Euhyh vwruld ghood fulwwrjudild

a cura di Alessandro Musesti
Università Cattolica del Sacro Cuore, Brescia

L'inizio della storia: il metodo Atbash

Ecco alcuni metodi crittografici usati nella storia per codificare messaggi.

Il metodo Atbash consiste nel sostituire la prima lettera dell'alfabeto con l'ultima, la seconda con la penultima, e così via.

Chiaro	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
Cifrato	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Il metodo prende il nome dallo scambio delle lettere nell'alfabeto ebraico: א(alef) con ת(tav), ב(bet) con ש(shin), da cui il nome אתבש(atbash).

Il metodo è molto antico: ad esempio, nel libro di Geremia si trova parecchie volte la parola ששך(Sheshakh) che sta per בבל(Babel).

Il cifrario di Cesare

Consiste nel sostituire ogni lettera con quella che viene tre lettere dopo nell'alfabeto (si chiama anche spostamento di 3). Il numero 3 in questo caso è la **chiave** di cifratura.

Chiaro	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
Cifrato	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caio Giulio Cesare usava questo metodo per comunicare con le truppe. Naturalmente può essere usata qualsiasi altra chiave (compresa tra 1 e 25). Un algoritmo tuttora usato (per gioco) è il ROT13, in cui la chiave scelta è 13 (in questo modo per crittare e decrittare si usa lo stesso algoritmo):

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

L'analisi delle frequenze con cui compaiono le lettere rende questi metodi molto deboli: ad esempio, se il testo è in lingua italiana, si possono cercare le lettere più frequenti, che saranno le vocali e,a,i,o. Da qui si può partire per trovare le altre. **Riuscite a scoprire il titolo di questo poster?**

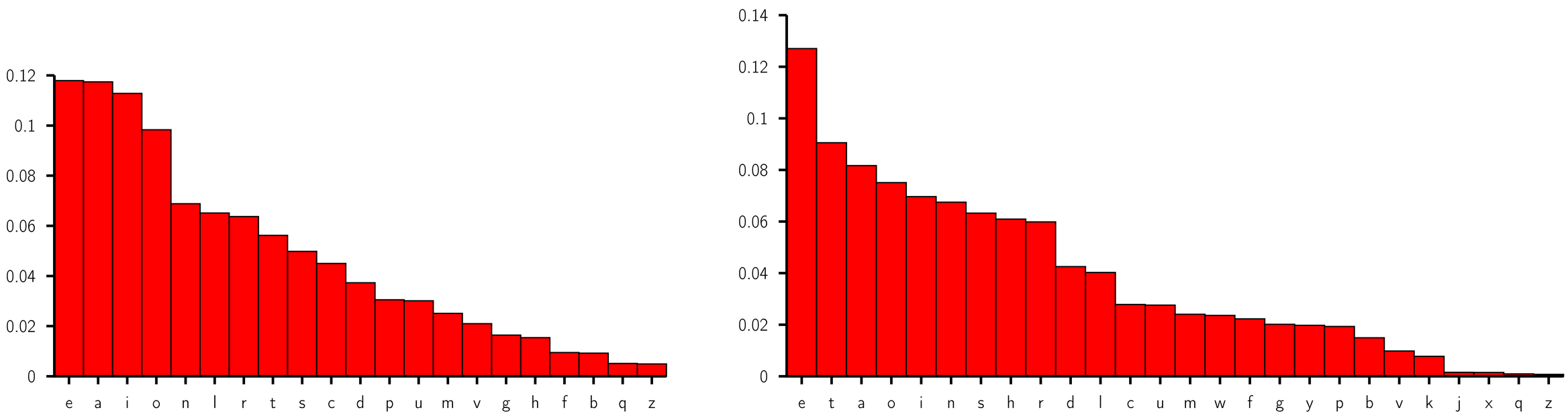

Figura : Frequenze delle lettere nella lingua italiana (a sinistra) e inglese (a destra)

Il cifrario di Vigenère (1586)

In questo metodo bisogna stabilire una parola, o una frase (anche lunga) comune: questa sarà la chiave segreta del cifrario.
Per esempio, la chiave segreta sia la parola RICERCA e supponiamo di voler cifrare la frase "la matematica è bella". In una tabella scriviamo la frase da cifrare e sotto di essa, ripetutamente, la parola-chiave. Poi ad ogni lettera "sommiamo" il valore della lettera corrispondente della parola-chiave (da A=0 a Z=25), trovando una nuova lettera:

Chiaro	l	a	m	a	t	e	m	a	t	i	c	a	e	b	e	l	l	a
Chiave	R	I	C	E	R	C	A	R	I	C	E	R	C	A	R	I	C	E
Cifrato	C	I	O	E	K	G	M	R	B	K	G	R	G	B	V	T	N	E

Questo codice è piuttosto robusto (non basta l'analisi delle frequenze per forzarlo) ma dipende molto dalla lunghezza della parola-chiave: se questa è corta, diventa abbastanza debole.

I blocchetti monouso (cifrario di Vernam, 1917)

Se nel cifrario di Vigenère prendiamo una parola-chiave lunga come il messaggio e formata da caratteri completamente casuali, otteniamo il cosiddetto cifrario di Vernam.
È stato dimostrato che questo è il modo più sicuro di scambiarsi un messaggio, ma ha una pecca: come condividere la chiave segreta, così lunga? Il serpente si morde la coda...
Nella realtà questo metodo è stato usato: ad esempio durante la II Guerra Mondiale venivano distribuite alcune copie di "blocchetti monouso", pagine e pagine di caratteri casuali (spesso creati mediante estrazione delle lettere da un'urna) opportunamente etichettati. Il messaggio da trasmettere mostrava all'inizio (in chiaro) il codice della pagina corrispondente, e poi veniva codificato con le lettere di quella pagina.
Ma questo metodo non si può usare per trasmettere il nostro numero di carta di credito a un negoziante: prima dovremmo andare fisicamente nel negozio e consegnargli un blocchetto monouso!

La macchina ENIGMA

È una macchina tedesca usata per codificare i messaggi durante la II Guerra Mondiale. Basata su tre rotori (scelti tra cinque disponibili), posizionati all'inizio in una posizione concordata e che poi continuavano a ruotare ad ogni lettera, cambiando cifrario ogni volta.
Nella figura vediamo il percorso fatto da una A che viene codificata in una D (e viceversa).

Verso i cifrari contemporanei: i cifrari poligrafici

Nei cifrari contemporanei non si usa più codificare una lettera alla volta, ma si suddivide il messaggio in blocchi di due o più lettere, e sono i blocchi ad essere codificati singolarmente. In questo modo la procedura si complica, poiché aumenta molto il numero dei simboli (esistono $26^2 = 676$ coppie di lettere possibili, e se si usano le terne il numero diventa $26^3 = 17576$) ma si rende molto più difficile l'analisi delle frequenze.
Gli attuali cifrari (DES, AES) si basano su questo principio.

Posizione rotori dentro la macchina

Riflettore	*Rotore sinistro*	*Rotore al centro*	*Rotore destro*	*Iniziale*
---K Q---	---S Q	Y Q---	---A Q	Q
M W	T W	U W	V W	W
I E	I E	F E	O E	E
H R	O R	H R	E R	R
U T	F T	X T	Y T	T
G Z	M Z	Z Z	F Z	Z
T U	Y U	M U	W U	U
E I	Z I	N I	L I	I
V O	E O	J O---	---D O	O
J A	Q A	G A	Q A---	---A---
C S	D S---	---O S	C S	S
L D	L D	P D	B D---	---D---
X F	B F	A F	S F	F
Z G	C G---	---Q G	P G	G
R H	K H	I H	T H	H
A J	J J	R J	K J	J
---Q K---	---G K	L K	R K	K
N P	V P	D P	G P	P
B Y	P Y	T Y	I Y	Y
F X	U X	W X	J X	X
S C	R C	V C	U C	C
O V	W V	K V	H V	V
Y B	N B	S B	X B	B
P N	X N	B N	Z N	N
W M	A M	C M	M M	M
D L	H L	E L	N L	L