

LABORATORIO



NUMERI E CRITTOGRAFIA

Conferenza di presentazione

Francesca Tovina

20 settembre 2018



Piano Lauree Scientifiche

In collaborazione con MIUR, con.Scienze, Confindustria

PROBLEMA

- Comunicare in modo segreto e sicuro
- Inviare messaggi cifrati che possano essere letti rapidamente dai destinatari, ma non da chi non è autorizzato.

Il problema è estremamente attuale: lo sviluppo dei sistemi elettronici facilita le comunicazioni, ma le rende vulnerabili se non vengono adeguatamente protette.

LA CRITTOGRAFIA

È l'arte (o una scienza?) che studia come rendere segreta e sicura la comunicazione tra due persone o entità nascondendo il significato del messaggio



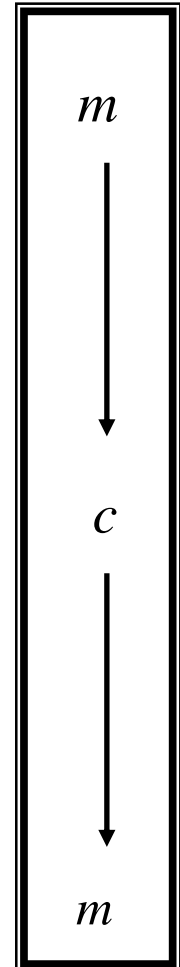
A

canale insicuro



B

- Supponiamo che A voglia mandare a B un messaggio m (detto **messaggio in chiaro**)
- A **cifra** il messaggio m ottenendo un messaggio c (detto **messaggio cifrato**) che invia a B
- B riceve c e lo **decifra** riottenendo il messaggio m



- **Il processo di cifratura deve poter essere invertito**, in modo da permettere di ritrovare il messaggio originale
- Chi riceve il messaggio c deve essere in grado di interpretare (“**decifrare, decriptare**”) c
- A e B si devono mettere d’accordo prima su come “cifrare” e “decifrare”, scegliendo un metodo efficace

Segretezza: il messaggio non deve essere leggibile a terzi.

Autenticazione: il destinatario deve poter essere sicuro di chi sia il mittente.

Integrità: il destinatario deve poter essere sicuro che il messaggio non sia stato modificato.

La scacchiera di Polibio

Nel libro X delle Storie,
(circa 200-118 a. C.)
Polibio attribuisce ai
suoi contemporanei
Cleoxeno e Democleito
l'introduzione di un
sistema di
telecomunicazione
(telegrafo ottico
trasmesso con due
gruppi di 5 torce)
qui adattato all'alfabeto
italiano, con l'aggiunta
di alcuni segni di
interpunzione

A	B	C	D	E
F	G	H	I	L
M	N	O	P	Q
R	S	T	U	V
Z	.	,	:	?

La scacchiera di Polibio è la base per un **cifrario a colpi**. Ogni lettera è rappresentata dalla coppia di numeri che indica la sua posizione nella scacchiera, cominciando dalla prima riga:

B è 12, P è 34, V è 45

Il messaggio viene battuto lasciando una pausa più breve tra i due numeri che si riferiscono ad una lettera e una pausa più lunga tra una lettera e l'altra.

DOMANI PIOVE

143331113224 3424334515

A	B	C	D	E
F	G	H	I	L
M	N	O	P	Q
R	S	T	U	V
Z	.	,	:	?

Decifrate:

11 32 14 11 43 15 11 13 11 34 33 52

A N D A T E A C A P O .

Abbiamo usato:

- **Alfabeto del messaggio in chiaro**
- **Alfabeto del messaggio cifrato**
- Una **corrispondenza biunivoca tra i due alfabeti**, definita dalla forma della scacchiera e dalla distribuzione dell'alfabeto in essa (tale scelta è detta "chiave")

Caratteristiche:

- Una lettera viene cifrata sempre allo stesso modo (cifrario monoalfabetico)
- La regola che mi permette di cifrare mi spiega anche come decifrare (e viceversa)

IL CRITTOSISTEMA DI CESARE

Svetonio, nella Vita dei dodici Cesari, racconta che Giulio Cesare utilizzava un sistema di cifrazione molto semplice: ogni lettera va sostituita con quella che si trova tre posti dopo

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

Ad esempio la frase

domani attaccheremo (testo in chiaro),

diventerà

GR P D Q N D Z Z D F F M H U H P R

- La crittografia fornisce **metodi effettivi** per effettuare cifratura e decifratura dei messaggi
- **Il processo di trasformazione dal messaggio in chiaro al messaggio cifrato e viceversa è spesso noto, ma si basa su una informazione specifica (detta “chiave”), senza la quale non si è in grado di operare**
- I metodi di cifratura si sono estremamente evoluti nell’arco della storia

CRITTOANALISI

- “What a man can invent, another can discover” (A. C. Doyle)

CRITTOANALISI

- studia come decifrare un messaggio senza esserne “autorizzati”
- ha il ruolo fondamentale di far capire quanto un sistema di cifratura/decifratura sia sicuro.

Riflettiamo sulla frase deccriptata:

11 32 14 11 43 15 11 13 11 34 33 52
A N D A T E A C A P O .

- Si riconosce la lunghezza di ogni parola
- **Ogni lettera viene criptata sempre allo stesso modo** (la A compare 4 volte)
- Criptare anche i segni di interpunzione riduce la possibilità che l'ultima lettera di un blocco sia una vocale.

Il crittosistema di Cesare

La decifrazione è altrettanto semplice, basta sostituire ad ogni lettera quella che si trova tre posti prima

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
u	v	z	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t

Generalizzazione

- E' possibile **generalizzare il sistema di Cesare usando uno spostamento di k posti**, anzichè di 3.
- k deve essere un numero compreso tra 1 e 20
- Ad esempio con $k=7$

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C	D	E	F	G

La frase dell'esempio precedente diventa
domani attaccheremo
MVTHUR HDDHLLQNBNTV

Sostituzione monoalfabetica

- Il crittosistema di Cesare è un cifrario in cui la stessa lettera è codificata sempre con la stessa lettera
- Ad esempio la lettera 'a' è sempre codificata con la lettera 'D', la 'b' è codificata con 'E', ...

Sostituzione monoalfabetica

- Il caso più generale è quello in cui l'alfabeto cifrato è una permutazione di quello in chiaro
- Un modo semplice per ricordare la permutazione è quello di usare una frase

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
N	E	L	M	Z	O	D	C	A	I	S	T	R	V	B	F	G	H	P	Q	U

in questo esempio la frase è

NEL MEZZO DEL CAMMIN DI NOSTRA VITA

- Ad esempio la frase **domani attaccheremo** diventa **MRSNTA NHHNLLCZFZSR**

Sostituzione monoalfabetica

- Esistono $21! = 51.090.942.171.709.440.000$ permutazioni possibili, cioè circa $51 \cdot 10^{18}$, ossia più di *cinquanta miliardi di miliardi*
- Una ricerca esaustiva per trovare la permutazione giusta è praticamente impossibile
- Eppure questo codice è tutt'altro che sicuro...

La **crittoanalisi** nasce sostanzialmente durante l'VIII e il IX secolo d. C., quando gli **arabi** si dedicarono allo studio approfondito della lingua scritta e, tra l'altro, stabilirono le frequenze delle varie lettere. In particolare, scoprirono che **le lettere più usate erano sostanzialmente le stesse in qualsiasi testo, purché abbastanza esteso.**

Come decifrare un codice monoalfabetico

- Usare simboli diversi al posto delle lettere non aumenta la difficoltà di decifrazione
- La debolezza del codice sta nelle ripetizioni di simboli

Frequenza delle lettere in italiano

Lettera	%	Lettera	%	Lettera	%
a	11,74	h	1,54	q	0,51
b	0,92	i	11,28	r	6,38
c	4,50	l	6,51	s	4,98
d	3,73	m	2,52	t	5,63
e	11,79	n	6,88	u	3,02
f	0,95	o	9,83	v	2,10
g	1,65	p	3,05	z	0,49

Come decifrare un codice monoalfabetico

- Sapendo che il testo è in italiano, è facile che l'ultima lettera di ciascuna parola sia una vocale (questa osservazione non è essenziale per il metodo, ma lo rende più breve)
- Si cercano i simboli più frequenti nel testo cifrato
- Si provano a sostituire con le lettere più frequenti in italiano
- Si cerca di vedere se si riesce a “intravedere” delle parti di parole
- Qualche tentativo può portare a parole improbabili, in tal caso si devono rivedere alcune scelte

Esempio

TRT QRDIA R NTMNFZ N GLPRIN

Lettera	Occor-	Lettera	Occor-	Lettera	Occor-
	renze		renze		renze
A	1	H	0	Q	1
B	0	I	2	R	4
C	0	L	1	S	0
D	1	M	1	T	3
E	0	N	4	U	0
F	1	O	0	V	0
G	1	P	1	Z	1

Esempio: **TRT QRDIA R NTMNFZ N GLPRIN**
inizio dalle lettere terminali di una parola e associando loro le vocali, in ordine di frequenza:

R = e, N = a , T = i, Z = o,

si ottiene **iei QeDIAe aiMNFZ a GLPeIa**

Rivediamo alcune scelte (la prima parola non ha senso)
T = n, (è la seconda consonante per frequenza: la prima è L che non sembra adatta), **R = o, Z = e,**

non QoDIAo anMaFe a GLPoIa

Ora introduciamo le consonanti più frequenti ancora mancanti (**l, r,t,s,c**) e reintroduciamo la **i**. Proviamo con **I = l, A = i, D = t, F = r, G = s , L=c:**

non Qotlio anMare a scPola

Posso modificare ancora **D = g** e continuare...

Strumenti per la crittografia moderna

- La matematica è lo strumento fondamentale per la crittografia
 - fornisce metodi per cifrare, decifrare, firmare e controllare messaggi
 - garantisce la sicurezza della crittografia
 - studia (unitamente all'informatica) come svolgere velocemente le operazioni crittografiche

Strumenti per la crittografia moderna

- **La crittografia moderna** è stata fortemente influenzata dall'informatica e dalla matematica ed **ha contribuito in modo essenziale a sviluppare l'informatica**
- L'informatica
 - pone nuove sfide rendendo possibile decifrare in modo semplice cifrari ritenuti impossibili
 - chiede nuove applicazioni e nuove tecniche: ad esempio lo scambio di chiavi, la crittografia a chiave pubblica, la firma digitale, ...
 - fornisce hardware e soprattutto software per la crittografia

Corrispondenza alfabeto/numeri

a	b	c	d	e	f	g	h	i	l
0	1	2	3	4	5	6	7	8	9

m	n	o	p	q	r	s	t	u	v	z
10	11	12	13	14	15	16	17	18	19	20

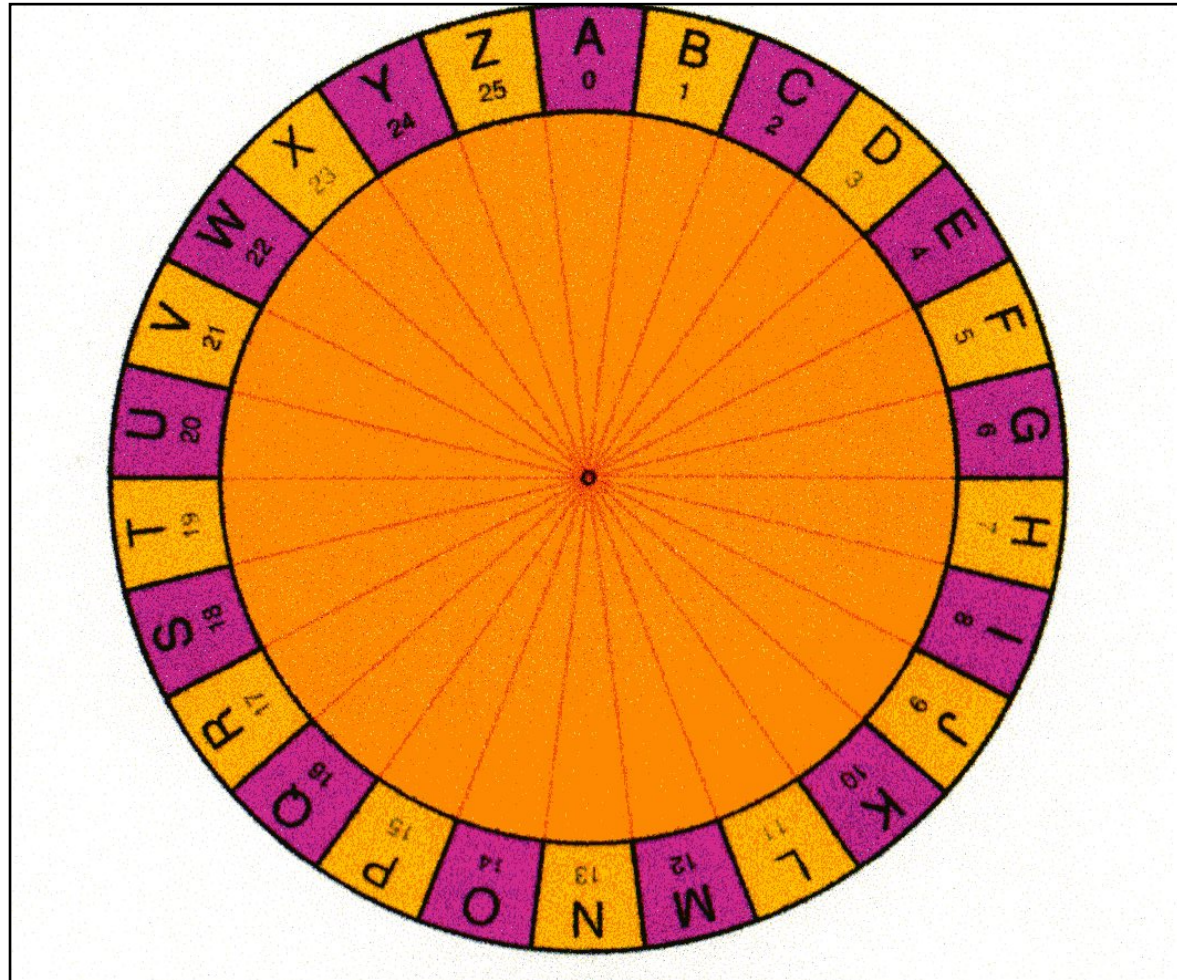
ASCII

traduttore in binario in <http://www.guardaqua.it/risorse/binario.php>

questo codice e' complicato

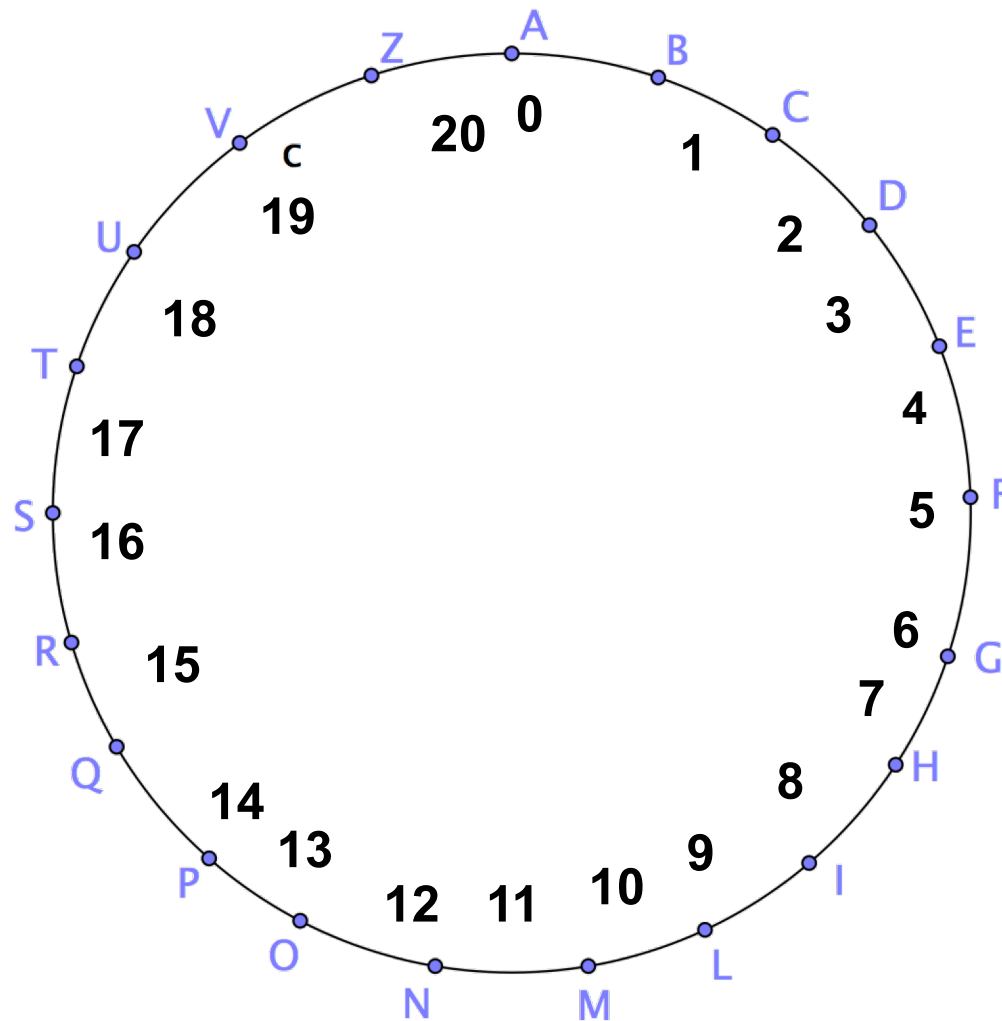
```
01110001 01110101 01100101 01110011
01110100 01101111 00100000 01100011
01101111 01100100 01101001 01100011
01100101 00100000 01100101 00100111
00100000 01100011 01101111 01101101
01110000 01101100 01101001 01100011
01100001 01110100 01101111
```

Il cifrario di Cesare e il disco cifrante



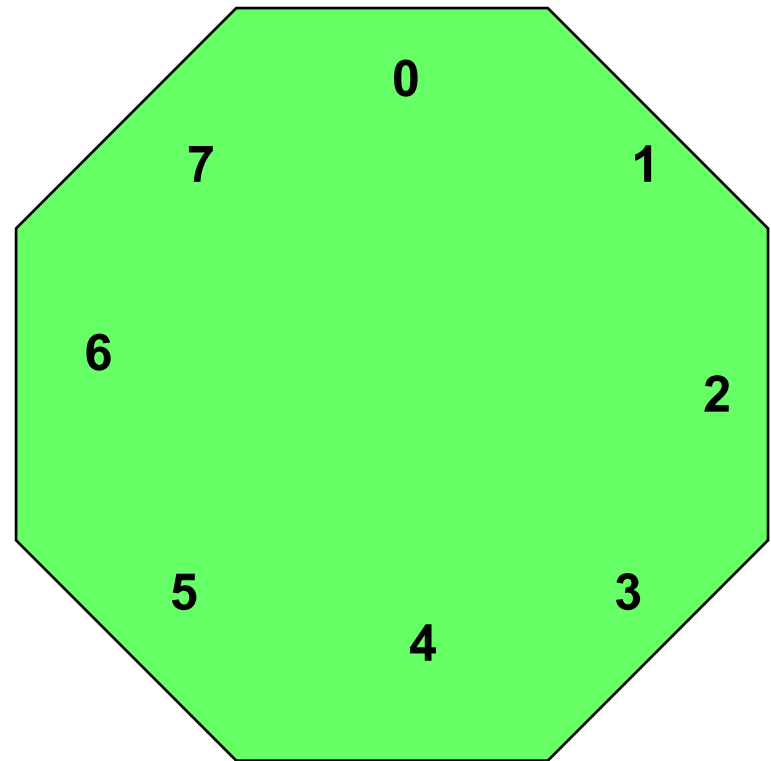
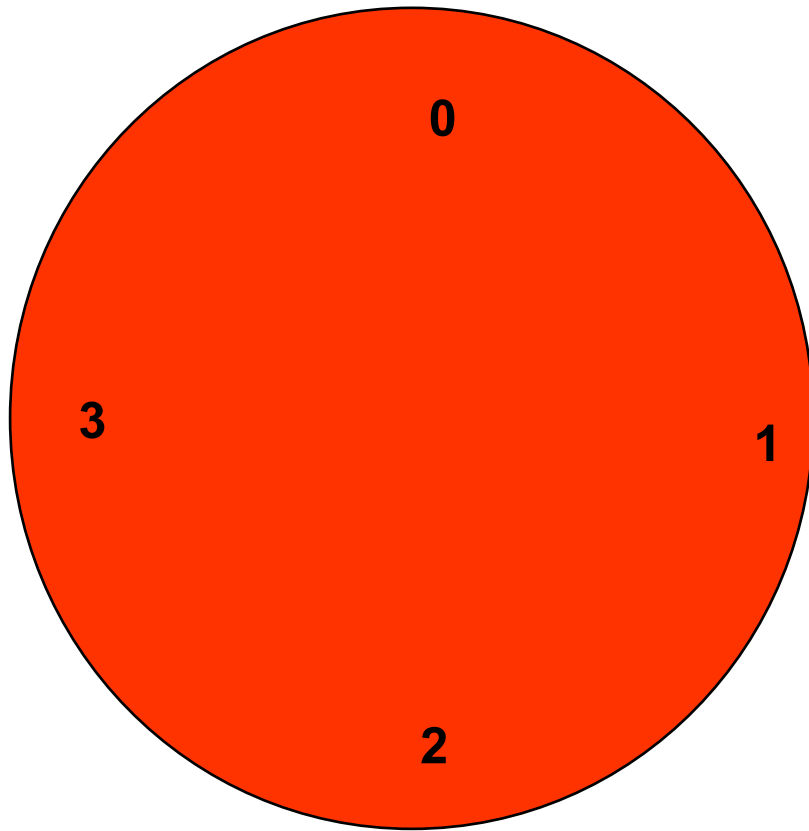
L'aritmetica modulare semplifica la cifratura

Il cifrario di Cesare e il disco cifrante



L'aritmetica modulare semplifica la cifratura

Orologio Modulo 4 e 8



Modulo 10

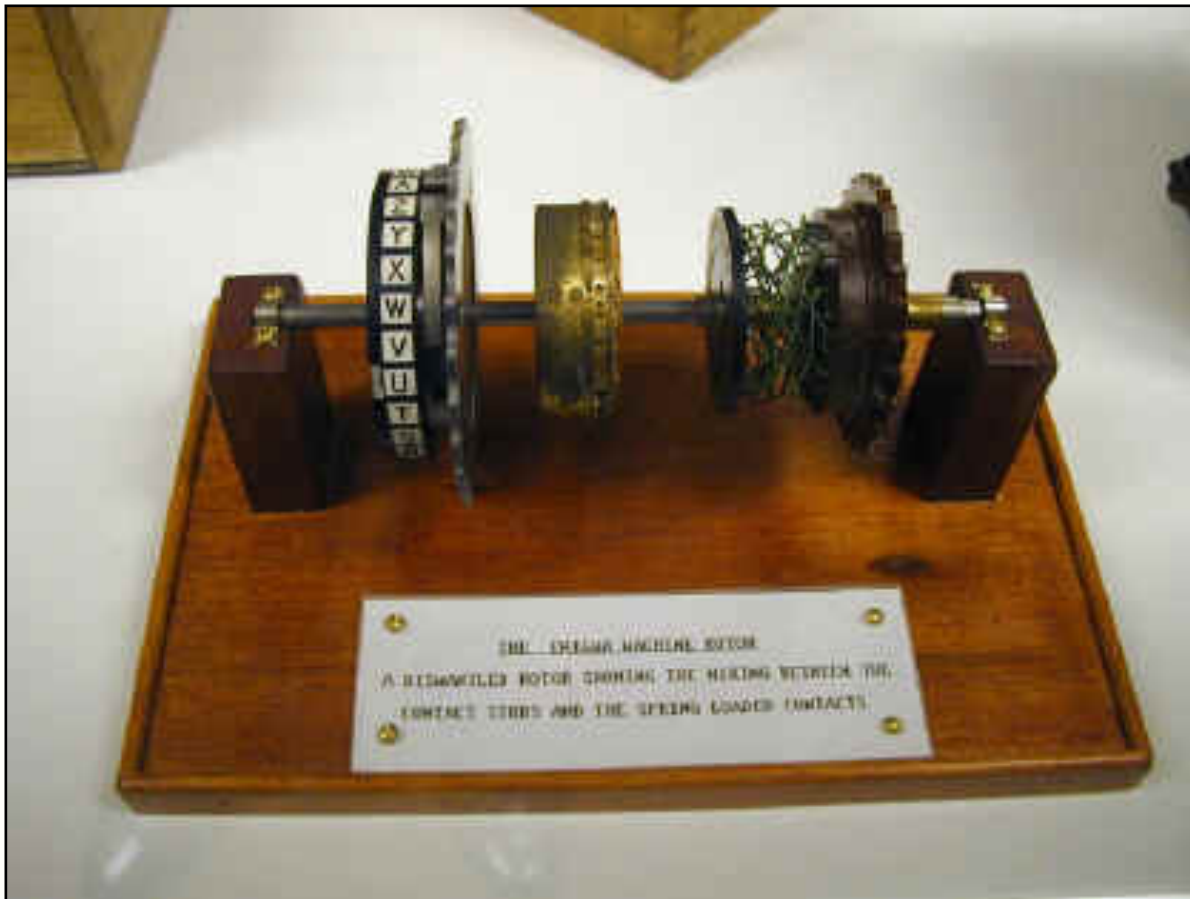
Considero la trasformazione ottenuta moltiplicando per 3. La moltiplicazione fornisce una legge di cifratura?

0	1	2	3	4	5	6	7	8	9
0	3	6	9	2	5	8	1	4	7

Enigma

- Tra la prima e la seconda Guerra Mondiale (e durante tutta la durata del conflitto) i tedeschi utilizzarono una macchina per cifrare e decifrare i messaggi militari
- Tale macchina, chiamata **Enigma**, era stata progettata da Scherbius e venduta all'esercito tedesco che ne acquistò migliaia di esemplari

Enigma



Enigma

- Enigma non è a sostituzione monoalfabetica
- La chiave di Enigma (modificata ogni giorno) è data da
 - la posizione iniziale di ogni scambiatore (26x26x26 combinazioni possibili)
 - l'ordine in cui gli scambiatori sono montati nella macchina (6 combinazioni possibili)
 - le connessioni sul pannello a prese multiple (miliardi di combinazioni diverse)
- **Il numero di chiavi possibili è enorme, dell'ordine di milioni di miliardi di combinazioni possibili**

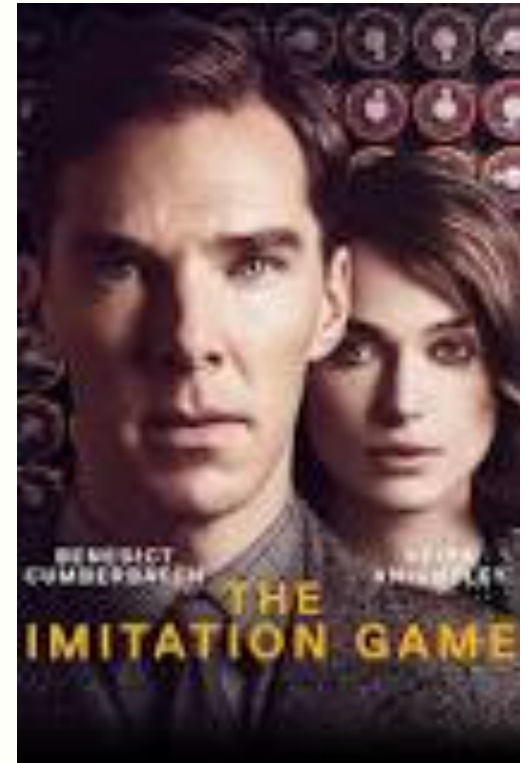
Per anni è stata ritenuta praticamente impossibile da violare e ne sono stati costruiti e utilizzati esemplari sempre più complessi. Il codice Enigma in realtà venne decifrato inizialmente dai polacchi e poi dagli inglesi



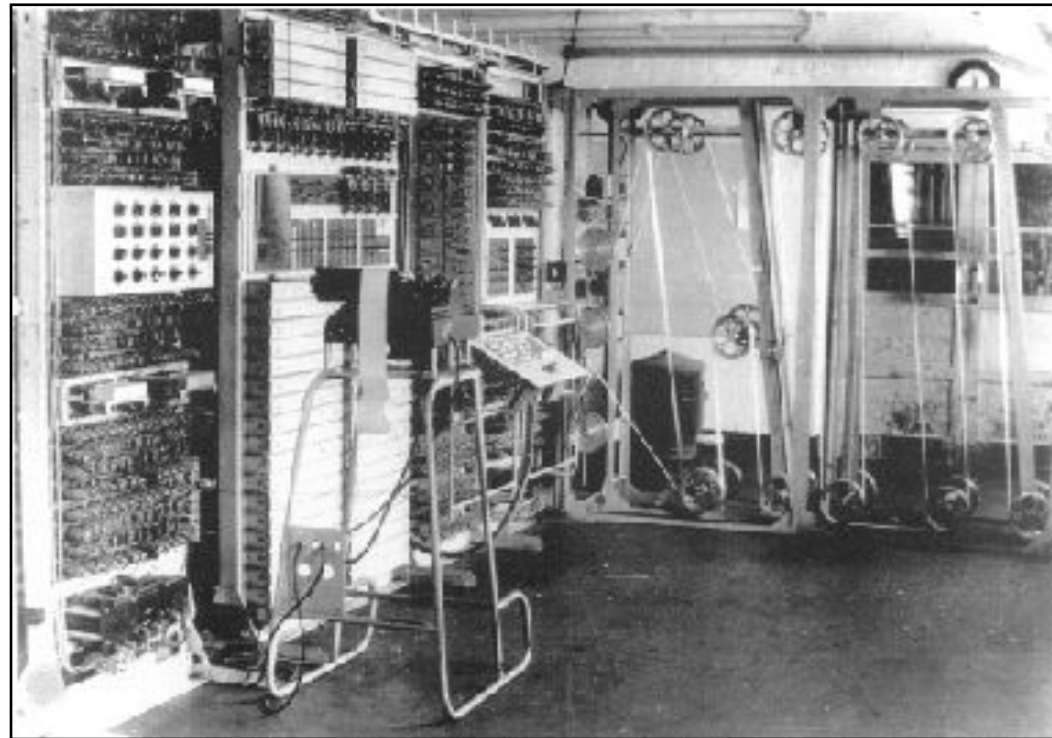
Marian Rejewski



Alan Turing



- Il contributo della matematica (e di Alan Turing in particolare) è stato determinante nel lavoro dei decifраторi ed ha condotto alla costruzione dei primi calcolatori elettronici. (cf., Colossus, in figura)
- La decifrazione di Enigma e il complessivo lavoro dei decifраторi ha sicuramente svolto un ruolo rilevante nella II Guerra Mondiale.



Crittografia a chiave pubblica

Una rivoluzione moderna

- Nel 1976, Diffie e Hellmann mettono le basi per un sistema crittografico in cui **la chiave per cifrare non permetta di ricavare la chiave per decifrare**: in tal modo è possibile (ad esempio per una banca) rendere pubblica la chiave per cifrare, permettendo a tutti di scrivere alla banca stessa in segretezza.
- Solo la banca è in grado di leggere il contenuto del messaggio, perchè possiede la chiave per decifrare

R. S. A.

(2002 Turing Award)

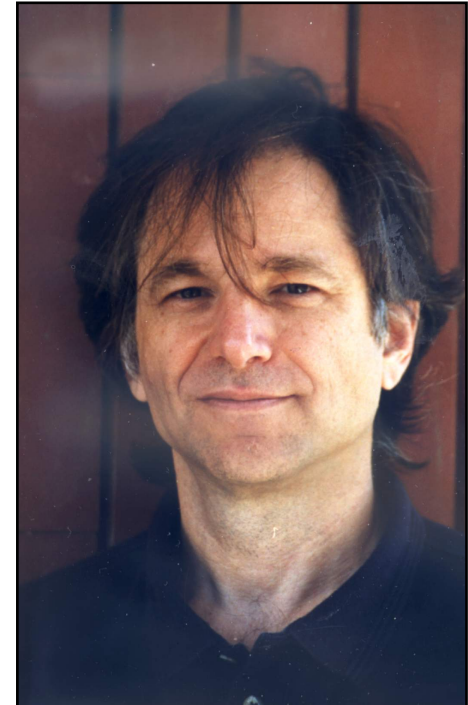
Ronald R. Rivest



Adi Shamir



Leonard Adleman



Crittografia a chiave pubblica

- Provare a decomporre 703

$$703 = 19 \times 37$$

- Provare a decomporre 1003 come prodotto di due fattori propri

$$1003 = 17 \times 59$$

Siamo abbastanza capaci di trovare nuovi numeri primi grandi, ma non siamo capaci di fattorizzare in modo efficiente

Maple, Comando ifactor(n)

```
> ifactor(25);
(5)2
> time();
0.110
> ifactor(89326);
(2) (59) (757)
> time();
0.126
> ifactor(7402381959371505873972948);
(2)2 (3)2 (23) (387784664719) (702937) (32797)
> time();
0.141
> ifactor(3750274916403228867928559493092386478392001);
(19) (249229639642279) (1952857271238834007) (405545243)
> time();
15.063
> ifactor(75037729587295017739462285912874098765394758993291);
(2621576403435079933578426134461) (815103613) (35115943987)
> time();
55.125
> ifactor(752972745436870989765432678796554689075425876598788653478900987665);
(3) (5) (13) (411357811644598812397146142918734353295386201) (538953807820091) (17417)
> time();
403.359
> |
```

```
> prevprime(752972745436870989765432678796554689075425876598788653478900987665) ;  
752972745436870989765432678796554689075425876598788653478900987481  
-  
> time() ;  
0.126  
-  
> nextprime(752972745436870989765432678796554689075425876598788653478900987665) ;  
752972745436870989765432678796554689075425876598788653478900987681  
-  
> time() ;  
0.142  
-  
> ifactor(752972745436870989765432678796554689075425876598788653478900987665) ;  
(3) (5) (13) (411357811644598812397146142918734353295386201) (538953807820091) (17417)  
-  
> time() ;  
391.092
```

- <http://www.rsa.com/>

Nel 2005 F. Bahr, M. Boehm, J. Franke, T. Kleinjung hanno calcolato i fattori del numero indicato con RSA-640: i fattori sono:

16347336458092538484431338838650908598417836700330
92312181110852389333100104508151212118167511579

e

1900871281664822113126851573935413975471896789968
515493666638539088027103802104498957191261465571

- Per calcolarli, hanno lavorato **5 mesi facendo lavorare più calcolatori in parallelo (per un equivalente di 30 anni di lavoro per un singolo calcolatore)**.

- La RSA è una ditta fiorentina che vende coppie di numeri primi molto grandi: questi numeri vengono utilizzati per il più diffuso metodo crittografico.

Sistema RSA

- **Chiave pubblica** (n, e) , formata da una coppia di numeri tali che
 n è prodotto di due primi p e q
il massimo comun divisore tra e e $(p-1)(q-1)$ è uguale a 1.
- **Chiave privata**: un numero d tale che $ed-1$ sia divisibile per $(p-1)(q-1)$ [si calcola facilmente se si conoscono p e q]

RSA esempio

- **Chiave pubblica** ($n=15, e=5$),
 n è prodotto di due primi $p=3$ e $q=5$
 $(p-1)(q-1) =$ non fattori in comune con 5
- **Chiave privata:** cerco un numero d tale che $5d-1$ sia divisibile per $(p-1)(q-1)=8$. Ho bisogno che $5d = 1 + 8a$: osservo che
 $5 \times 5 = 25 = 1 + 24 = 1 + 3 \times 8$: dunque $d=3$ va bene
[il prodotto ed coincide con 1 sull'orologio con 8 ore]

Chiave pubblica: (1003, 3)

Chiave privata: ?

- Voglio scrivere “vieni qui”
- Trascrivo in cifre: 21 08 04 13 08 16 20 08
- Divido in blocchi più piccoli di 1003:
210 804 130 816 200 823
(ho aggiunto, in fondo, una $x=23$)

Chiave pubblica: ($n=1003, e=3$)

- I blocchi sono:

$$m_1=210 \quad m_2=804 \quad m_3=130 \quad m_4=816 \quad m_5=200 \quad m_6=823$$

- **Cifro ogni blocco, facendone la potenza di indice e :**

- $c_1 = m_1^e \text{ modulo } n$ cioè $(210)^3 \text{ modulo } 1003$: $c_1=301$

- $c_2 = (804)^3 \text{ modulo } 1003$: dunque $c_2=975$

- $c_3 = (130)^3 \text{ modulo } 1003$: dunque $c_3=430$

- $c_4 = (816)^3 \text{ modulo } 1003$: dunque $c_4=357$

- $c_5 = (200)^3 \text{ modulo } 1003$: dunque $c_5=72$

- $c_6 = (823)^3 \text{ modulo } 1003$: dunque $c_6=445$

Chiave pubblica: ($n=1003$, $e=3$)

Chiave privata: ?

- Il destinatario sa che $1003 = 17 \times 59$ (chiamo $p=17$, $q=59$)
Deve calcolare la chiave privata d tale che $ed-1$ sia divisibile per $(p-1)(q-1)=16 \times 58 = 928$. Ricava **$d=619$** .
- Decifra ogni blocco, iniziando dal primo: **la procedura è uguale a quella della cifratura, ma l'esponente da usare è la chiave segreta**
- $m_1 = c_1^d$ modulo n cioè $(301)^{619}$ modulo 1003 : **$m_1=210$**
- $m_2 = (975)^{619}$ modulo 1003 : dunque **$m_2=804$**
- $m_3 = (430)^{619}$ modulo 1003 : dunque **$m_3=130$**
- $m_4 = (357)^{619}$ modulo 1003 : dunque **$m_4=816$**
- $m_5 = (72)^{619}$ modulo 1003 : dunque **$m_5=200$**
- $m_6 = (445)^{619}$ modulo 1003 : dunque **$m_6=823$**