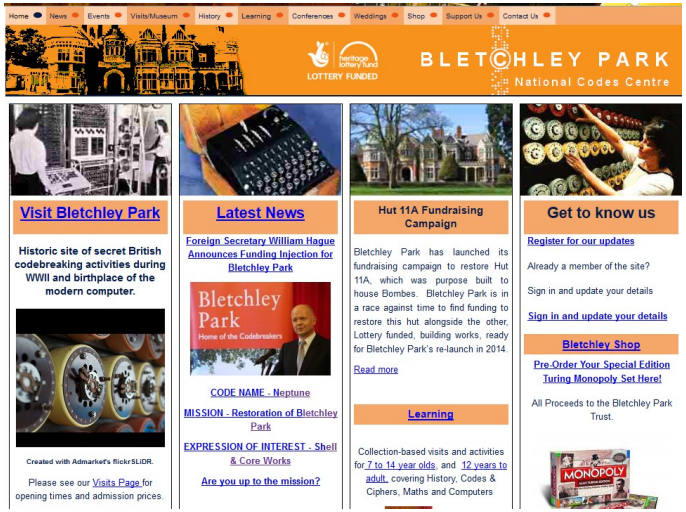
. . . a Bletchley Park



"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)

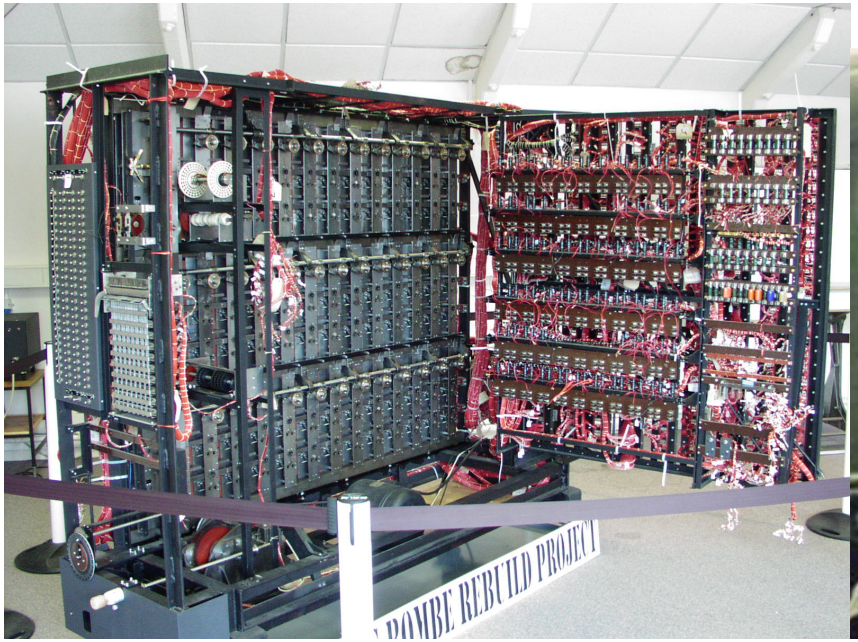
Alan Turing ebbe un ruolo cruciale nel team per la decrittazione dell'Enigma, la "macchina da cifra" impiegata dall'esercito e dalla marina tedesca (e, in seguito, ad esportare in USA le tecniche sviluppate).

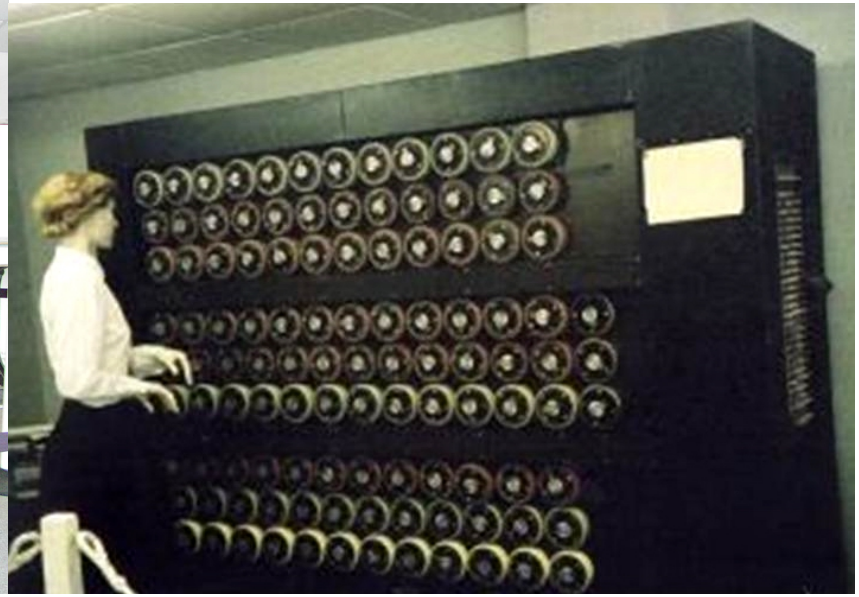
Enigma: attacco

- 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 (attacco *forza bruta*)





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

Quando si fermano un operatore verifica se il msg ha senso o è un false stop.

Se conosciamo il messaggio (crib) allora l'arresto equivale all'identificazione della chiave.

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 anche "shark", 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 anche "shark", l'ENIGMA a 4 rotori usato dai sommergibili.
  Oltre ad averci aperto il mondo dell'informatica che caratterizza la nostra vita quotidiana, Turing è stato fondamentale per la vittoria degli alleati nella seconda guerra mondiale che ha permesso l'attuale civiltà.

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 (=21,3,8,13,4). 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
21	3	8	13	4	21	3	8	13	4	21	3	8	13	4	21	3	8	13	4
9	9	14	21	15	22	14	12	12	12	8	17	12	17	17	9	11	22	5	5
J	J	O	V	P	W	O	M	M	M	I	R	M	R	R	J	L	W	F	F

Testo in cifra: JJOVPWOMMMMIRMRRJLWFF
(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= 21,3,8,13,4 = 10101, 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
10101	00011	01000	01101	00100	10101	00011	01000	01101	00100
11011	00101	01110	00101	01111	10100	01000	01100	10100	01100
♢	F	O	F	P	U	Q	M	U	M

O	N	E	E	N	O	I	O	S	A
01101	01110	00100	00100	01101	01110	01000	01110	01010	00001
10101	00011	01000	01101	00100	10101	00011	01000	01101	00100
01000	01101	01100	01001	01001	11011	01011	00110	00111	00101
I	N	M	J	J	♢	L	G	H	F

Testo in cifra: ♢FOFP UQMUM INMJJ ♢LGHF

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.

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. (cifrario perfetto–C. E. Shannon)

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. (cifrario perfetto–C. E. Shannon)
- Come comunichiamo la chiave?

Il cifrario perfetto

La linea rossa

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




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.

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.

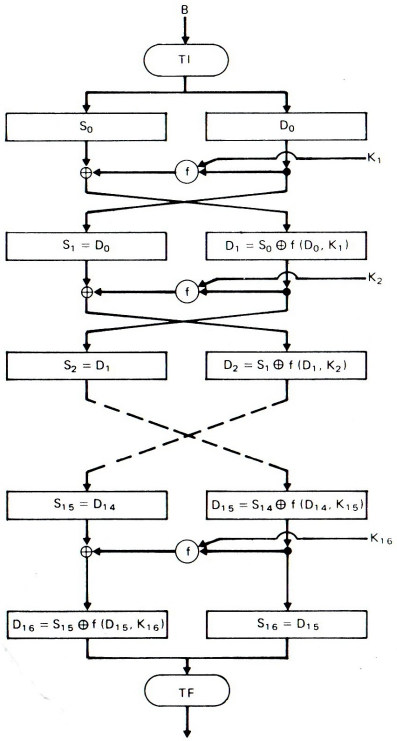
Crittografia informatica

Crittografia informatica

- Si deve assumere il principio diKerckhoffs nella sua forma più stringente: l'algoritmo per la cifrazione/decifrazione dev'essere pubblico.
- In pratica, è a disposizione di chiunque (in rete) un *codice sorgente* (p.es., un programma C) che implementa la codifica (e uno per la decodifica, eventualmente lo stesso)
- La chiave (meglio se non troppo lunga) va tenuta invece segreta.
- Il codice dev'essere attaccabile solo dalla *forza bruta* e anche mettendo assieme molti calcolatori il tempo necessario ad applicare la forza bruta dev'essere disarmante!
- Dev'essere veloce (comunicazioni riservate anche telefoniche)!

Data Encryption Standard

- 1973 il National Bureau of Standards (ora NIST) richiede un algoritmo standard di cifratura
- 1975 IBM (Horst Feistel et al) definisce il codice che nel 1976/77 diventa DES (Data Encryption Standard)
- Il funzionamento del DES è pubblico (soddisfa il principio di Kerckhoffs).
- Del DES tutto è noto tranne la chiave, costituita da 8 bytes, ove un bit per byte è un bit di controllo (desumibile dalla chiave).
- Dunque la vera lunghezza della chiave è 56 bits (spazio di $2^{56} \approx 7.2 \times 10^{16}$).



Data Encryption Standard

Qualche numero e la fine del DES

- Malgrado anni e anni di studi non si arrivò mai a metodi più intelligenti della forza bruta
- $2^{56} \approx 7.2 \cdot 10^{16}$
- Supponiamo di saper testare una chiave in $1\mu s$
- Dunque sapremmo verificare $10^6 \cdot 60 \cdot 60 \cdot 24 = 8.64 \cdot 10^{10}$ chiavi al giorno.
- Farebbero circa 834 000 giorni (2285 anni)
- Ma se avessimo 100 000 calcolatori, basterebbero 8 giorni!

Data Encryption Standard

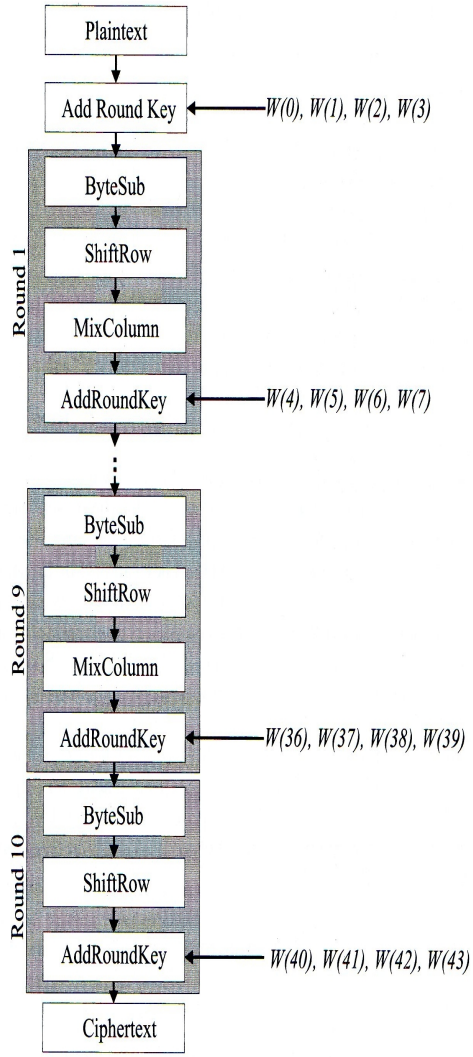
Qualche numero e la fine del DES

- Malgrado anni e anni di studi non si arrivò mai a metodi più intelligenti della forza bruta
- $2^{56} \approx 7.2 \cdot 10^{16}$
- Supponiamo di saper testare una chiave in $1\mu s$
- Dunque sapremmo verificare $10^6 \cdot 60 \cdot 60 \cdot 24 = 8.64 \cdot 10^{10}$ chiavi al giorno.
- Farebbero circa 834 000 giorni (2285 anni)
- Ma se avessimo 100 000 calcolatori, basterebbero 8 giorni!
- In seguito a una competizione, Rocke Verser preparò un programma in grado di distribuire il lavoro su PC vari collegati in Internet. Nel 1997 furono necessari 5 mesi (ovviamente con carico piuttosto irregolare) a forzare il DES. Nel 1998 bastarono 39 giorni.

Advanced Encryption Standard

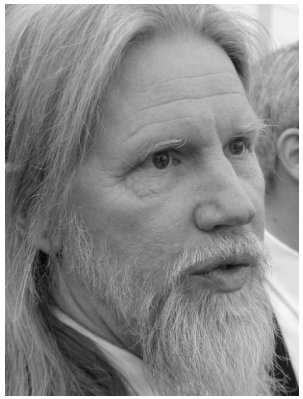
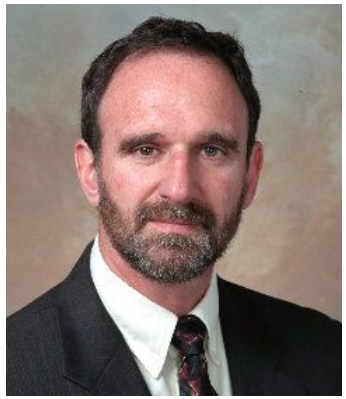
- L'algoritmo Rijndael di Joan Daemen and Vincent Rijmen fu annunciato dalla NIST come standard (AES) nel 2002

- 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.

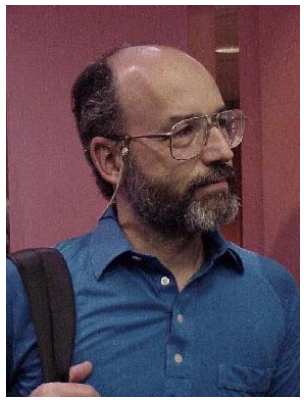
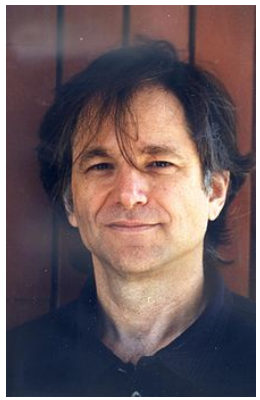


Crittografia a chiave pubblica

Idea “astratta” di Whitfield Diffie e Martin Hellman nel 1976 — Turing award nel 2016

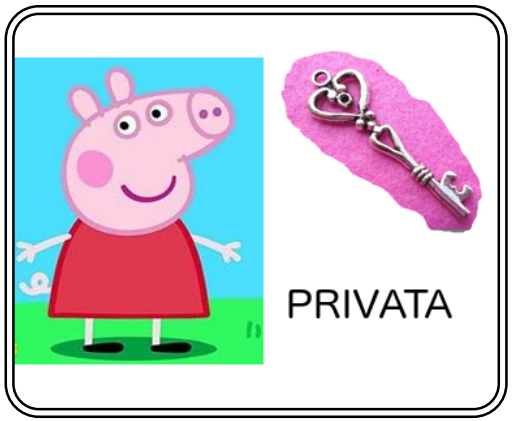



Realizzazione concreta (algoritmo “difficile”) nel 1978 di Ronald Rivest, Adi Shamir e Leonard Adleman (RSA) — Turing award nel 2002

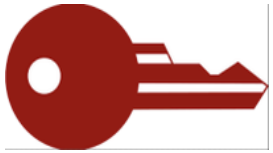
Crittografia a chiave pubblica

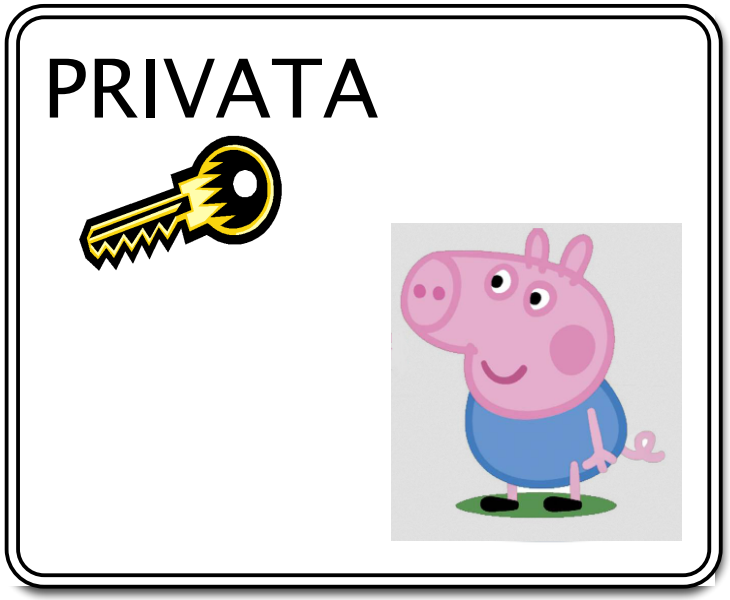
Peppa spedisce un messaggio a George



PUBBLICA

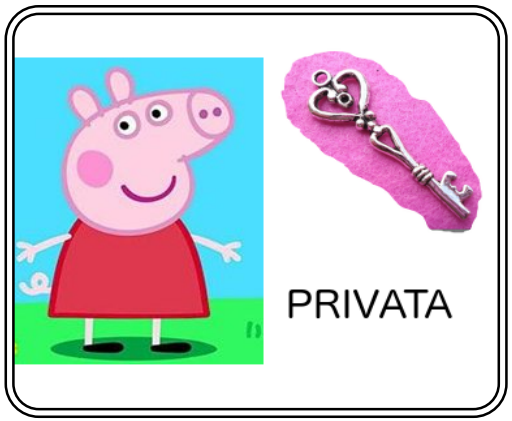
PUBBLICA



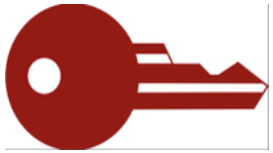


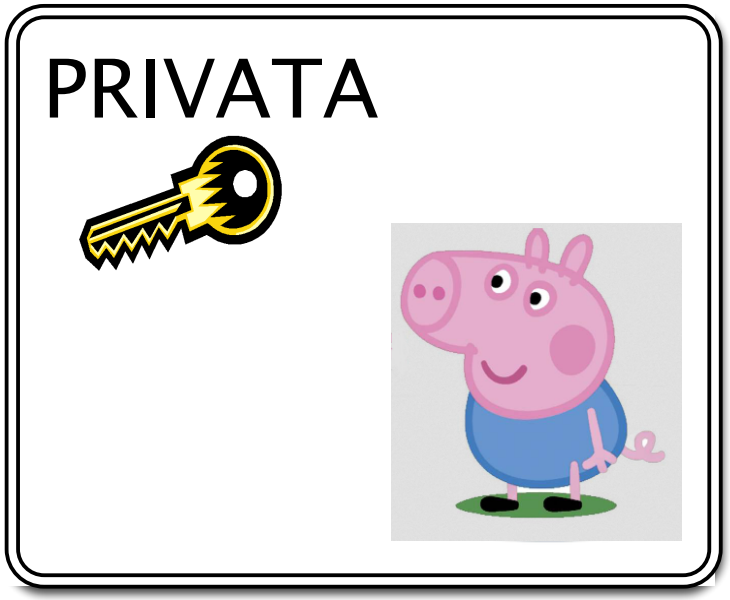
Crittografia a chiave pubblica

Peppa spedisce un messaggio a George



PUBBLICA

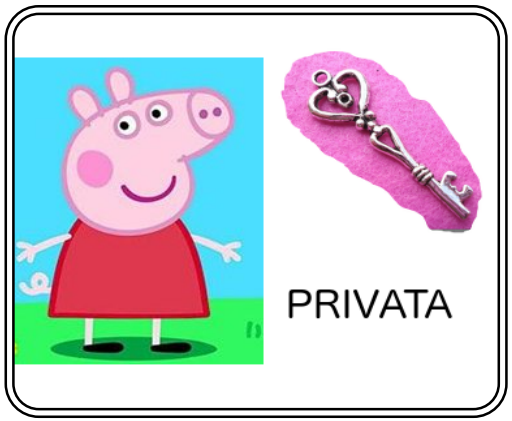




CIAO

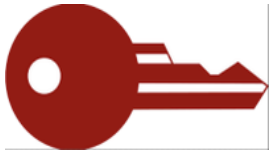
Crittografia a chiave pubblica

Peppa spedisce un messaggio a George



PUBBLICA

PUBBLICA



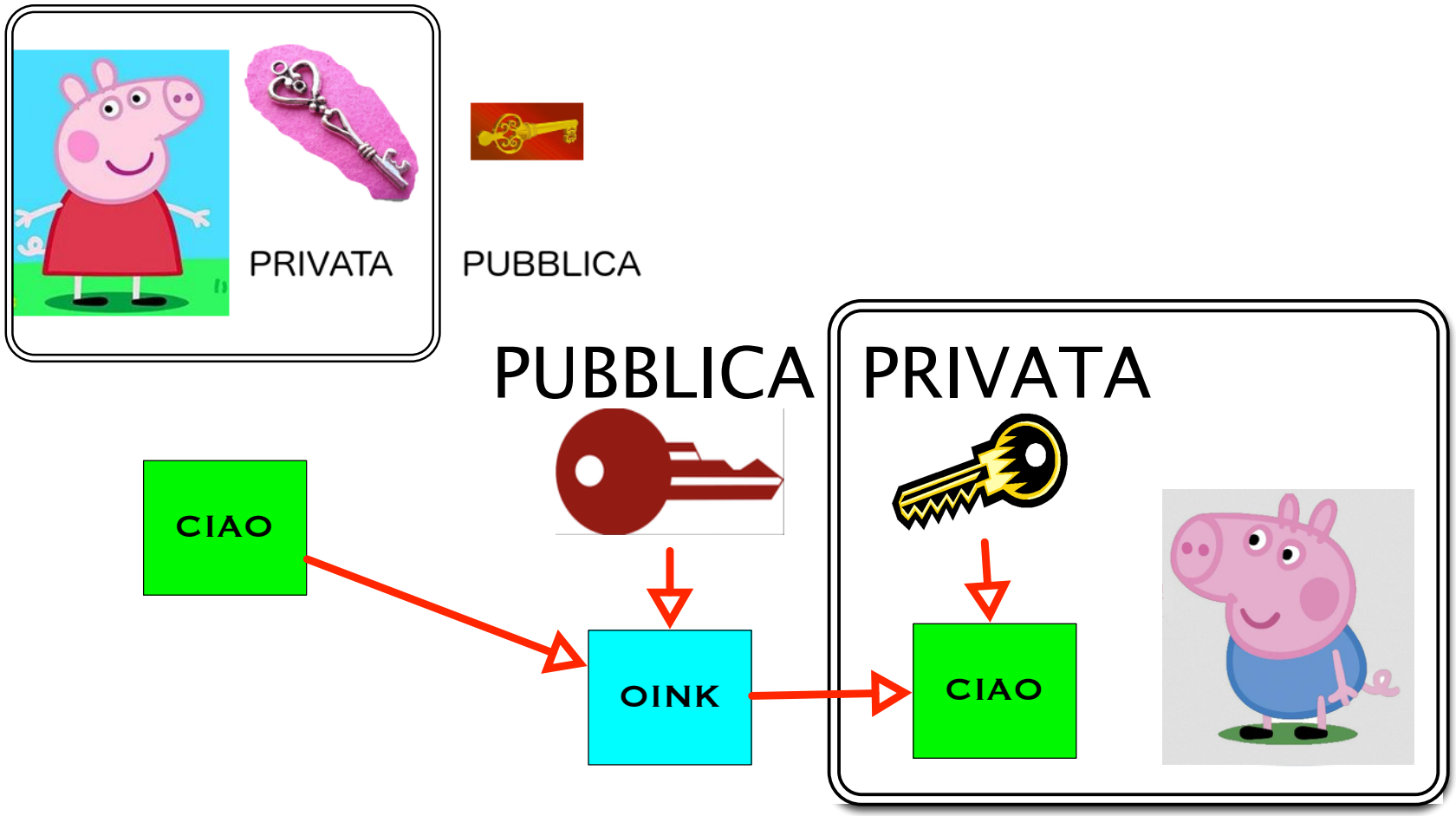
CIAO

OINK

PRIVATA

Crittografia a chiave pubblica

Peppa spedisce un messaggio a George



Crittografia a chiave pubblica

Idee generali

- L'operazione di decifrazione, sapendo la chiave privata dev'essere algoritmicamente facile
- L'operazione di decrittazione (per la spia) deve essere algoritmicamente impraticabile.
- Anche se l'impresa è possibile, avendo tempo a sufficienza: un modo è quello di provare tutti i messaggi di una data lunghezza, codificarli con la chiave pubblica di George, quando inseriamo CIAO, troveremo OINK: abbiamo capito che Peppa ha scritto CIAO.
- Così si scopre il messaggio ma non la chiave privata.

Crittografia a chiave pubblica

La sicurezza mondiale è basata su una scommessa

trova un fattore di n:
prova i da 2 a $\sqrt{n}$
se n diviso i ha resto 0
allora stampa i e finisci
(altrimenti aumenta i)

Crittografia a chiave pubblica

La sicurezza mondiale è basata su una scommessa

trova un fattore di n:
  prova i da 2 a $\sqrt{n}$
    se n diviso i ha resto 0
    allora stampa i e finisci
    (altrimenti aumenta i)

Nel caso peggiore compie un numero di passi pari a $\sqrt{n}$.
Se n è un numero di 100 cifre, ogni divisione mi costa $10^{-10}s$, e dispongo di 10^9 processori, mi serve tempo

$$\approx \frac{10^{-10}\sqrt{10^{100}}}{3600 \cdot 24 \cdot 365 \cdot 10^9} = 3 \cdot 10^{23} \text{ANNI}$$

Crittografia a chiave pubblica

La sicurezza mondiale è basata su una scommessa

trova un fattore di n:
  prova i da 2 a $\sqrt{n}$
    se n diviso i ha resto 0
    allora stampa i e finisci
    (altrimenti aumenta i)

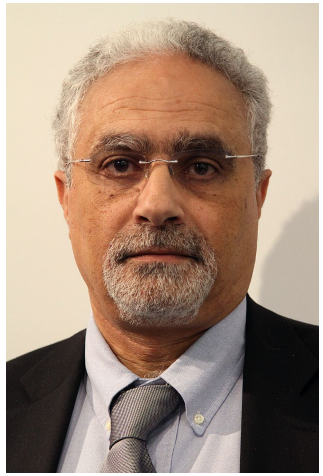
Nel caso peggiore compie un numero di passi pari a $\sqrt{n}$.
Se n è un numero di 100 cifre, ogni divisione mi costa $10^{-10}s$, e dispongo di 10^9 processori, mi serve tempo

$$\approx \frac{10^{-10}\sqrt{10^{100}}}{3600 \cdot 24 \cdot 365 \cdot 10^9} = 3 \cdot 10^{23}\text{ANNI}$$

Ma nessuno ha mai dimostrato che non si può fare in un altro modo!

Elgamal e il logaritmo discreto

- Nel 1985 Taher Elgamal architetta un altro sistema di cifratura a chiave pubblica.
- La forza del sistema di cifratura è basata sulla difficoltà computazionale di calcolare il logaritmo in un campo finito (in breve *logaritmo discreto*).



Elgamal e il logaritmo discreto

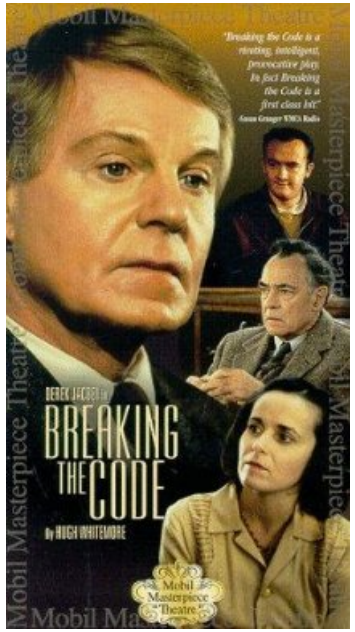
Una nuova scommessa

- Considerate $\mathbb{Z}_p$ con p numero primo e considerate l'aritmetica modulo p (ovvero se il risultato a di una operazione è $\geq p$ prendiamo il resto della divisione tra a e p).
- Ad esempio, in $\mathbb{Z}_7$, $2 \cdot 6 = 12 \equiv_7 5$,
  $3^1 = 3$ $\quad 3^2 = 9 \equiv_7 2$, $\quad 3^3 = 27 \equiv_7 6$,
  $3^4 = 81 \equiv_7 4$ $\quad 3^5 = 3^4 \cdot 3 \equiv_7 4 \cdot 3 \equiv_7 5$ $\quad 3^6 = 3^5 \cdot 3 \equiv_7 5 \cdot 3 \equiv_7 1$
- Cosideriamo ora due numeri α e x (numeri tra 1 e $p-1$, α meglio se radice primitiva come 3 nell'esempio sopra).
- Calcoliamo $\beta = \alpha^x$ modulo p (non è difficile farlo in modo efficiente).
- Dati α, β e p, trovare x è possibile ma, ancora, computazionalmente impraticabile (se p è un numero di 200 cifre o più).

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/`

Generali sulla crittografia:

- Andrea Sgarro. Codici segreti. 1989 (Mondadori)
- Simon Singh. Codici & segreti. La storia affascinante dei messaggi cifrati dall’antico Egitto a Internet. 2001. (BUR Biblioteca Univ. Rizzoli)