

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

Agostino Dovier

Dip di Matematica e Informatica, CLP Lab, Univ. di Udine

03/14/15

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)

← Rembrandt: 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 ב ל

Babel/Babilonia

ש ש כ

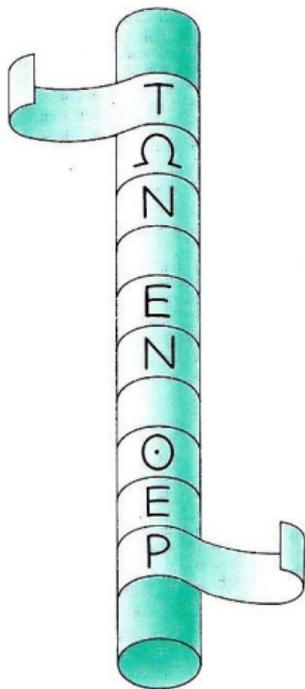
Sheschach



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 (\approx 400 AC) — trasposizione



Α	Τ	Μ	Α	Κ	Α
Ω	Ω	Ο	Ν	Λ	
Ν	Π	Ο	Ε	Τ	
	Υ	Ν	Η	Υ	
Ε	Λ	Τ	Ξ	Χ	
Ν	Α	Ω		Α	
	Ι	Ν	Μ		
Ο	Ξ		Ε		
Ε		Ε	Ν		
Ρ	Ο	Υ			

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

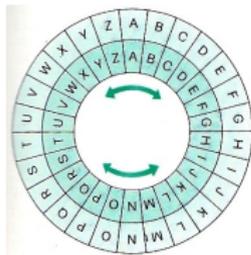
Cifrari a sostituzione monoalfabetica

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

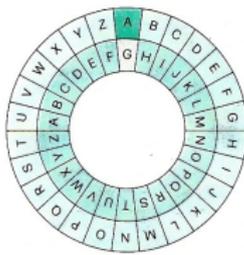
- La “chiave” segreta è la lettera iniziale (la D per Cesare).
- Anche ammettendo che la spia conosca il tipo di codifica usata (Principio di Kerckhoffs 1835–1903) deve essere difficile per lei/lui identificare tale la chiave.
- Ci sono una ventina di chiavi: il codice è troppo debole.

Cifrari a sostituzione monoalfabetica

Macchine di cifra



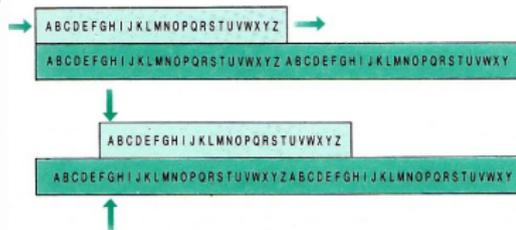
L.B. Alberti
(1404–1472)



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 $\{A, \dots, Z\}$.

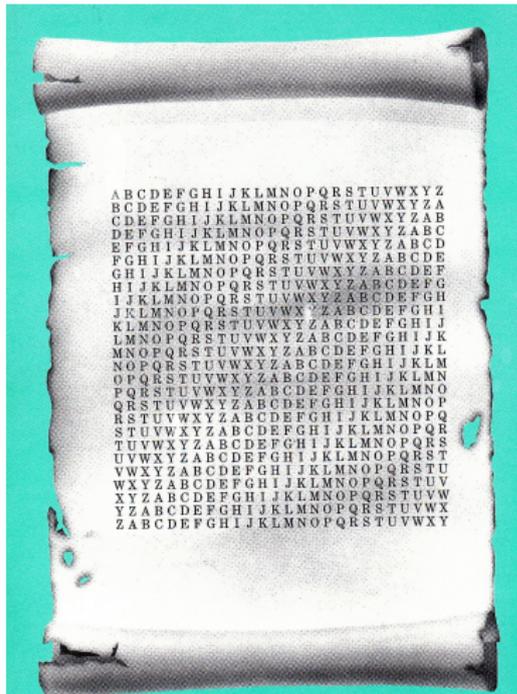
A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
M	V	F	T	H	C	K	L	D	N	O	P	Q	R	A	G	E	X	S	B	I

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

Edgar Allan Poe. **Lo scarabeo d'oro** (1843)

Cifrari a sostituzione polialfabetica

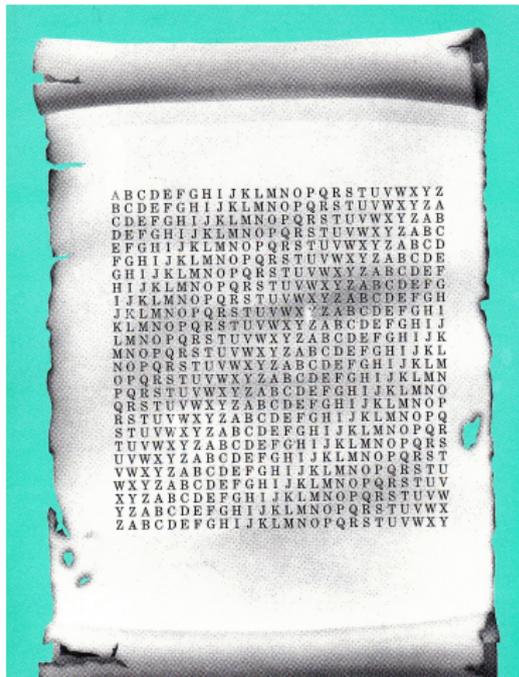
Blaise de Vigenère (1523–1596)



Cifrari a sostituzione polialfabetica

Cifrazione

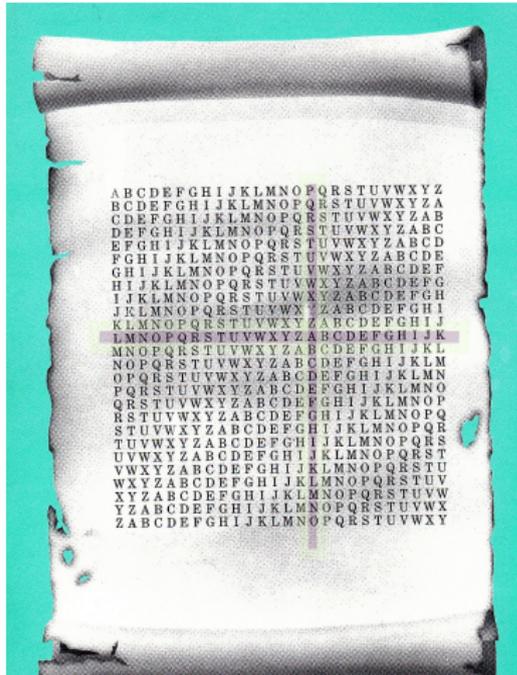
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

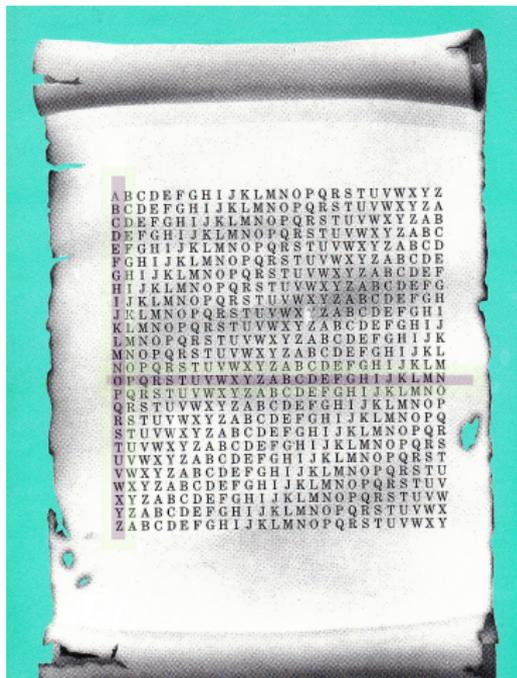
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

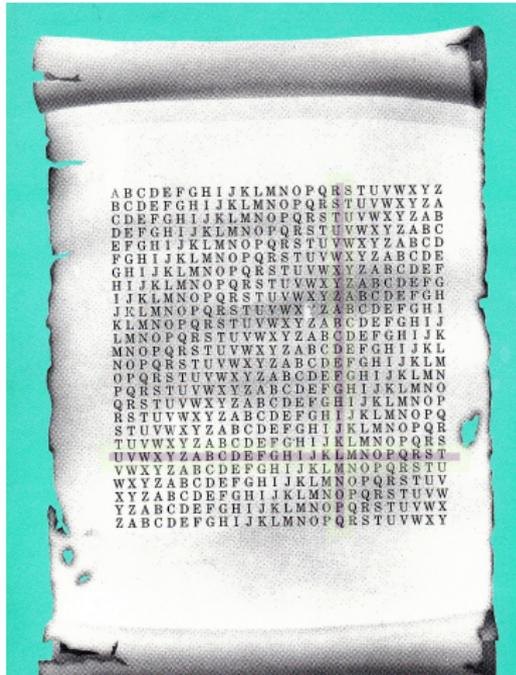
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

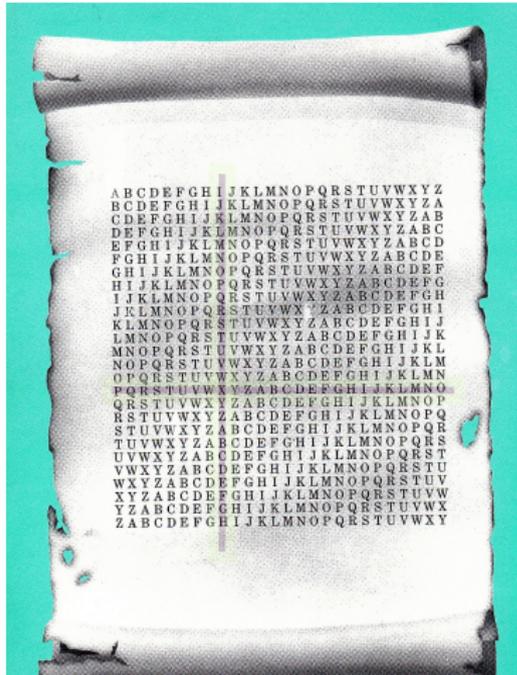
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



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

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

- Anche se su ogni lettera della chiave ci sono solo 21 scelte, in tutto ce ne sono ben $21^n = \underbrace{21 \cdot 21 \cdot \dots \cdot 21}_n$.
- 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

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvtvtjgtsgnuctsgtsgtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsгнуctsgtsgtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsгнуctsgtsgtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsгнуctsgtsgtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsгнуctsgtsgtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvtjgtsгнуctsgtsgtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvtjgtsгнуctsgtsgtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsgtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsgtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvtvjgtsгнуctsgtsgtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvtvjgtsгнуctsgtsgtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsгнуctsgtsgtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsгнуctsgtsgtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsгнуctsgtsqtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsгнуctsgtsqtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsгнуctsgtsgtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsгнуctsgtsgtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Decrittazione

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvtvjgtsgnuctsgtsgtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvtvjgtsgnuctsgtsgtugrfnlbpdp

Cifrari a sostituzione polialfabetica

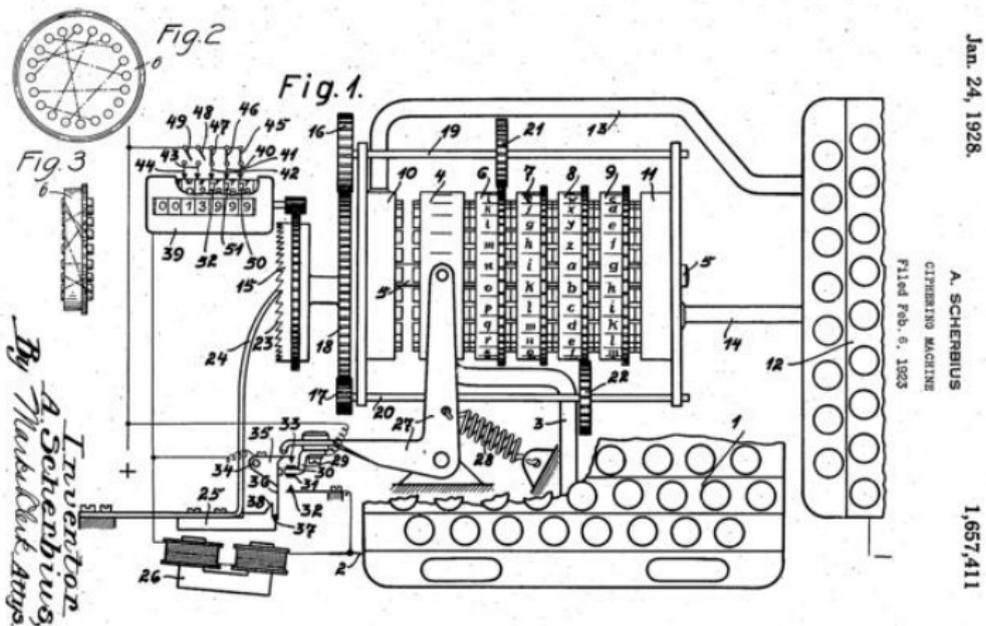
Decrittazione e limiti

- 1 Con l'allineamento visto, si determina la lunghezza della parola chiave.
- 2 Congettata 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.

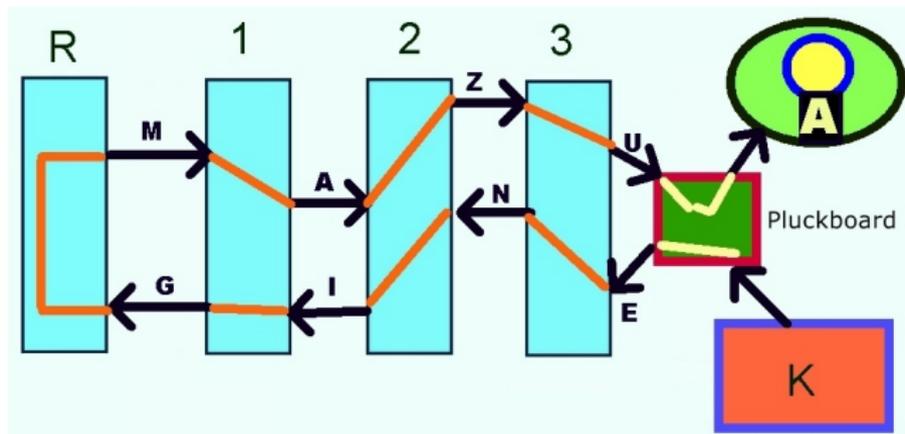


Enigma: funzionamento

- 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

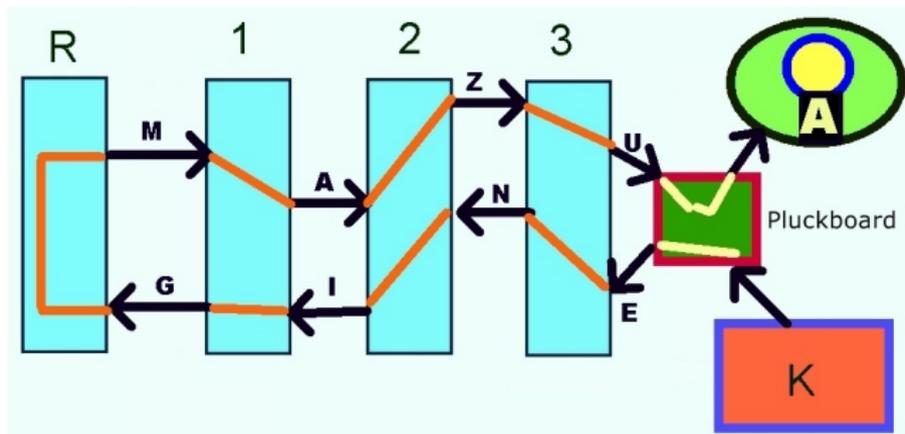
È una macchina a rotori **non fissi** che si muovono con moto **odometrico** dopo ogni lettera codificata—stepping motion (come i vecchi contachilometri o i contatori dell'acqua o del gas).



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

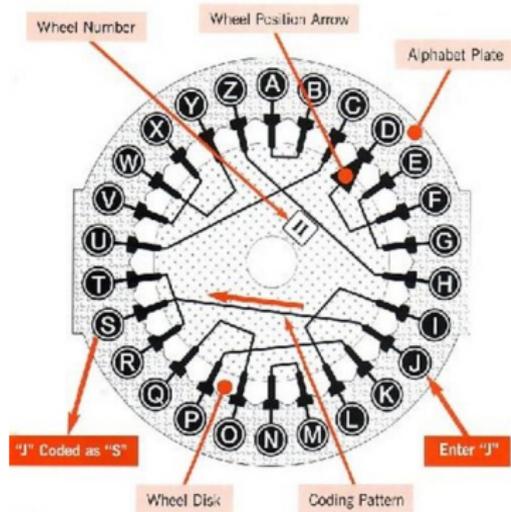
Enigma: funzionamento

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 ($k = 1, \dots, 13$) abbiamo:

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

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 cumbersome 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

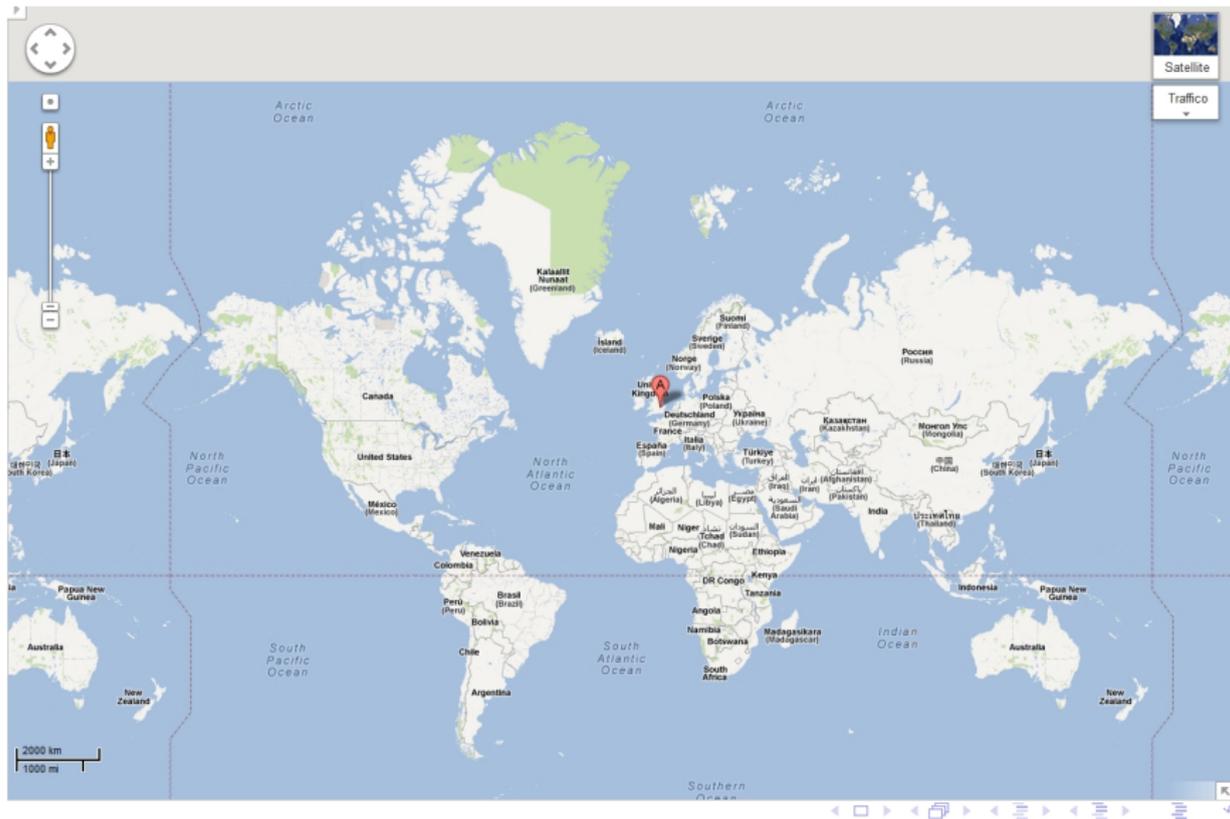
The Amateur Athletic Association championships for this year were concluded at Loughborough College Stadium, Leicestershire, on Saturday, with the second, and last, day of the Decathlon and the decision of the Marathon championship.

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. 31min. 20-1-5sec., 1; T. Richards (South London Harriers), 2hrs. 36min. 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.~~

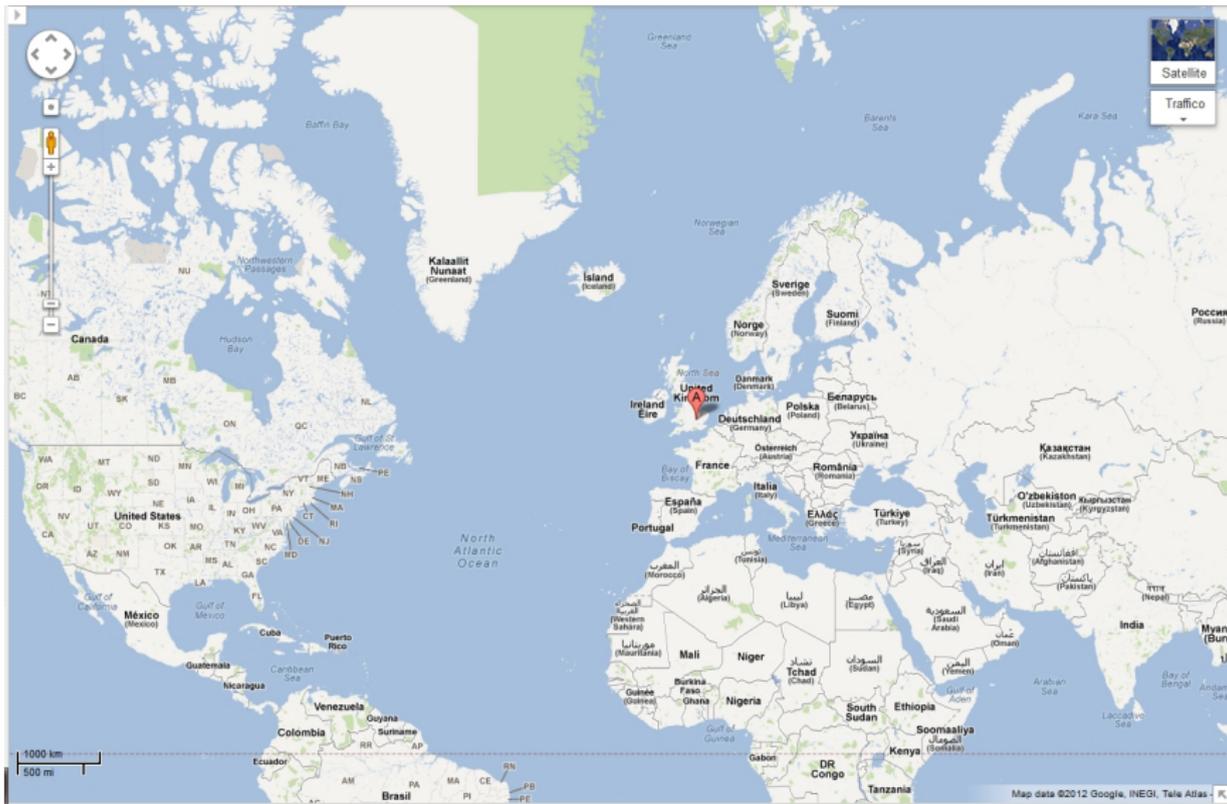
DECATHLON CHAMPIONSHIP.—H. J. Moesgaard-Kjeldsen (Polytechnic Harriers, London), 5,965 points, 1; Captain H. Whittle (Army and Reading A.C.), 5,650, 2;

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

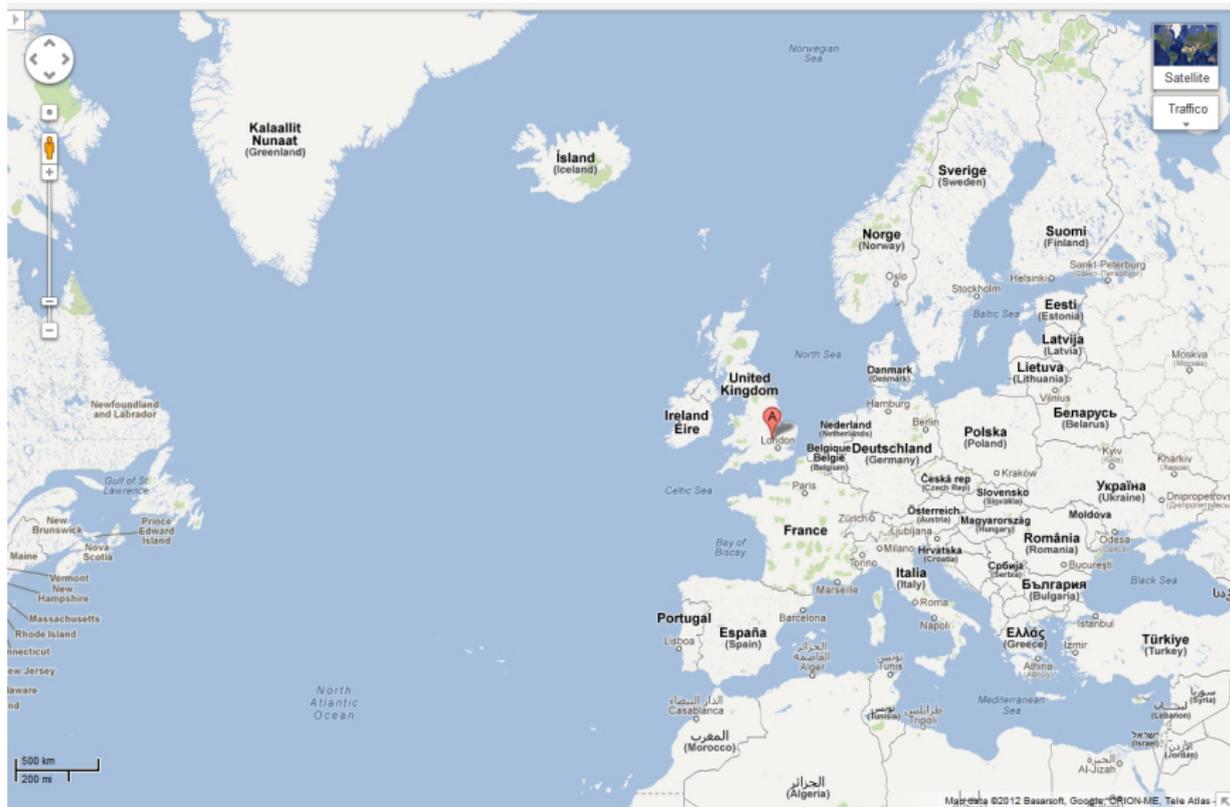
... a Bletchley Park



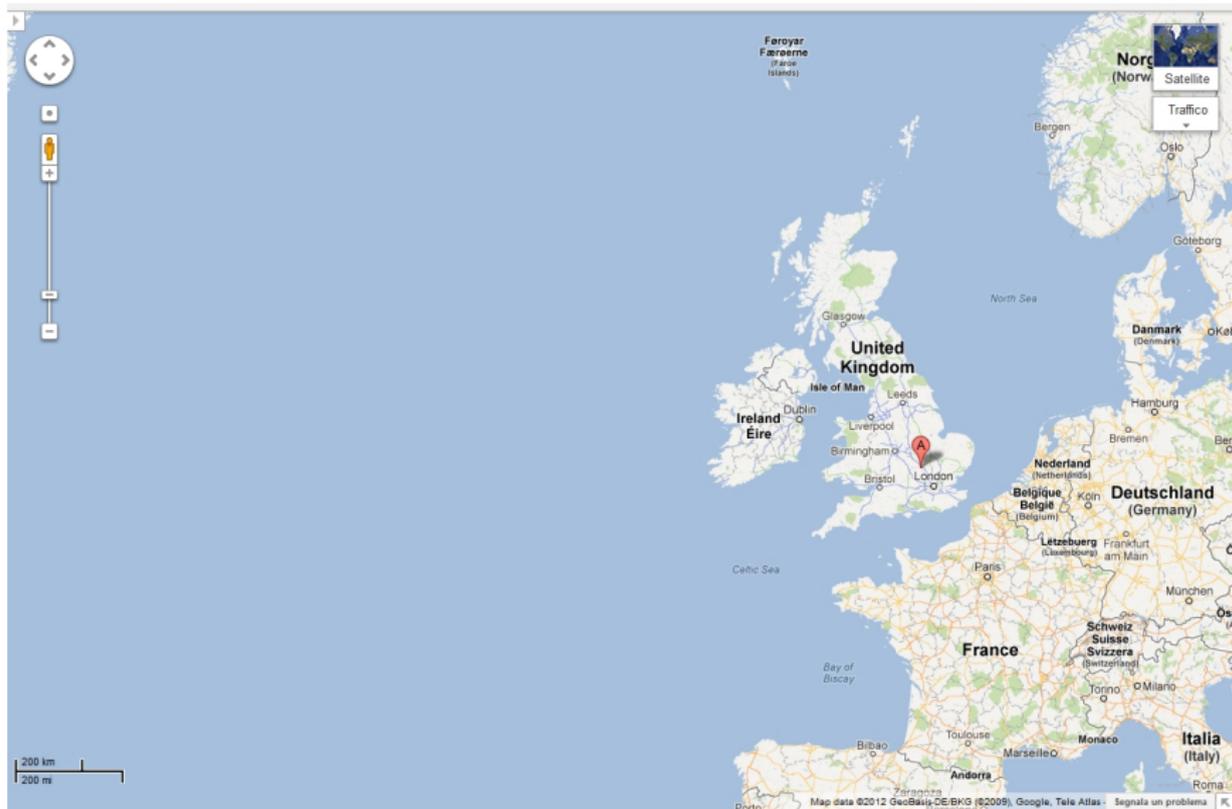
... a Bletchley Park



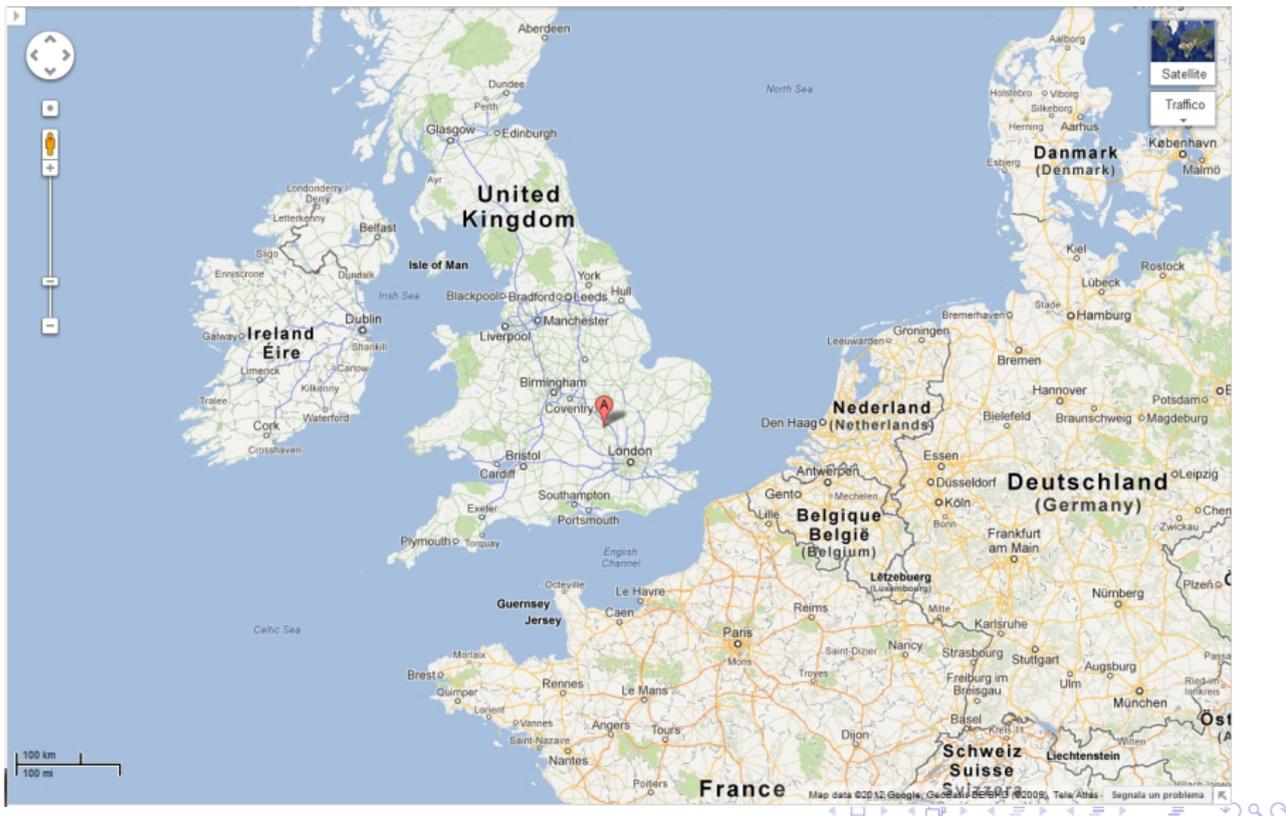
... a Bletchley Park



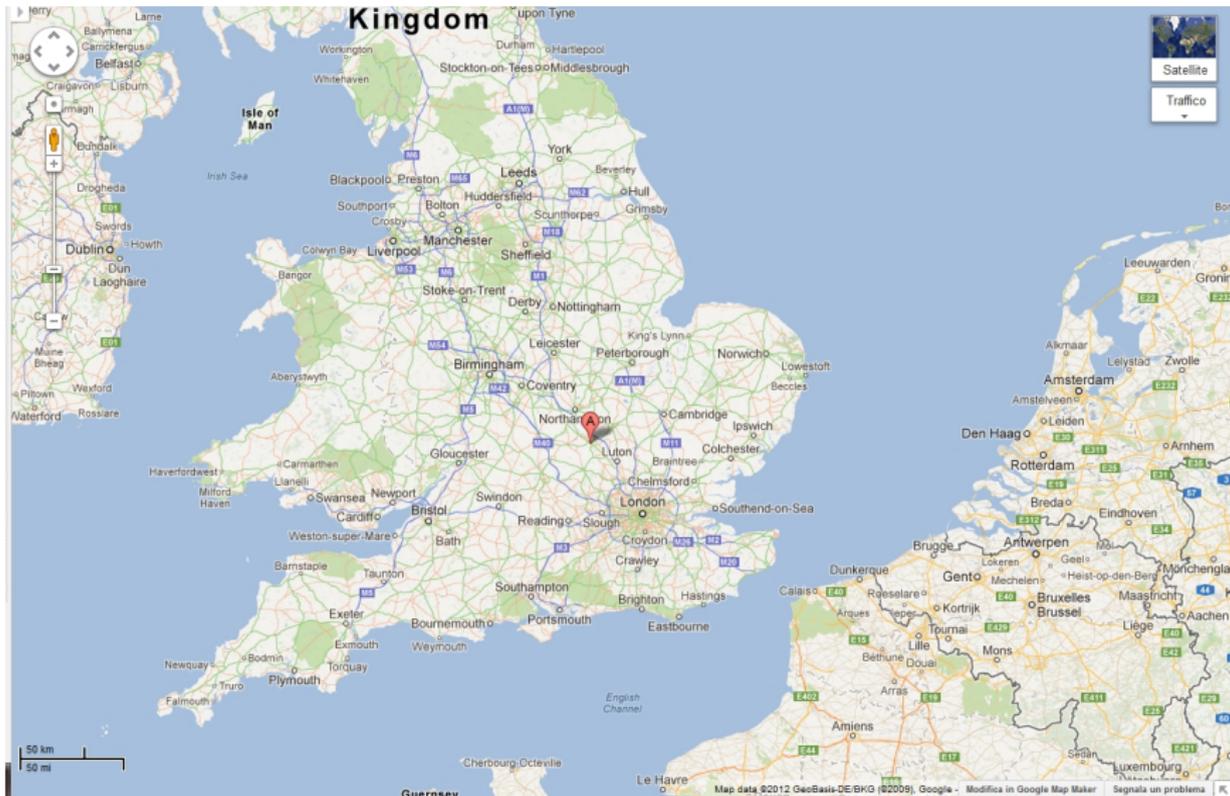
... a Bletchley Park



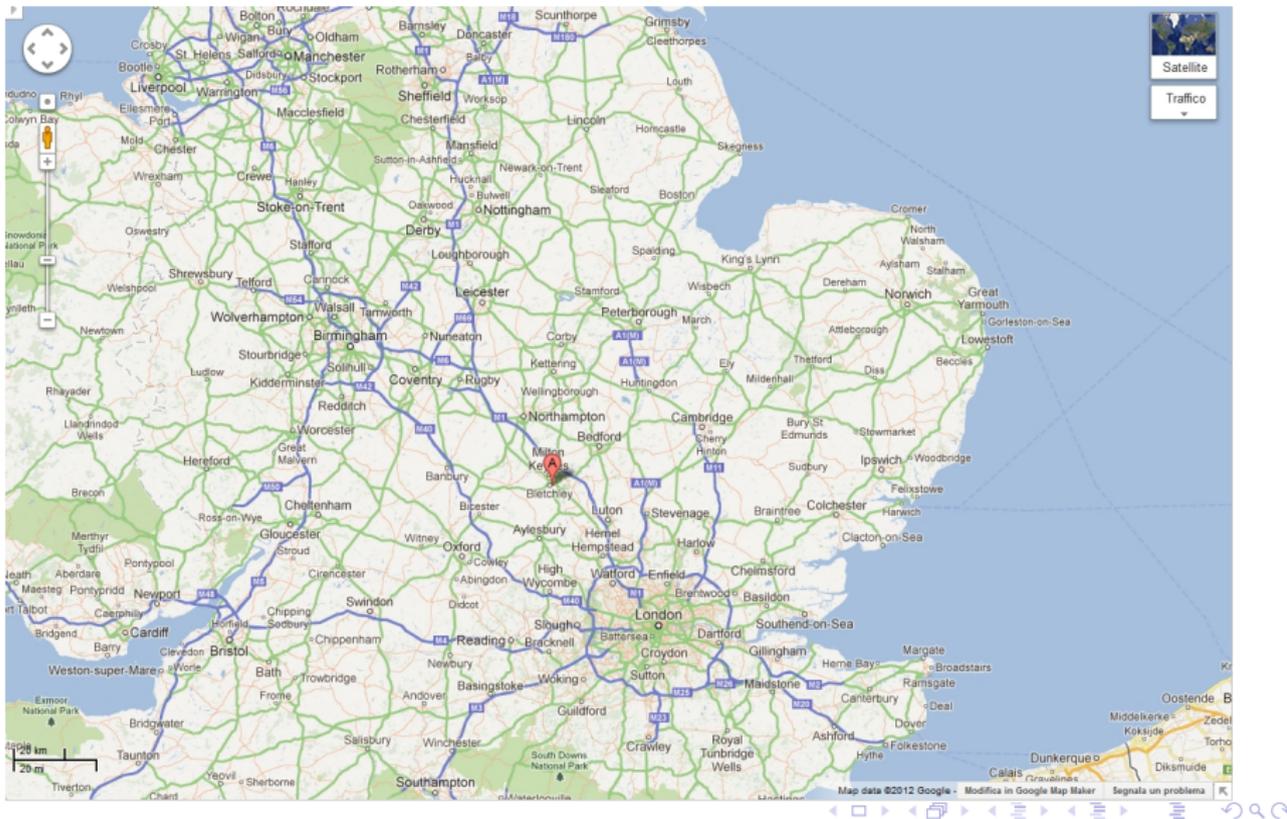
... a Bletchley Park



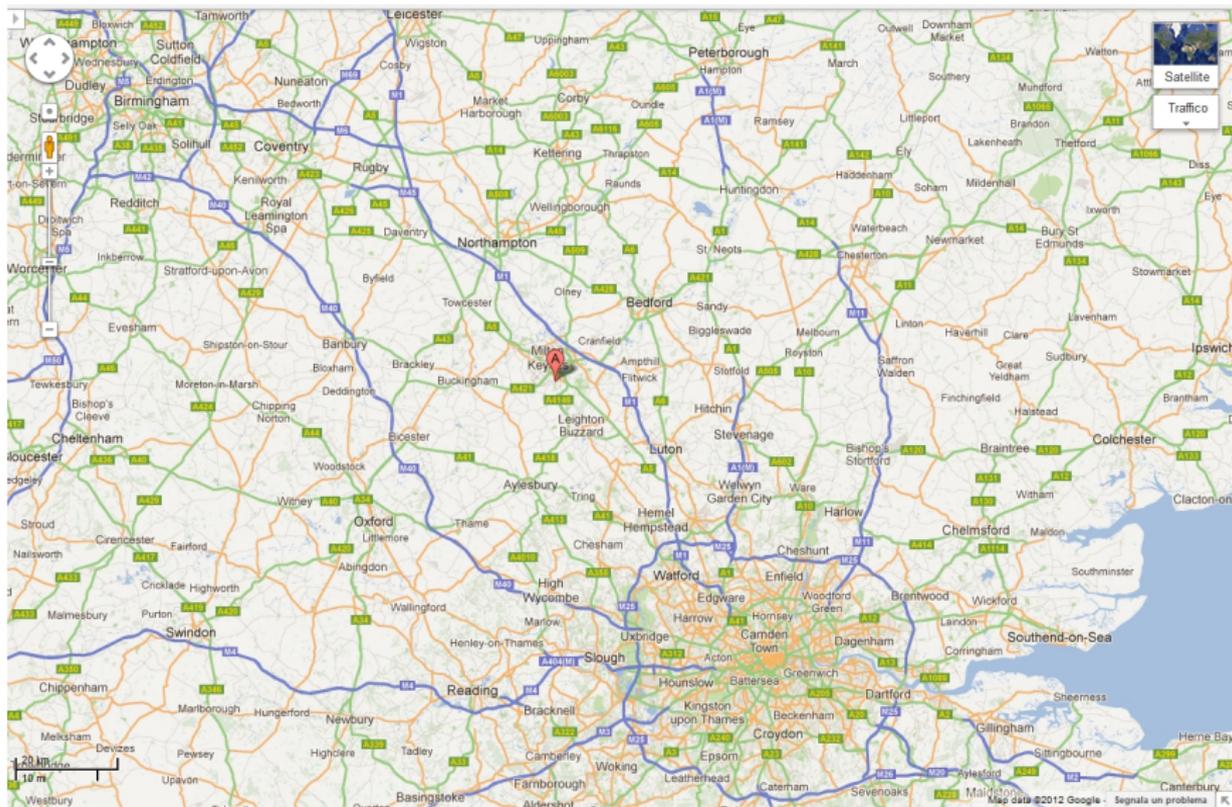
... a Bletchley Park



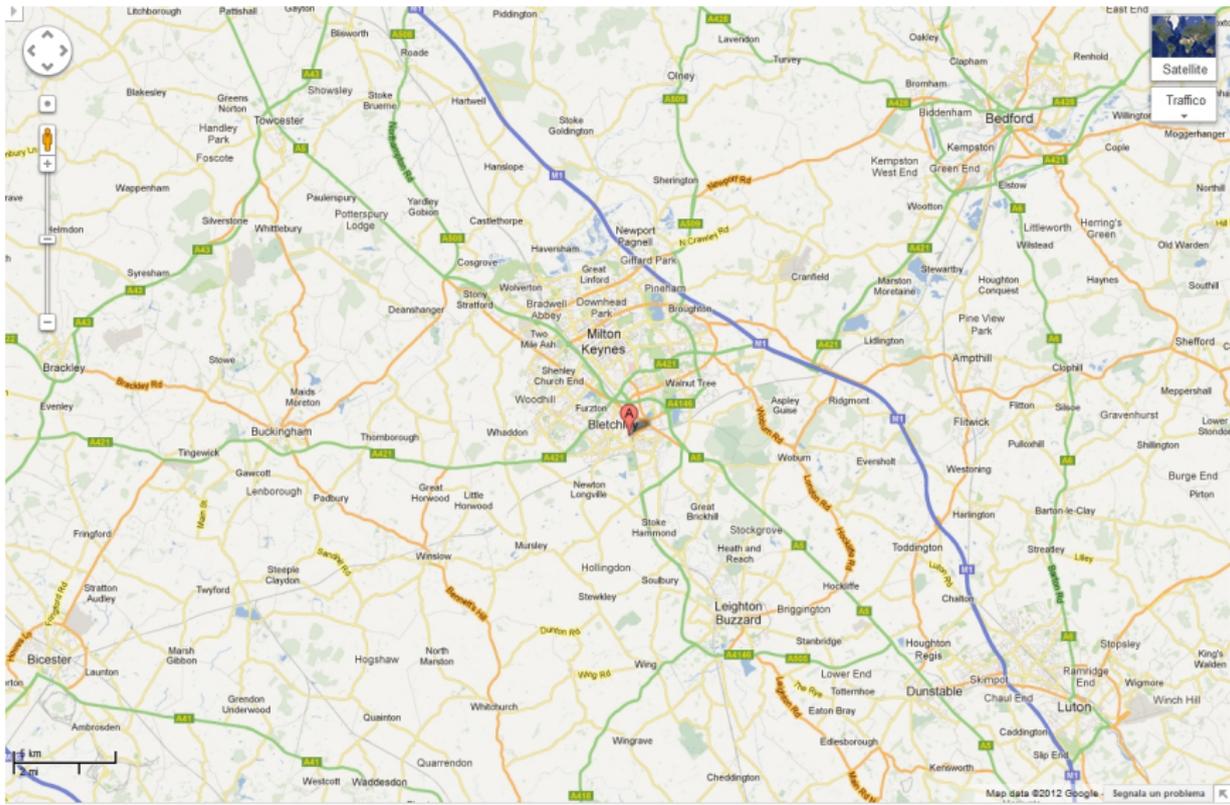
... a Bletchley Park



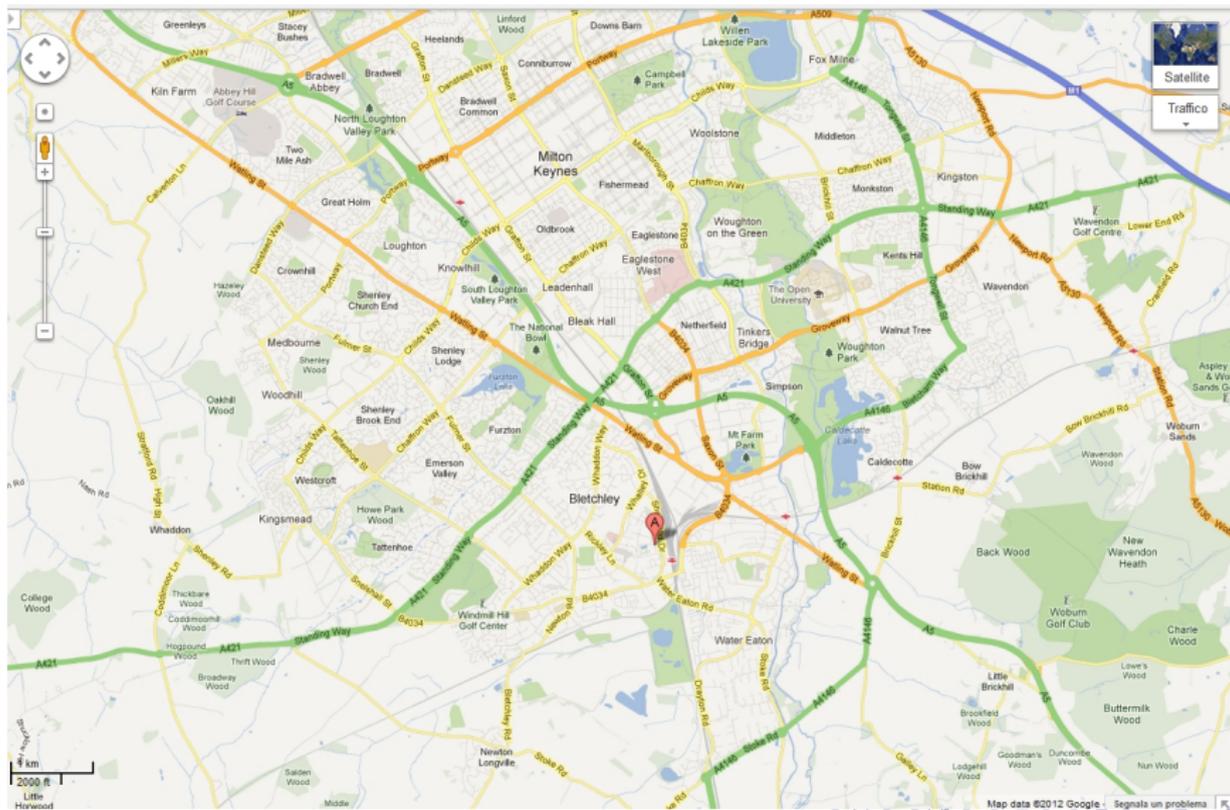
... a Bletchley Park



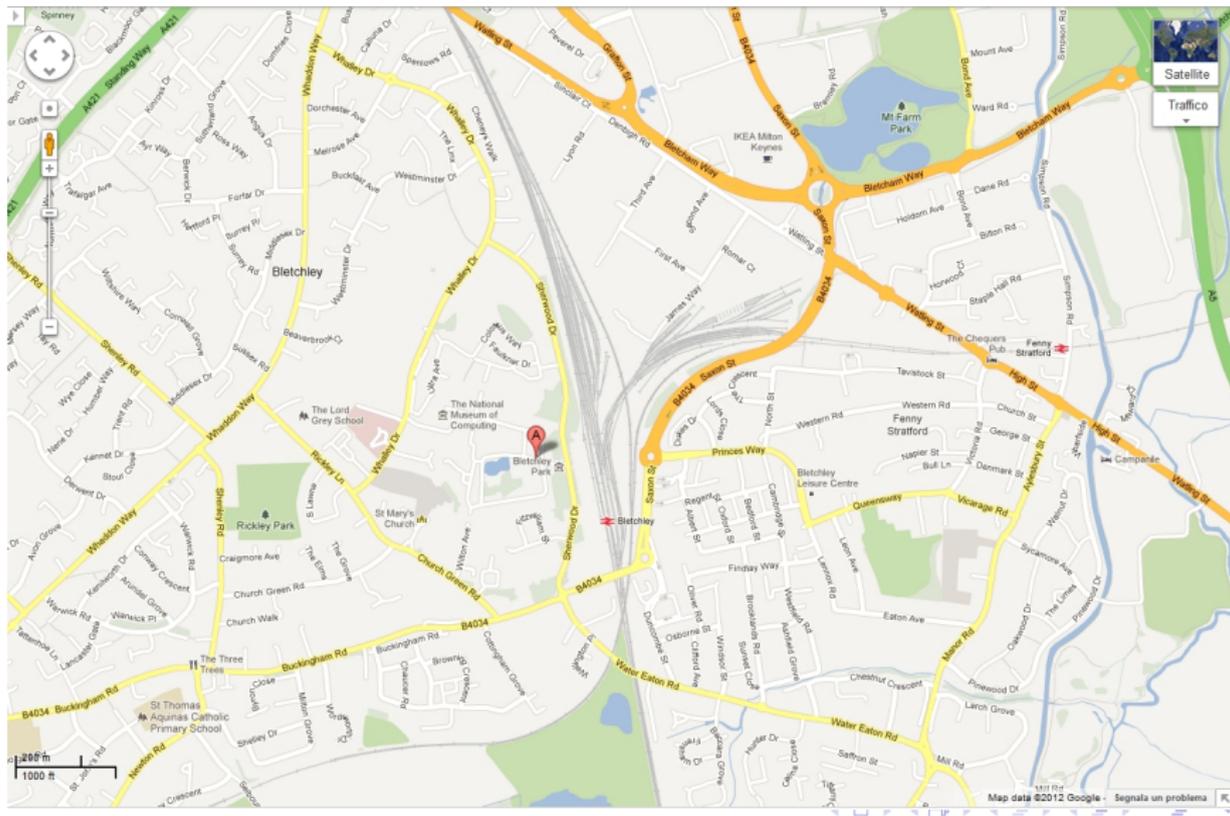
... a Bletchley Park



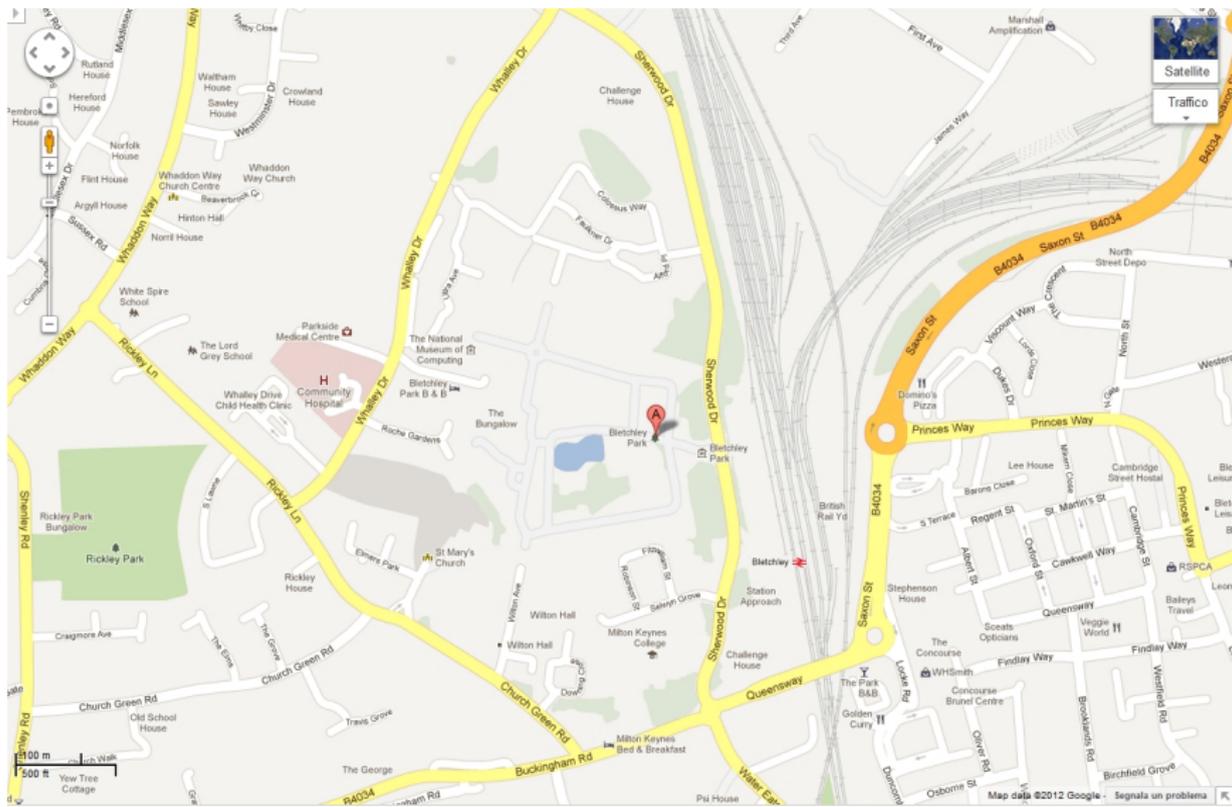
... a Bletchley Park



... a Bletchley Park



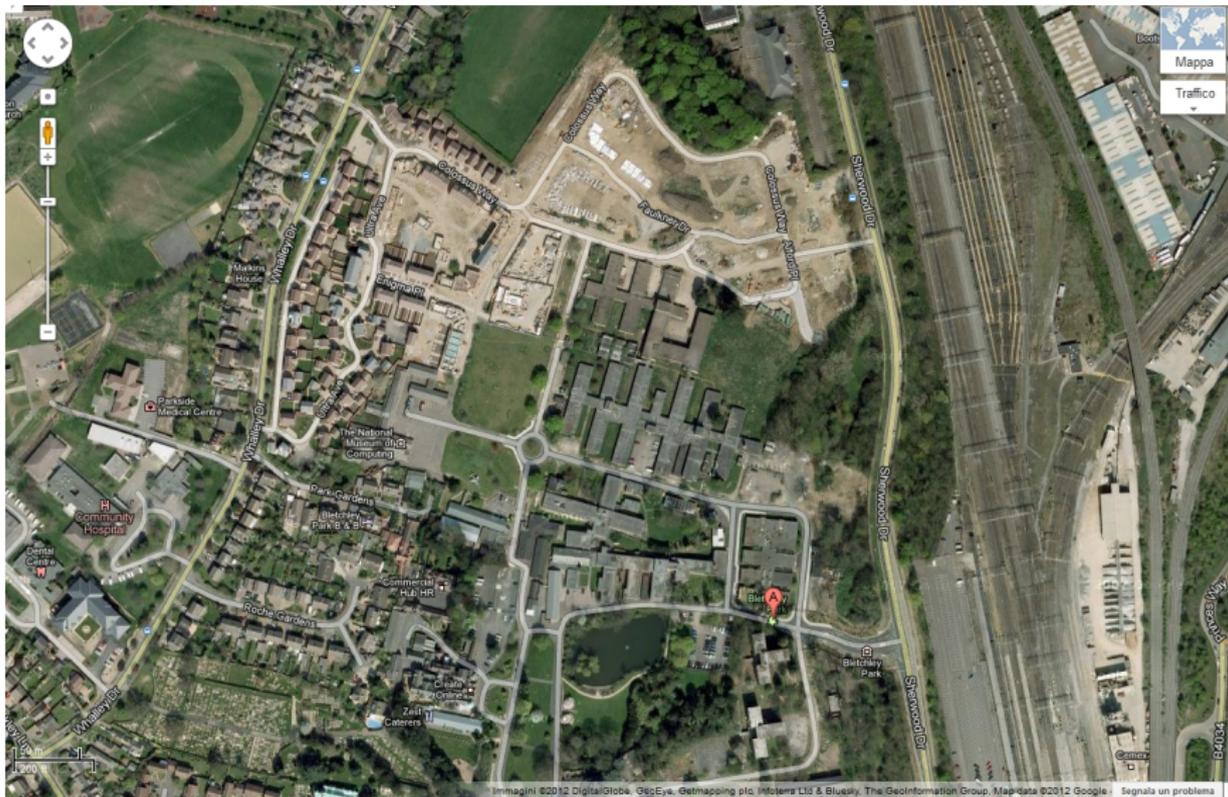
... a Bletchley Park



... a Bletchley Park



... a Bletchley Park



... a Bletchley Park

HOME ABOUT VISITING CONTACT DONATE SHOP SUPPORT LINKS

LETTER PUMPS

BLETCHLEY PARK
National Codes Centre

Visit Bletchley Park
Historic site of secret British codebreaking activities during WWII and birthplace of the modern computer

Latest News
Foreign Secretary William Hague Announces Funding Initiative for Bletchley Park

Get to know us
Register for our website
Already a member of the site?
Sign in and update your details
[Sign in and update your details](#)

Bletchley Shop
The Codes Store Special Edition During Membership Set Day

Learning
Collection-based visits and activities for 2 to 16 year olds, and 12 years to adult, covering History, Codes & Cyphers, Maths and Computers

© 2014 Bletchley Park
All Proceeds to the Bletchley Park Trust

“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

[Visit Bletchley Park](#)
 Historic site of secret British codebreaking activities during WWII and birthplace of the modern computer.

[Latest News](#)
 Foreign Secretary William Hague Announces Funding Visit to Bletchley Park

[The TTA Fundraising Campaign](#)
 Bletchley Park has launched its fundraising campaign to restore the TTA, which was purpose built to house Bletchley Park in its race against time to beat Enigma to restore their site alongside the other Lottery funded, building works, ready for Bletchley Park to re-launch in 2012.

[Get to know us](#)
 Register for our website
 Already a member of the site?
 Sign in and update your details
[Sign in and update your details](#)

[Bletchley Shop](#)
 The Codes Store Special Edition During Monday Set Day
 All Proceeds to the Bletchley Park Trust.

[EXPLOSION OF INTEREST - 2011](#)
 A Code Exhibit
[Are you up to the challenge?](#)

Collection-based data and activities for 2.5m 3d game sets, over 12 years in total, covering History, Codes & Cyphers, Maths and Computers.

“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

Visit Bletchley Park

Historic site of secret British codebreaking activities during WWII and birthplace of the modern computer

Latest News

Enigma Secretary William Tutte Secret-Breaking Activities for Bletchley Park

The TMA Fundraising Campaign

Bletchley Park has launched its fundraising campaign to reach the £11A, which was purpose built to house Bletchley Park in a race against time to get ready to restore this site alongside the other Lottery funded, building works, ready for Bletchley Park to re-opens in 2012

Get to know us

Register for site updates

Already a member of the site? Sign in and update your details

Sign in and update your details

Bletchley Shop

The Codes Store Special Edition During Monday Set Day

All Proceeds to the Bletchley Park Trust

Events

Collection-based talks and activities for 2 to 24 year olds, with 12 years to 1800, covering History, Codes & Cyphers, Maths and Computers

Contact Us

ENTER OUR ADDRESS HERE WITH PLEASE USE OUR VISIT PAGE FOR OPENING TIMES AND ADDRESS PLEASE

FAQs

EXPRESSION OF INTEREST - 2012

8,500,000

REASON: Reopening of Bletchley Park

Are you up to the challenge?

“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)

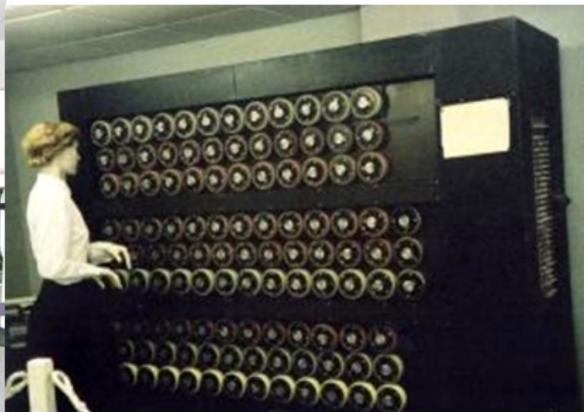
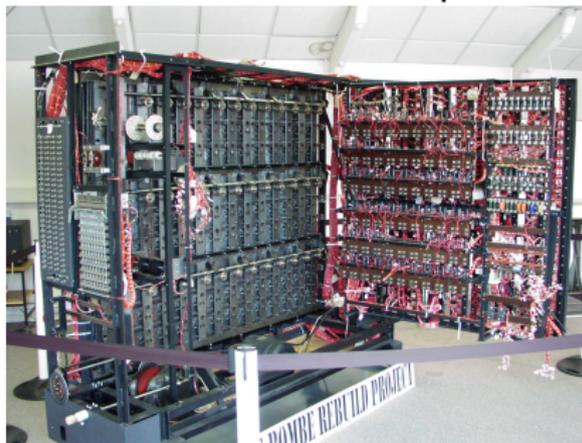
Alan Turing ebbe un ruolo cruciale nel team per la decrittazione dell’Enigma, la “macchina da cifra” impiegata dall’esercito e dalla marina tedesca (e, in seguito, ad esportare in USA le tecniche sviluppate).

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:

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

- 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.

Crittografia informatica

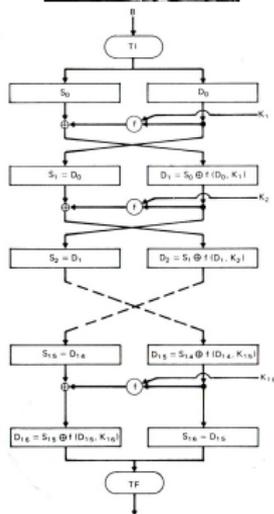


Crittografia informatica

- Si deve assumere il principio di Kerckhoffs 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 $1\mu\text{s}$
- 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, Roche 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.

Crittografia a chiave pubblica

Idea “astratta” di Whitfield Diffie e Martin Hellman nel 1976

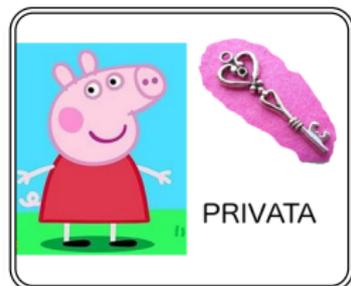


Realizzazione concreta (algoritmo “difficile”) nel 1978 di Ronald Rivest, Adi Shamir e Leonard Adleman (RSA) — Turing award 2002



Crittografia a chiave pubblica

Peppa spedisce un messaggio a George



PUBBLICA

PUBBLICA

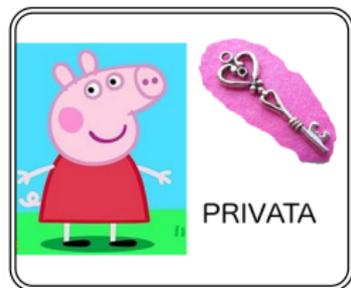


PRIVATA



Crittografia a chiave pubblica

Peppa spedisce un messaggio a George



PUBBLICA



PUBBLICA

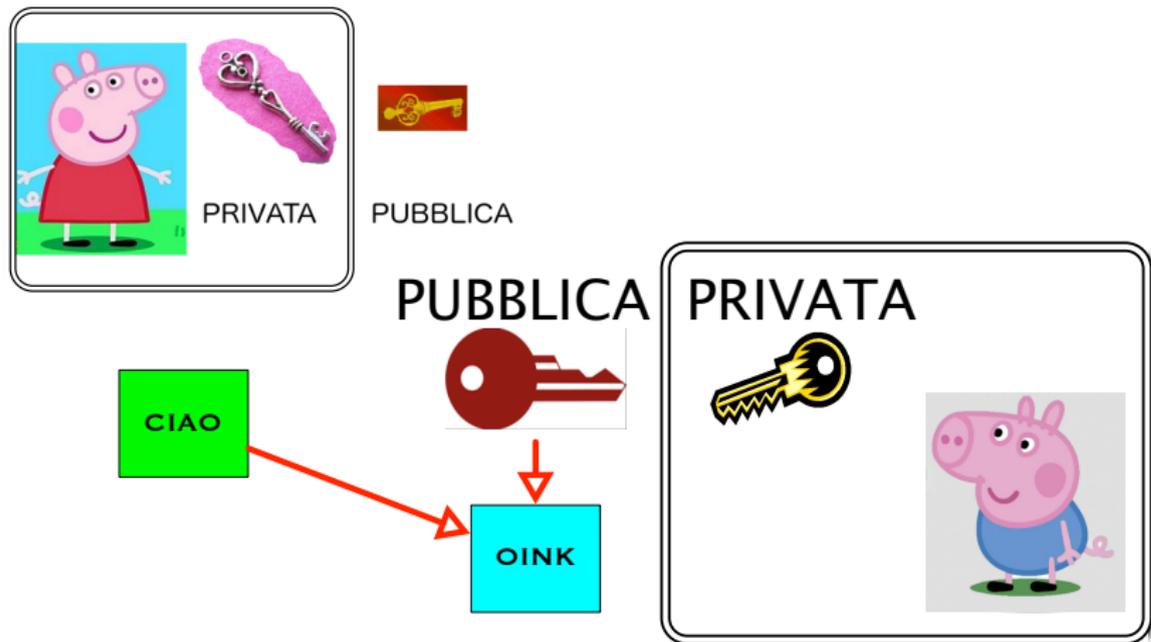


PRIVATA



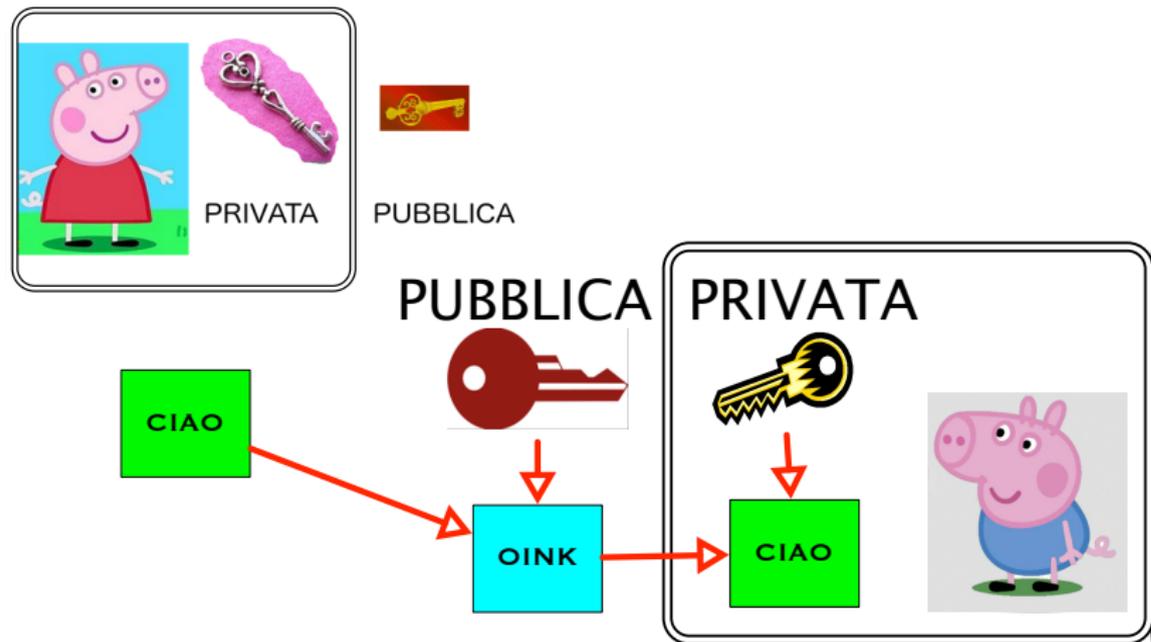
Crittografia a chiave pubblica

Peppa spedisce un messaggio a George



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!

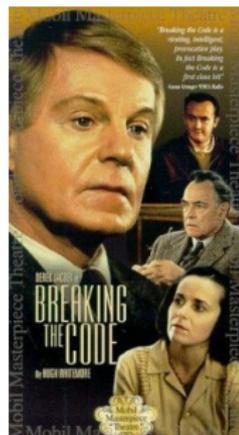
Films 'su' Turing



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)

