Codici Segreti

Agostino Dovier

Dip di Matematica e Informatica, Univ. di Udine

Ringrazio l'amico e maestro Andrea Sgarro per il materiale tratto dal suo meraviglioso quanto introvabile testo

Codici Segreti

Il festino di Baldassarre (Rembrandt)

- MENE TEKEL PERES (mina, siclo, mezza mina: tre monete)
- Spiegazione nel V Libro del profeta Daniele:
  - ✓ Mene $\approx$ mnh (misurare)
  - ✓ Tekel $\approx$ tql (pesare)
  - ✓ Peres $\approx$ prs (dividere).
- Dio ha misurato il regno di Baldassarre e gli ha posto un termine, l'ha pesato sulla bilancia trovandolo mancante, il regno sta per essere diviso e consegnato ai Medi e ai Persiani.

Codici Segreti

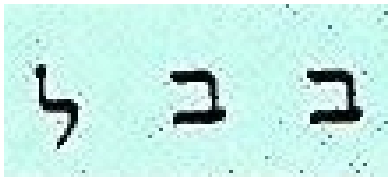
La profezia di Daniele

- MENE TEKEL PERES (mina, siclo, mezza mina: tre monete)
- Spiegazione nel V Libro del profeta Daniele:
  - ✓ Mene $\approx$ mnh (misurare)
  - ✓ Tekel $\approx$ tql (pesare)
  - ✓ Peres $\approx$ prs (dividere).
- Dio ha misurato il regno di Baldassarre e gli ha posto un termine, l'ha pesato sulla bilancia trovandolo mancante, il regno sta per essere diviso e consegnato ai Medi e ai Persiani.

Codici Segreti

Atbash Ebraico (libro di Geremia) — sostituzione

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



Babel/Babilonia

Sheschach

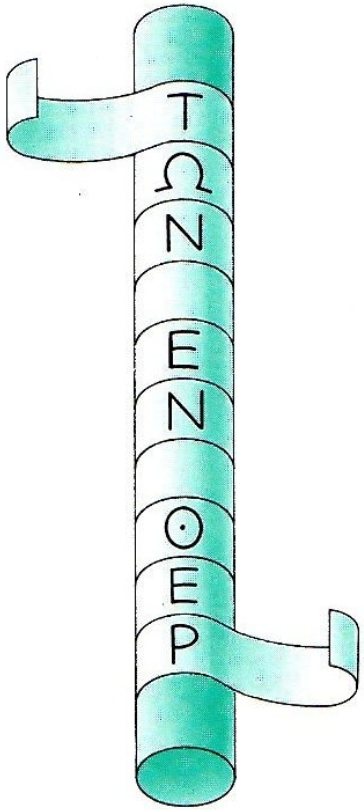
Codici Segreti

Giulio Cesare (100–44 AC) — sostituzione

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

Codici Segreti

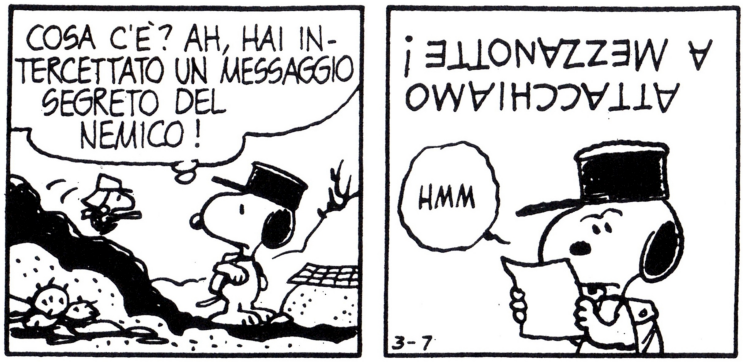
Scitala spartana (≈ 400 AC) — trasposizione



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

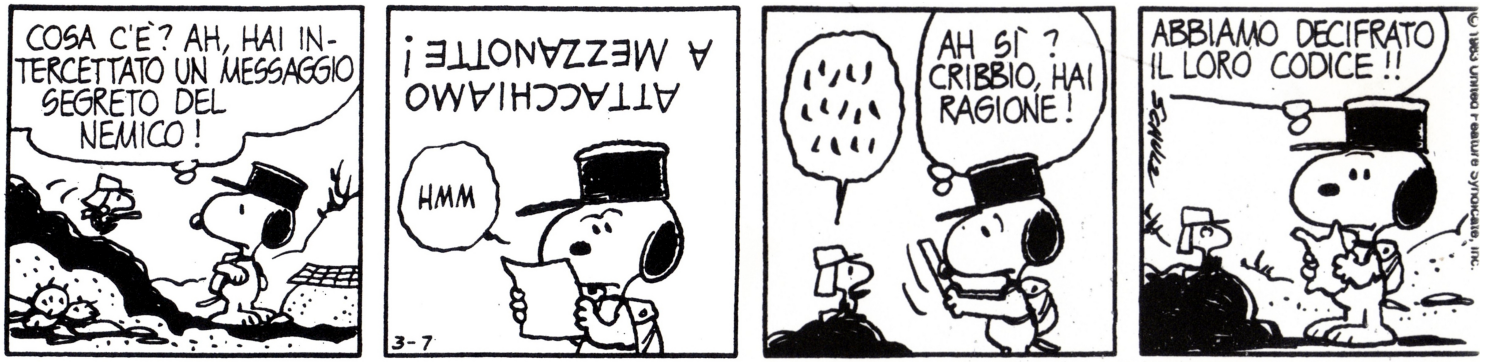
Codici Segreti

Altro codice a Trasposizione



Codici Segreti

Altro codice a Trasposizione



Codici Segreti

Mary Stuart (1542–1587)

- Regina di Scozia, con vita parecchio infelice,
- usò un nomenclatore per corrispondere con gli alleati francesi per cospirare contro l'Inghilterra.
- I crittografi di corte inglesi decrittarono i messaggi.
- Finì male.

Codici Segreti

Il telegramma Zimmerman (1917)

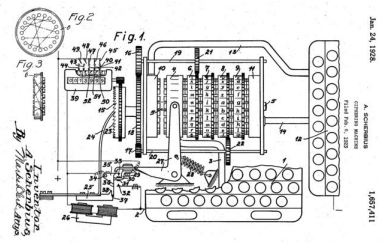
I servizi segreti inglesi intercettano un telegramma cifrato del ministro tedesco Zimmermann all'ambasciatore tedesco a Washington

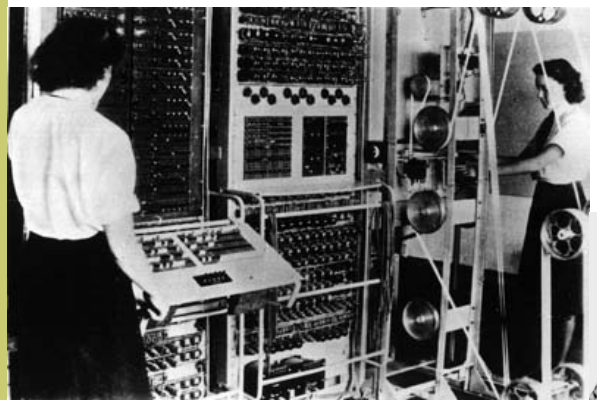
- Il telegramma ripartì da Washington per il Messico
- Grave errore: usarono diverso cifrario
- Fu decrittato.
- Si proponeva alleanza con Messico offrendo in cambio territori del Texas, New Mexico e Arizona.
- Gli USA entrarono nella I guerra mondiale.

Codici Segreti

enigma

Durante la seconda guerra mondiale la macchina da cifra denominata ENIGMA (Arthur Scherbius 1878–1929) fu uno dei punti di forza dell'esercito tedesco.



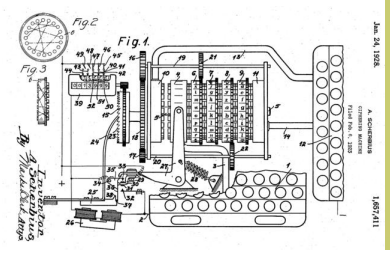


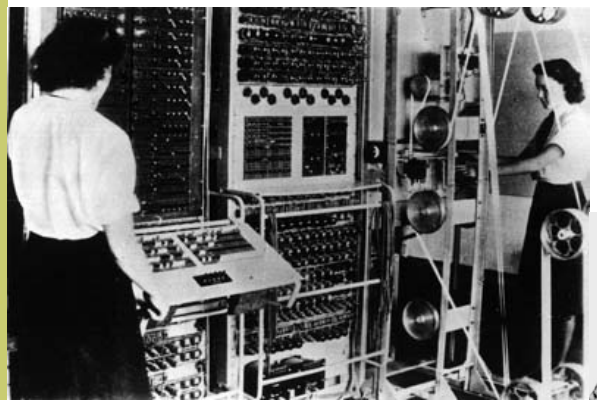
Sfruttando dei risultati dei matematici polacchi e progettando le "bombe" (ed in seguito il primo calcolatore elettronico a valvole termoioniche COLOSSUS) un team coordinato da Alan M. Turing (1912–1954) riuscì a forzare l'ENIGMA invertendo le sorti del conflitto.

Codici Segreti

ENIGMA

Durante la seconda guerra mondiale la macchina da cifra denominata ENIGMA (Arthur Scherbius 1878–1929) fu uno dei punti di forza dell'esercito tedesco.



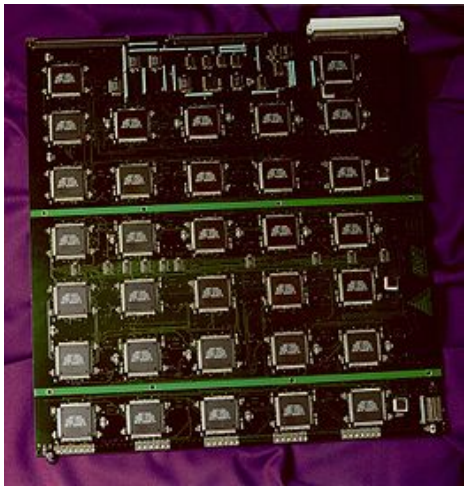


Sfruttando dei risultati dei matematici polacchi e progettando le "bombe" (ed in seguito il primo calcolatore elettronico a valvole termoioniche COLOSSUS) un team coordinato da Alan M. Turing (1912–1954) riuscì a forzare l'ENIGMA invertendo le sorti del conflitto.

Codici Segreti

Data Encription Standard (DES)

Negli anni ’70 viene pubblicato il DES come standard per la crittografia. Per la prima volta viene fornita liberamente al crittografo la “macchina” da cifra.

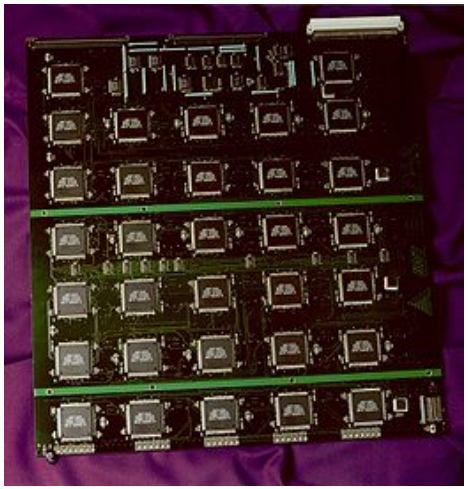


Nel 1996 il DES è violato, nel 1997 (progetto DESCHALL) è violato in pubblico, nel 1998 Il DES cracker dell’EFF (Deep Crack—250K$) viola una chiave DES in 56 ore.

Codici Segreti

Data Encription Standard (DES)

Negli anni ’70 viene pubblicato il DES come standard per la crittografia. Per la prima volta viene fornita liberamente al crittografo la “macchina” da cifra.



Nel 1996 il DES è violato, nel 1997 (progetto DESCHALL) è violato in pubblico, nel 1998 Il DES cracker dell’EFF (Deep Crack—250K$) viola una chiave DES in 56 ore.

Codici Segreti

Wikileaks

Novembre 2010. Wikileaks dichiara di avere milioni di file riservati e inizia la loro pubblicazione in rete.

Scopriamo che i festini di Baldassarre continuano 2500 anni dopo.

Codici Segreti

Wikileaks

Novembre 2010. Wikileaks dichiara di avere milioni di file riservati e inizia la loro pubblicazione in rete.

Scopriamo che i festini di Baldassarre continuano 2500 anni dopo.

Codici Segreti

Terminologia

- Il testo in chiaro o messaggio viene trasformato in un
- testo in cifra o crittogramma
- Tale operazione si dice cifratura
- La decifrazione o decifratura è l'operazione legittima, facile per il destinatario desiderato.
- La spia che intercetta il crittogramma e vuole decifrarlo opera (se ci riesce) una decrittazione
- Similmente ci sono termini diversi per la crittografia (parte costruttiva), per la crittanalisi (parte distruttiva), e per la crittologia (disciplina complessiva).
- Spesso si usa comunque crittografia come sinonimo di crittologia.

Codici Segreti

Terminologia

- Il testo in chiaro o messaggio viene trasformato in un
- testo in cifra o crittogramma
- Tale operazione si dice cifratura
- La decifrazione o decifratura è l'operazione legittima, facile per il destinatario desiderato.
- La spia che intercetta il crittogramma e vuole decifrarlo opera (se ci riesce) una decrittazione
- Similmente ci sono termini diversi per la crittografia (parte costruttiva), per la crittanalisi (parte distruttiva), e per la crittologia (disciplina complessiva).
- Spesso si usa comunque crittografia come sinonimo di crittologia.

Codici Segreti

Terminologia

- Il testo in chiaro o messaggio viene trasformato in un
- testo in cifra o crittogramma
- Tale operazione si dice cifratura
- La decifrazione o decifratura è l'operazione legittima, facile per il destinatario desiderato.
- La spia che intercetta il crittogramma e vuole decifrarlo opera (se ci riesce) una decrittazione
- Similmente ci sono termini diversi per la crittografia (parte costruttiva), per la crittanalisi (parte distruttiva), e per la crittologia (disciplina complessiva).
- Spesso si usa comunque crittografia come sinonimo di crittologia.

Codici Segreti

Il principio di Kerckhoffs

- Auguste Kerchoffs von Nieuvenhof (1835–1903)
- Scrive La cryptographie militaire (1883)
- Illustra differenza tra crittografia di tipo tattico (basta che il segreto duri qualche ora o giorno) e strategico (meglio se per sempre)
- Enuncia il principio: *La sicurezza di un sistema strategico è affidata interamente o comunque essenzialmente alla segretezza della chiave*
- Dobbiamo assumere che il nemico conosca il tipo di cifrario impiegato (se non lo sa, meglio).
- La crittografia moderna (da DES in poi) l'ha preso come dogma.

Cifrari a sostituzione monoalfabetica

Giulio Cesare (100–44 AC)

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

- L'operazione di cifratura avviene mediante l'applicazione di una sostituzione di lettere.
- Vi è dunque una funzione biiettiva

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

- Essendo biiettiva, è invertibile, ovvero esiste f^{-1} tale che $f^{-1}(f(x)) = x$ per ogni $x \in \{A, \ldots, Z\}$.
- Per la cifratura si usa f.
- Per la decifratura si usa f^{-1}, nota al legittimo destinatario ma non alla spia.
- La spia, ammettendo conosca il sistema di cifratura usato deve "indovinare" f^{-1} (in questo caso va bene anche f).
- Nel caso del cifrario di Cesare, ci sono solo 21 (anzi 20) funzioni possibili (chiave: lettera iniziale).

Cifrari a sostituzione monoalfabetica

- L'operazione di cifratura avviene mediante l'applicazione di una sostituzione di lettere.
- Vi è dunque una funzione biiettiva

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

- Essendo biiettiva, è invertibile, ovvero esiste f^{-1} tale che $f^{-1}(f(x)) = x$ per ogni $x \in \{A, \ldots, Z\}$.
- Per la cifratura si usa f.
- Per la decifratura si usa f^{-1}, nota al legittimo destinatario ma non alla spia.
- La spia, ammettendo conosca il sistema di cifratura usato deve "indovinare" f^{-1} (in questo caso va bene anche f).
- Nel caso del cifrario di Cesare, ci sono solo 21 (anzi 20) funzioni possibili (chiave: lettera iniziale).

Cifrari a sostituzione monoalfabetica

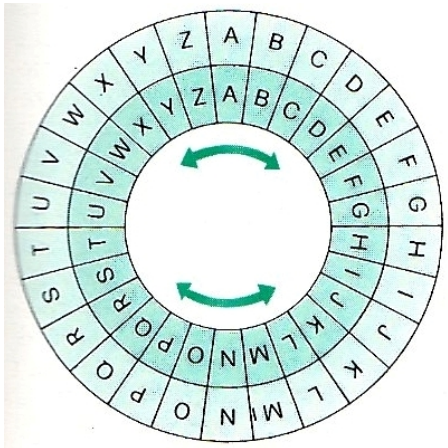
- L'operazione di cifratura avviene mediante l'applicazione di una sostituzione di lettere.
- Vi è dunque una funzione biiettiva

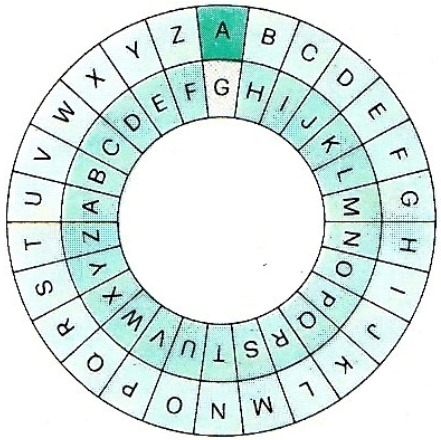
$$f : \{A, \ldots, Z\} \longrightarrow \{A, \ldots, Z\}$$

- Essendo biiettiva, è invertibile, ovvero esiste f^{-1} tale che $f^{-1}(f(x)) = x$ per ogni $x \in \{A, \ldots, Z\}$.
- Per la cifratura si usa f.
- Per la decifratura si usa f^{-1}, nota al legittimo destinatario ma non alla spia.
- La spia, ammettendo conosca il sistema di cifratura usato deve "indovinare" f^{-1} (in questo caso va bene anche f).
- Nel caso del cifrario di Cesare, ci sono solo 21 (anzi 20) funzioni possibili (chiave: lettera iniziale).

Cifrari a sostituzione monoalfabetica

Leon Battista Alberti (1404–1472)



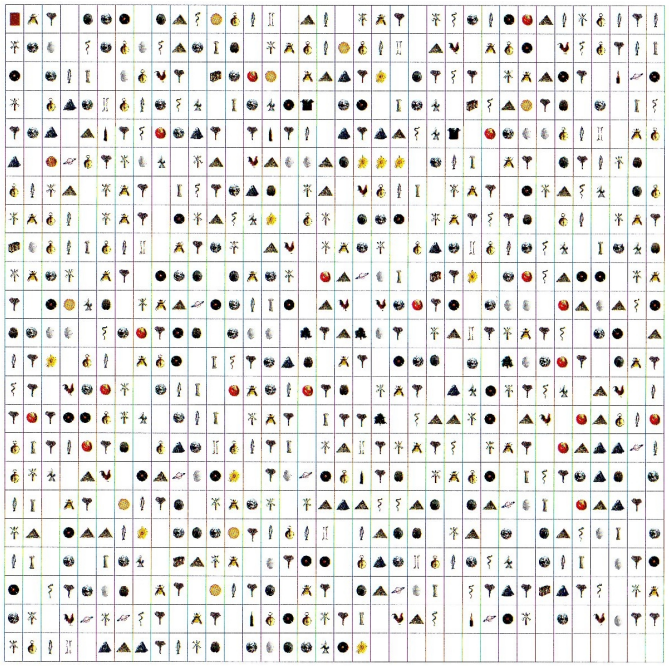


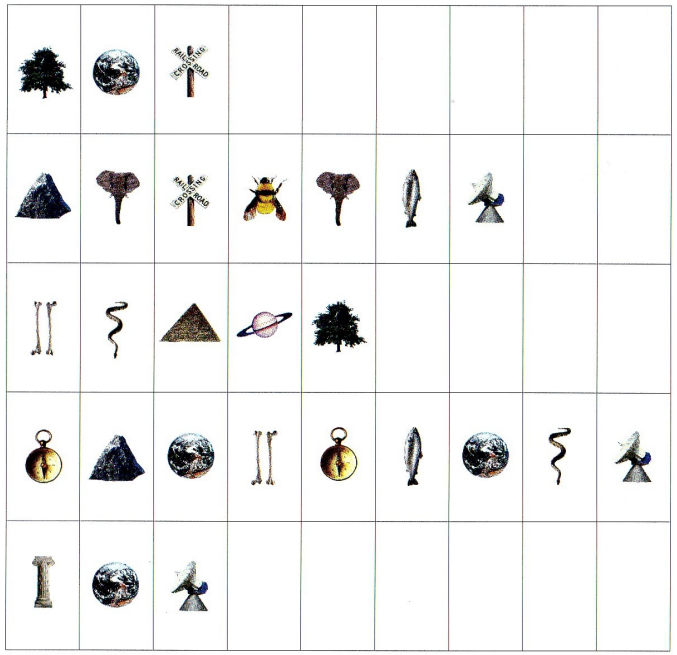
Cifrari a sostituzione monoalfabetica

Giovan Battista Della Porta (1535–1615)

Codici Segreti

Pat Metheny (1997)



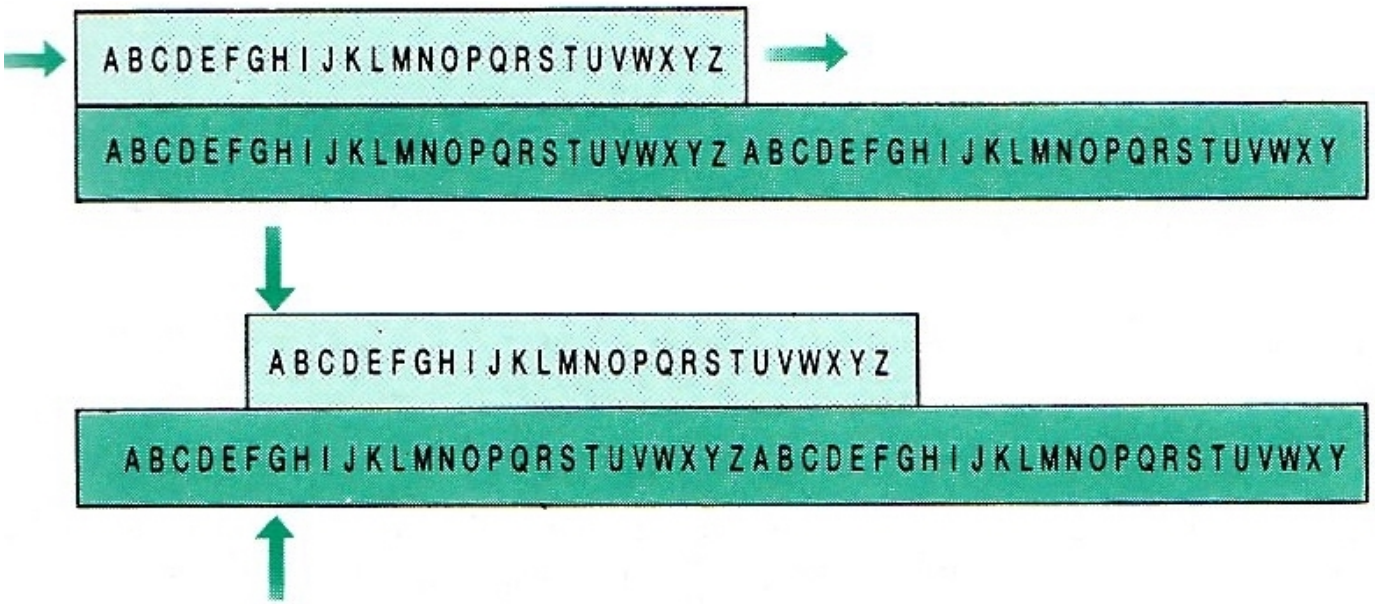


Codici Segreti

Pat Metheny (1997)

Cifrari a sostituzione monoalfabetica

Il regolo di Saint Cyr



Cifrari a sostituzione monoalfabetici

Cifrari completi

- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.
- Le funzioni possibili diventano 21! (in realtà un po' meno ... non vogliamo troppe identità...)
- Ma cominciano a diventare numeri pesanti per la forza bruta.

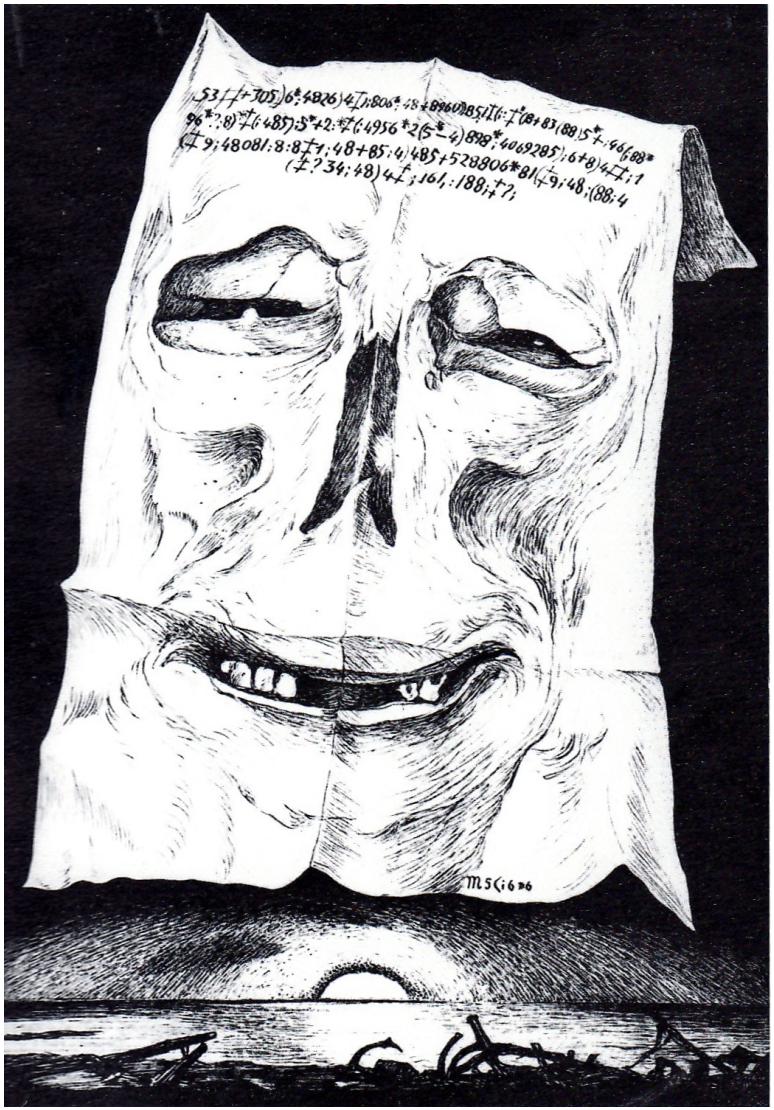
Cifrari a sostituzione monoalfabetici

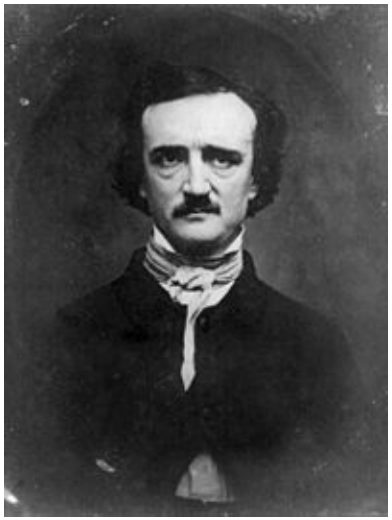
Cifrari completi

- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.
- Le funzioni possibili diventano 21! (in realtà un po' meno ... non vogliamo troppe identità...)
- Ma cominciano a diventare numeri pesanti per la forza bruta.

Cifrari a sostituzione monoalfabetica

Decrittazione





Cifrari a sostituzione monoalfabetica

Decrittazione

Viene usata la statistica linguistica.

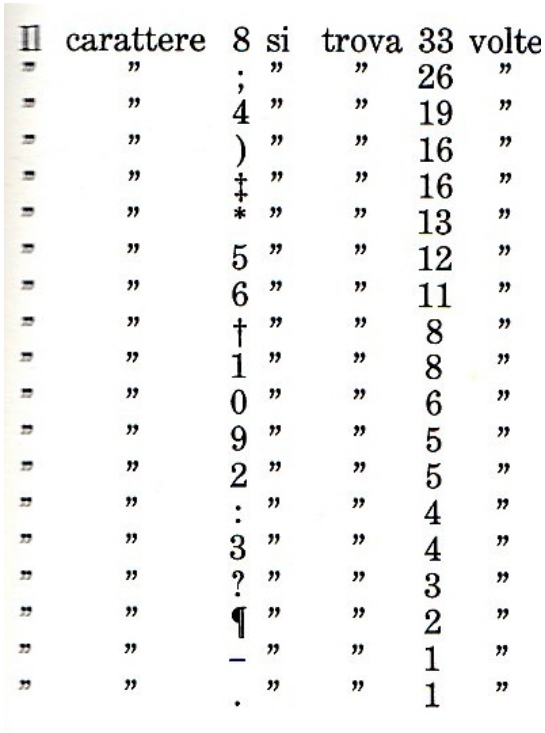
Il	carattere	8	si	trova	33	volte
=	”	;	”	”	26	”
=	”	4	”	”	19	”
=	”	)	”	”	16	”
=	”	‡	”	”	16	”
=	”	*	”	”	13	”
=	”	5	”	”	12	”
=	”	6	”	”	11	”
=	”	†	”	”	8	”
=	”	1	”	”	8	”
=	”	0	”	”	6	”
=	”	9	”	”	5	”
=	”	2	”	”	5	”
=	”	:	”	”	4	”
=	”	3	”	”	4	”
=	”	?	”	”	3	”
=	”	¶	”	”	2	”
=	”	–	”	”	1	”
=	”	.	”	”	1	”

Eccezioni: *Gadsby* (E. W. Wright), *La disparition* (G. Perec) tradotto in *A void* (G. Adair). Tutti senza lettera e.

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	”

Eccezioni: *Gadsby* (E. W. Wright), *La disparition* (G. Perec) tradotto in *A void* (G. Adair). Tutti senza lettera e.

Codici Segreti

Francesco Bacone (1561–1626)

- Codifica binaria (5 bits dell'ASCII):
  $A \mapsto 00001$,
  $B \mapsto 00010$,
  $C \mapsto 00011, \ldots$
- Testo di copertura:
  IO NON DICO PAROLACCE
  QUANDO PARLO IN AULA
- Messaggio in chiaro: CRIBBIO

C	R	I	B	B	I	O
00011	10101	01001	00010	00010	01001	01111
IONON	DICOP	AROLA	CCEQU	ANDOP	ARLOI	NAULA

Crittogramma:

IONon	dIcOp	ArOLa	CCEqU	ANDoP	ArLOi	Naula

- Per confondere la statistica si inseriscono nel testo in chiaro prima della codifica le "nulle" ovvero lettere a bassa probabilità in posti casuali (una ogni tanto, che non pregiudicano la comprensione)
- Ad ogni lettera molto probabile (p.es. le vocali) venogono associati più nomi, per esempio:

$$e \mapsto \{i, \clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$$

  alternadole mediante lancio di monete.
- Il cifrario comincia ad essere robusto ...

Codici Segreti

Nomenclatori (omofonici)

Poi potevano essere ulteriormente cifrati.