Codici Segreti

Agostino Dovier

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

23 febbraio 2016

Codici Segreti

A. Dovier

Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

Codici Segreti

Il festino di Baldassarre (Rembrandt)

Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

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

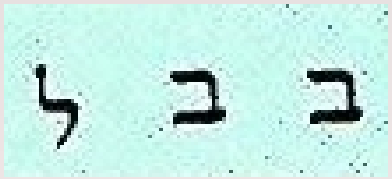
La profezia di Daniele

- 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

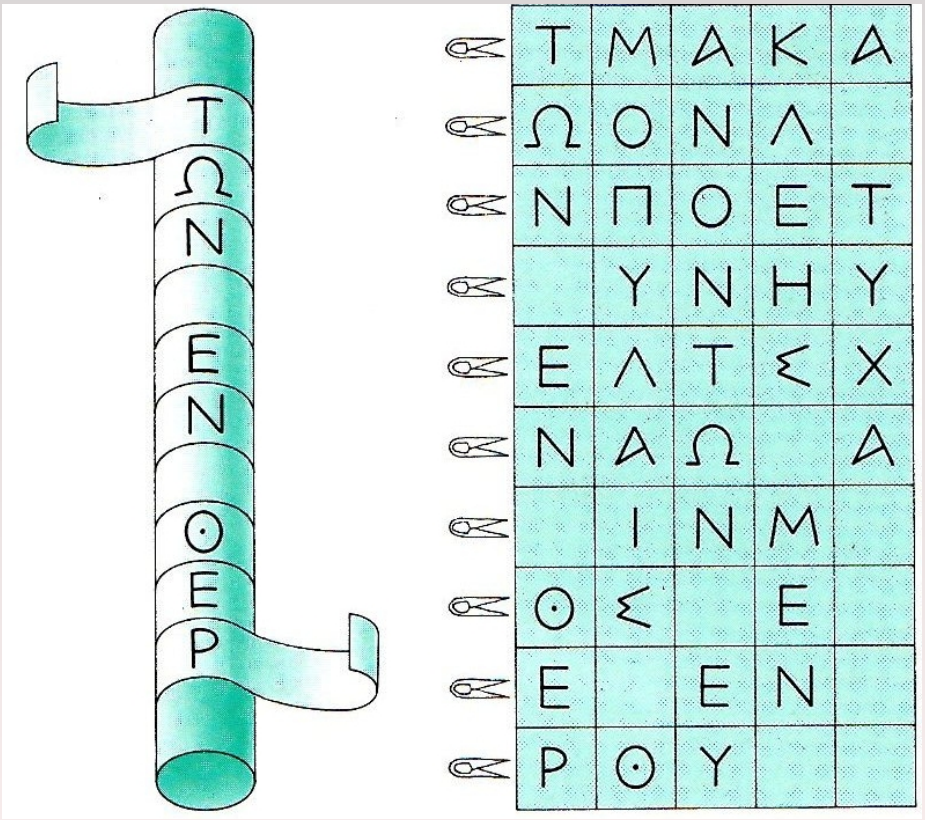
Codici Segreti

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

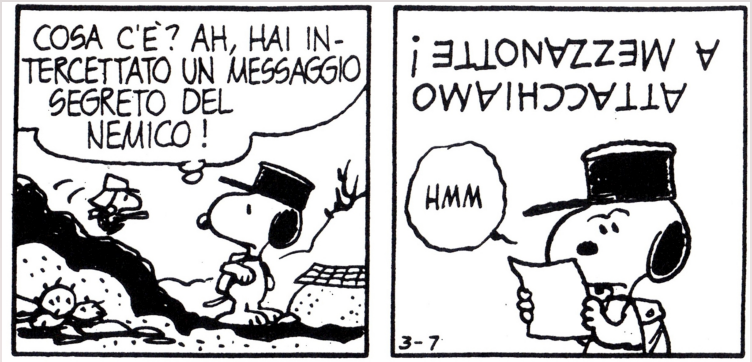
Codici Segreti

Scitala spartana (≈ 400 AC) — trasposizione



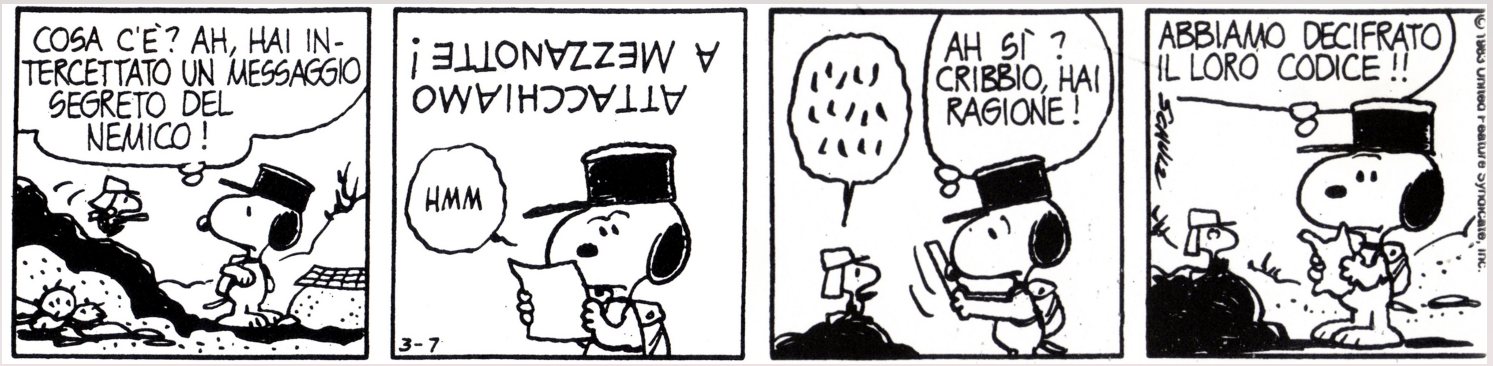
Codici Segreti

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

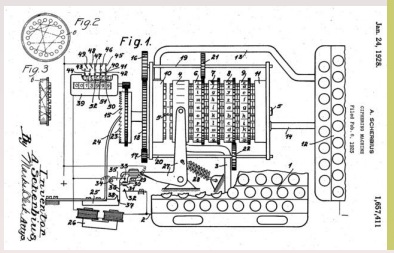
- Il telegramma ripartì da Washington per il Messico
- Grave errore: usarono diverso cifrario
- Fu decrittato.
- Si proponeva alleanza con Messico offrendo in cambio territori del Texas, New Mexico e Arizona.
- Gli USA entrarono nella I guerra mondiale.

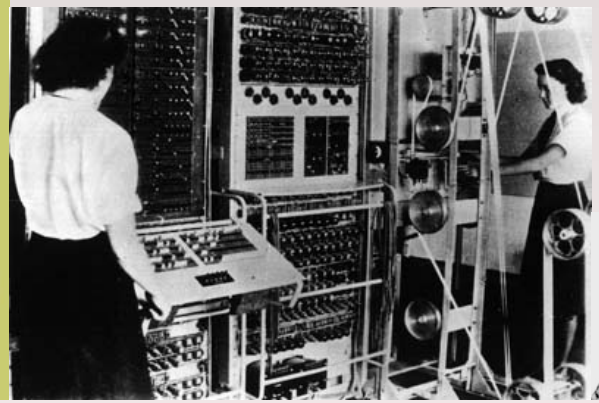
Codici Segreti
A. Dovier
Introduzione
Cifrari monoalfabetici
Confondere la statistica
Cifrari polialfabetici
Il cifrario perfetto

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.

Introduzione

Cifrari monoalfabetici

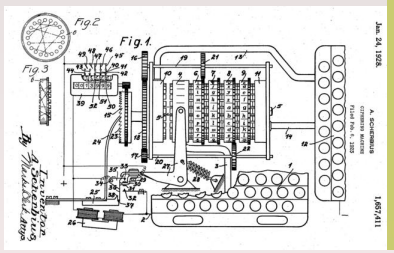
Confondere la statistica

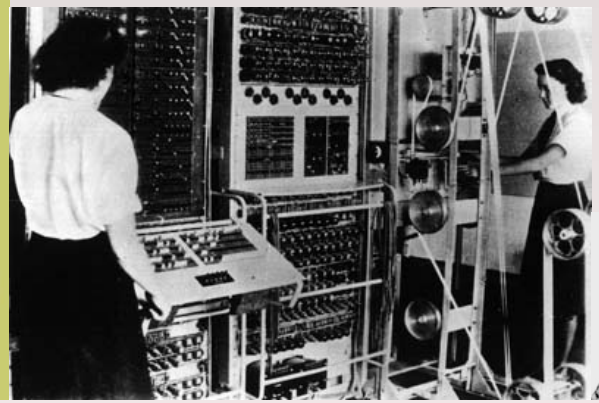
Cifrari polialfabetici

Il cifrario perfetto

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.



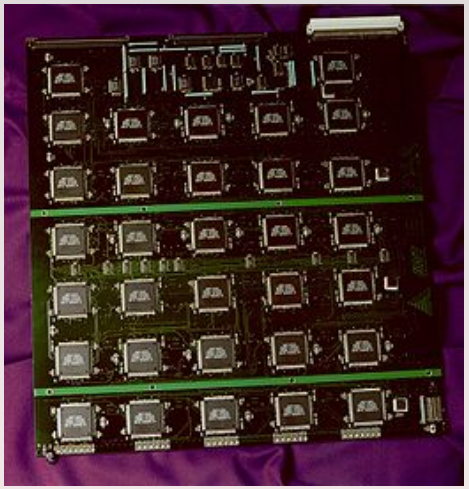


Sfruttando dei risultati dei matematici polacchi e progettando le "bombe" (ed in seguito il primo calcolatore elettronico a valvole termoioniche COLOSSUS) un team coordinato da Alan M. Turing (1912–1954) riuscì a forzare l'ENIGMA invertendo le sorti del conflitto.

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.

Introduzione

Cifrari monoalfabetici

Confondere la statistica

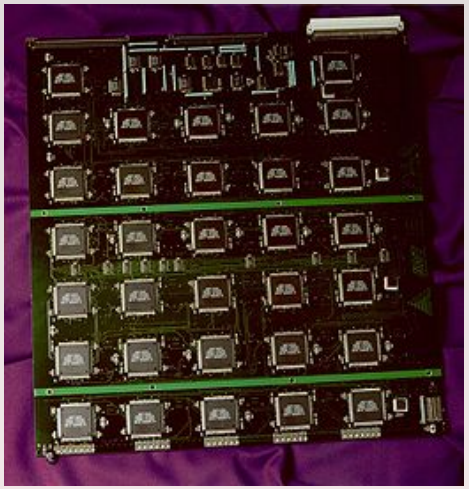
Cifrari polialfabetici

Il cifrario perfetto

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.

Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

Codici Segreti

Wikileaks

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

Poi c'è Anonymous . . .
Dicembre 2015: Hillary Clinton propone un
"Manhattan-like project" to break encryption

Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

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.

Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

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.

Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

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

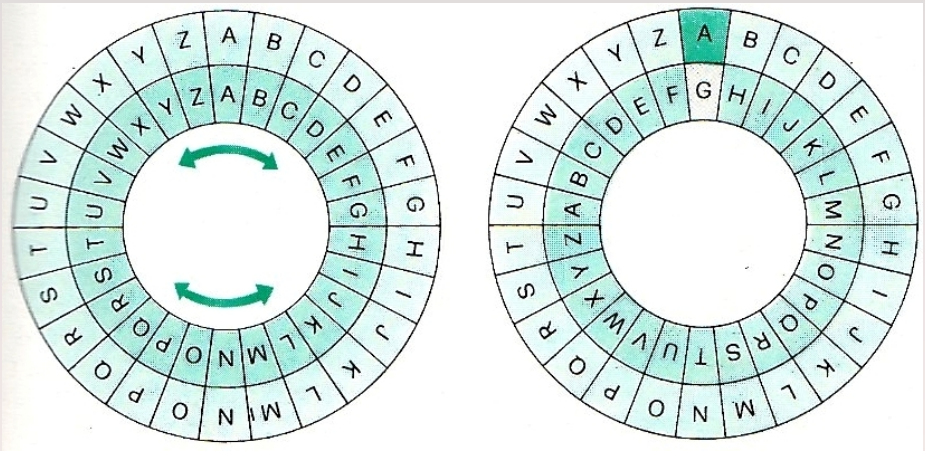
- L'operazione di cifratura avviene mediante l'applicazione di una sostituzione di lettere.
- Vi è dunque una funzione biiettiva

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

- 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)

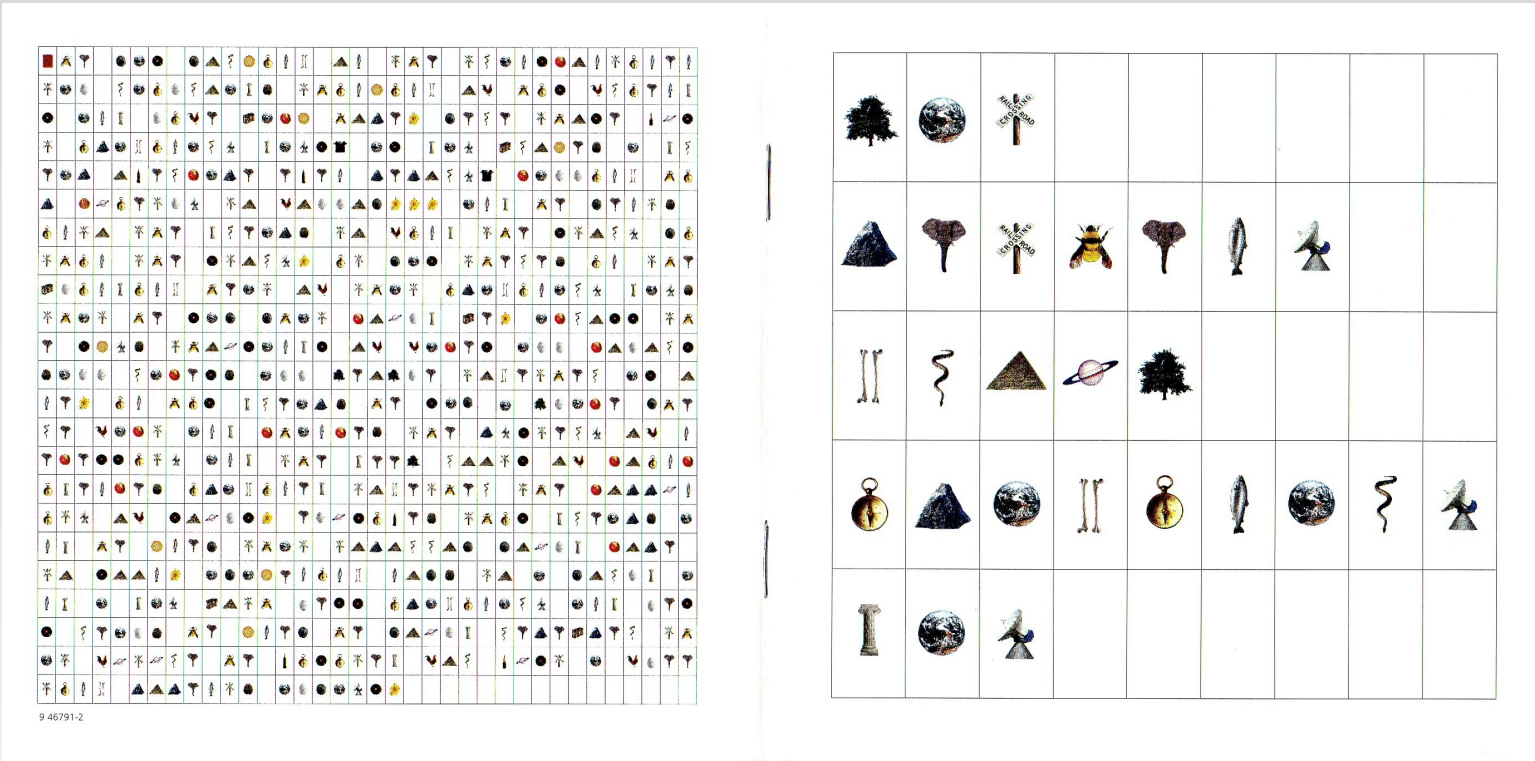


Cifrari a sostituzione monoalfabetica

Giovan Battista Della Porta (1535–1615)

Codici Segreti

Pat Metheny (1997)



Introduzione

Cifrari monoalfabetici

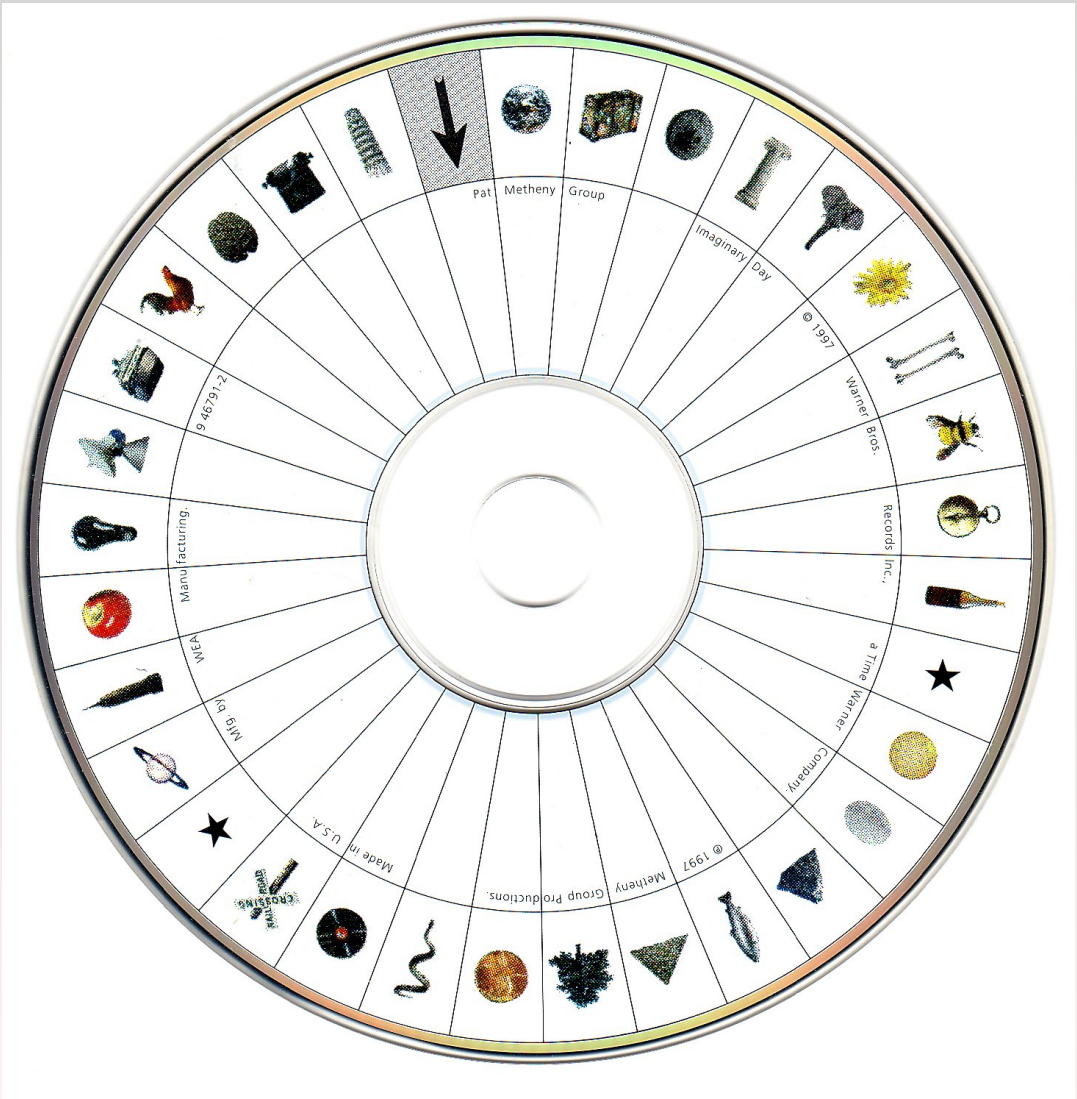
Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

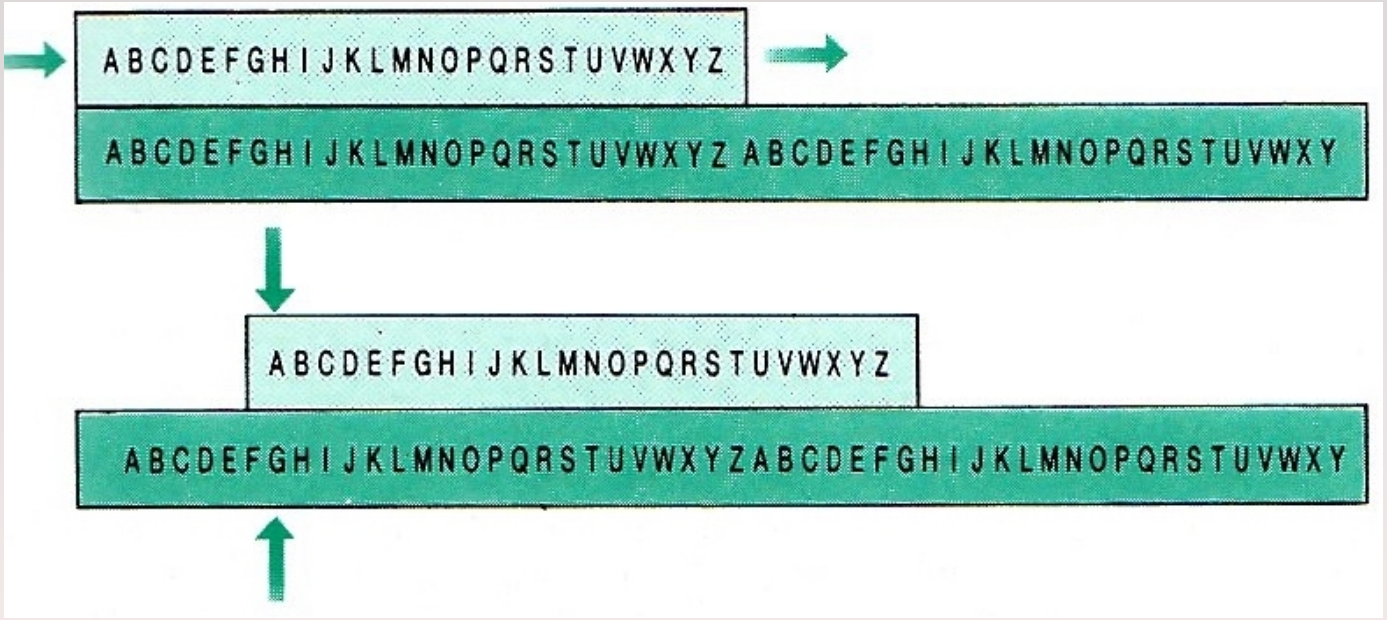
Codici Segreti

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.

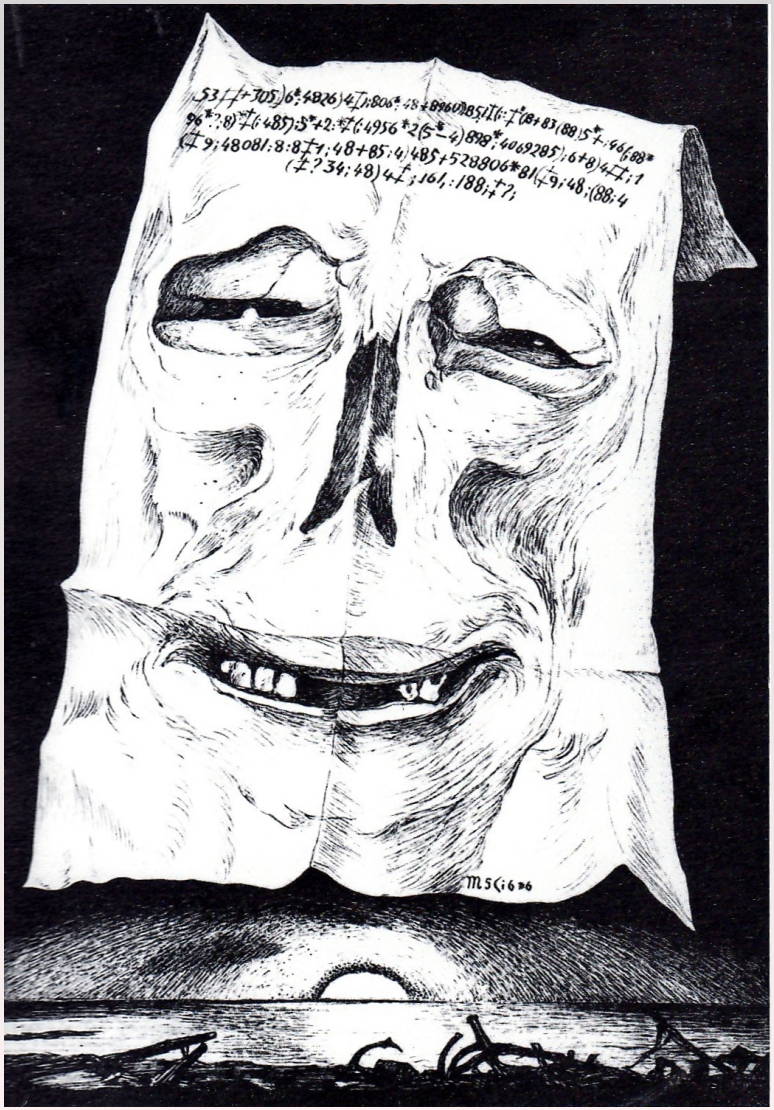
Cifrari a sostituzione monoalfabetici

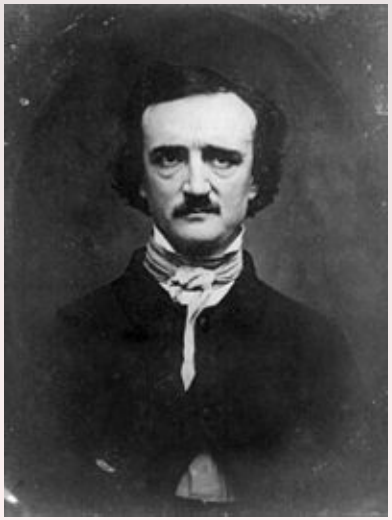
Cifrari completi

- 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

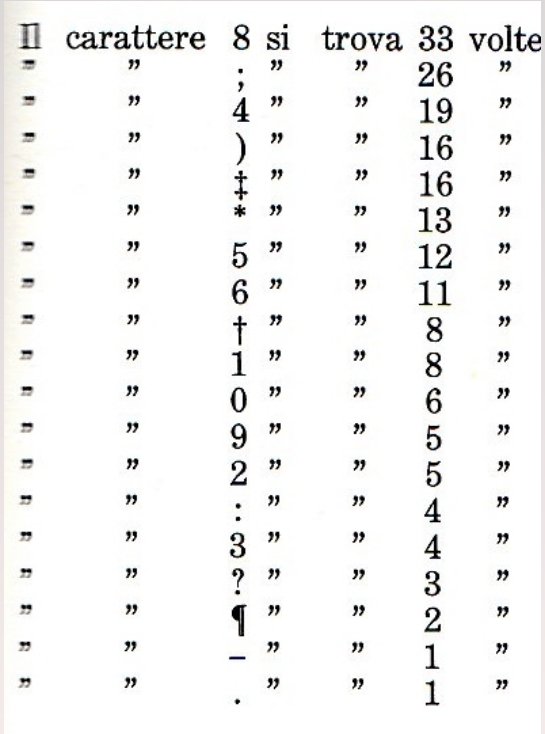




Cifrari a sostituzione monoalfabetica

Decrittazione

Viene usata la statistica linguistica.



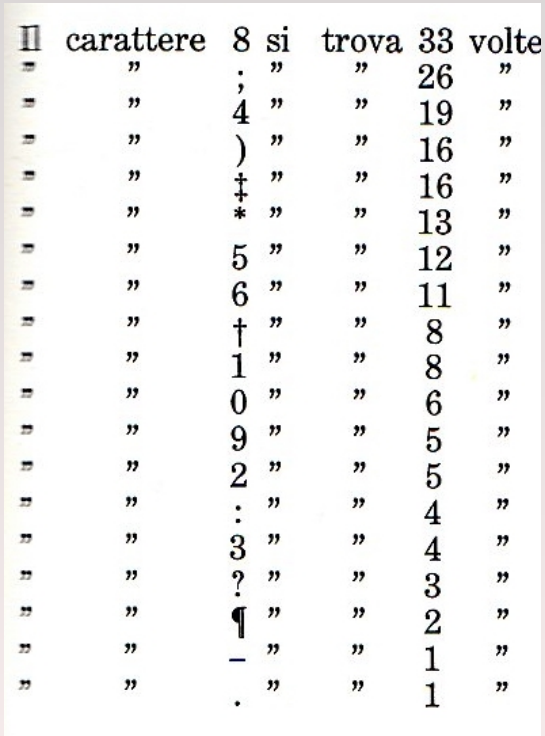
Il	carattere	8	si	trova	33	volte
=	”	;	”	”	26	”
=	”	4	”	”	19	”
=	”	)	”	”	16	”
=	”	‡	”	”	16	”
=	”	*	”	”	13	”
=	”	5	”	”	12	”
=	”	6	”	”	11	”
=	”	†	”	”	8	”
=	”	1	”	”	8	”
=	”	0	”	”	6	”
=	”	9	”	”	5	”
=	”	2	”	”	5	”
=	”	:	”	”	4	”
=	”	3	”	”	4	”
=	”	?	”	”	3	”
=	”	¶	”	”	2	”
=	”	–	”	”	1	”
”	”	.	”	”	1	”

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

Codici Segreti
A. Dovier
Introduzione
Cifrari monoalfabetici
Confondere la statistica
Cifrari polialfabetici
Il cifrario perfetto

- 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
A. DOVIER
INTRODUZIONE
CIFRARI MONOALFABETICI
CONFONDERE LA STATISTICA
CIFRARI POLIALFABETICI
IL CIFRARIO PERFETTO

Codici Segreti

Nomenclatori (omofonici)

Poi potevano essere ulteriormente cifrati.

Codici Segreti
A. Dovier
Introduzione
Cifrari monoalfabetici
Confondere la statistica
Cifrari polialfabetici
Il cifrario perfetto

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).

Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

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).

Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

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).

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

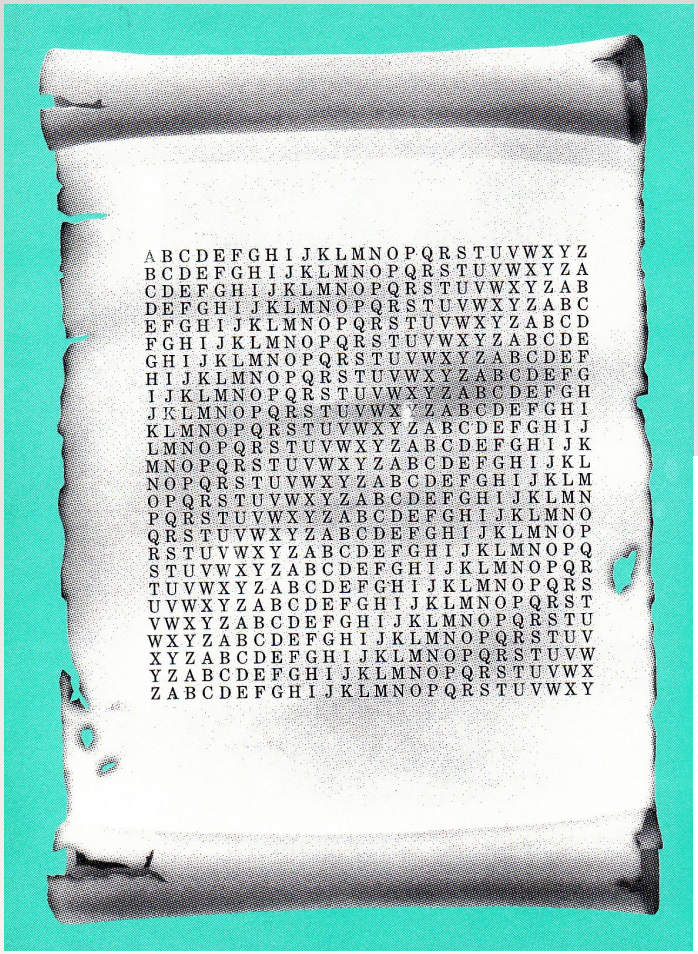
n indica l'iniziale della parola *n*-esima del testo.
Se non si conosce il testo chiave, e si evitano le ripetizioni, è un buon sistema.

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).

Codici Segreti
A. Dovier
Introduzione
Cifrari monoalfabetici
Confondere la statistica
Cifrari polialfabetici
Il cifrario perfetto

Cifrari a sostituzione polialfabetica

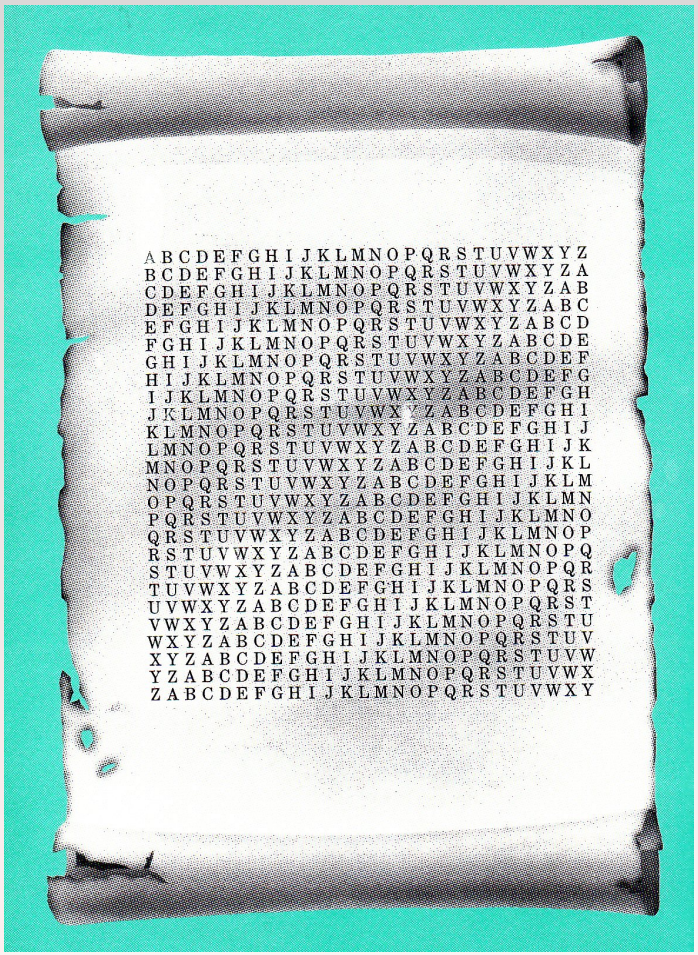
Blaise de Vigenère (1523–1596)



Cifrari a sostituzione polialfabetica

Cifrazione

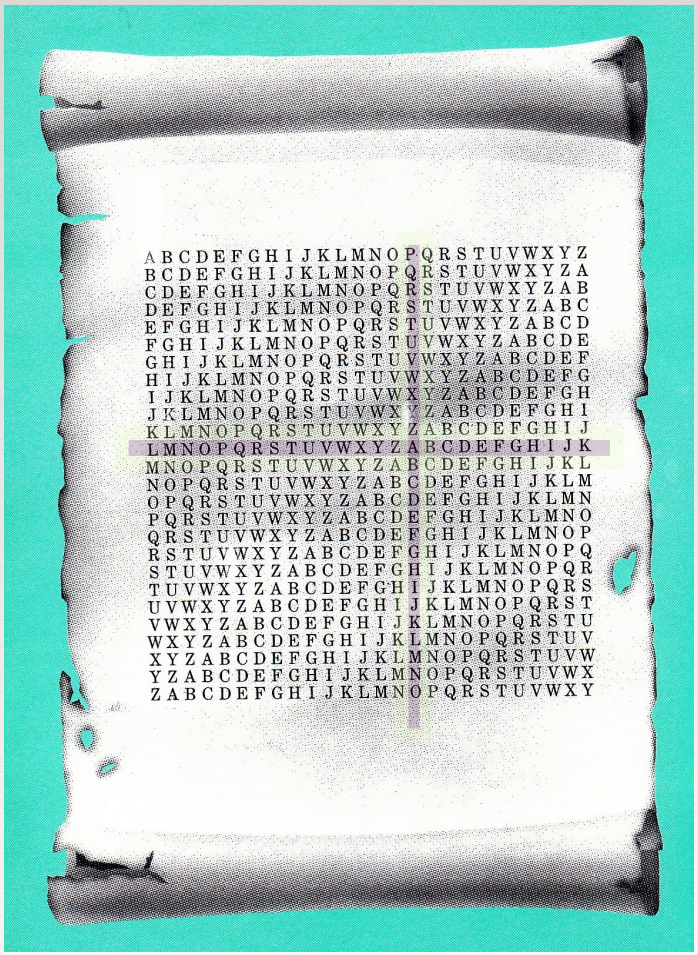
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

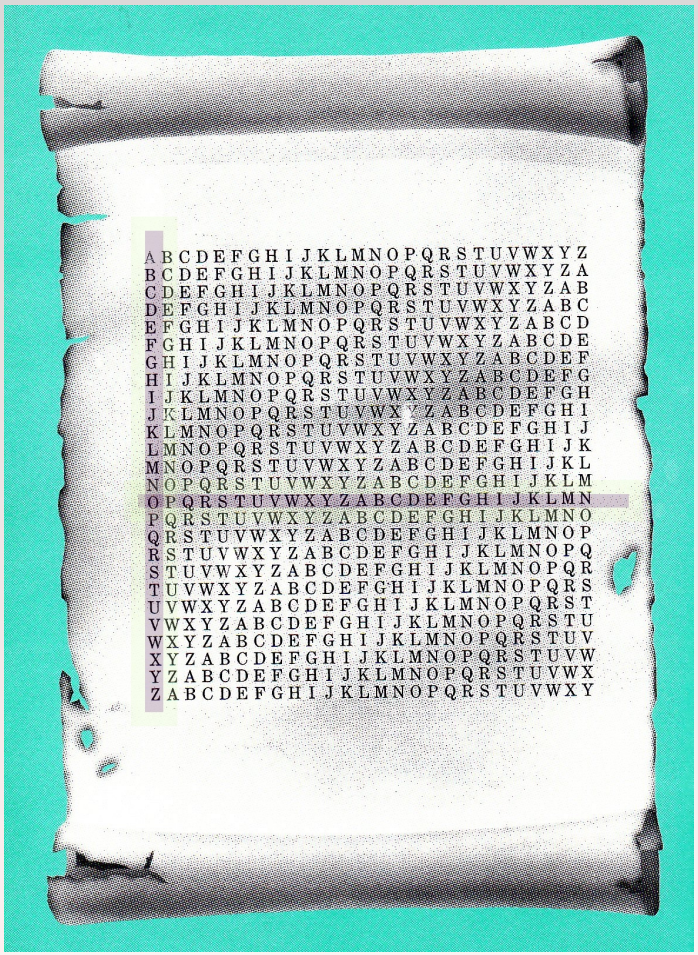
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

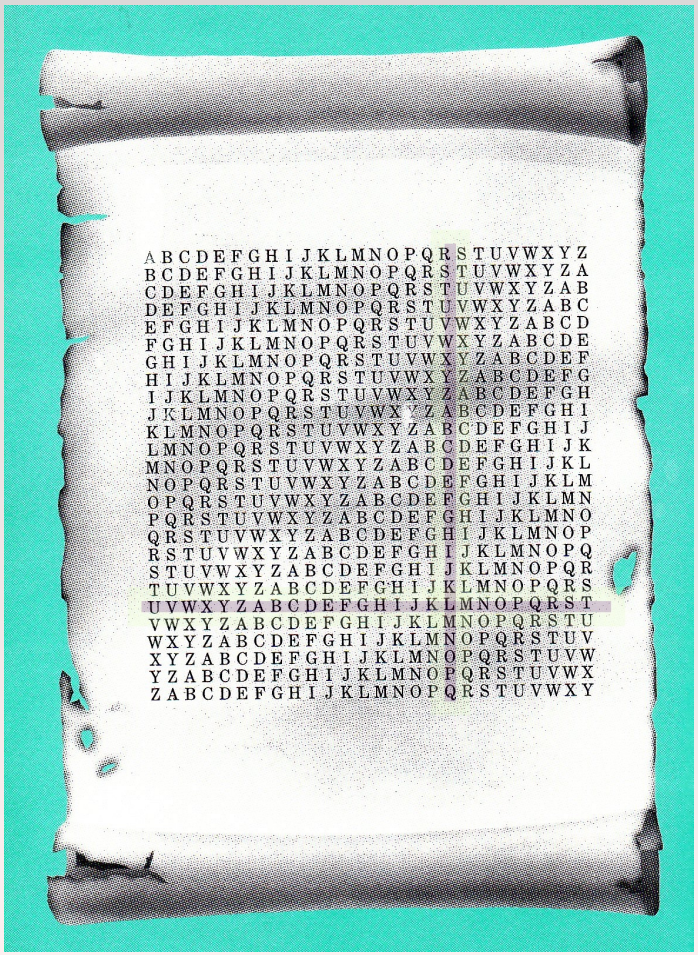
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

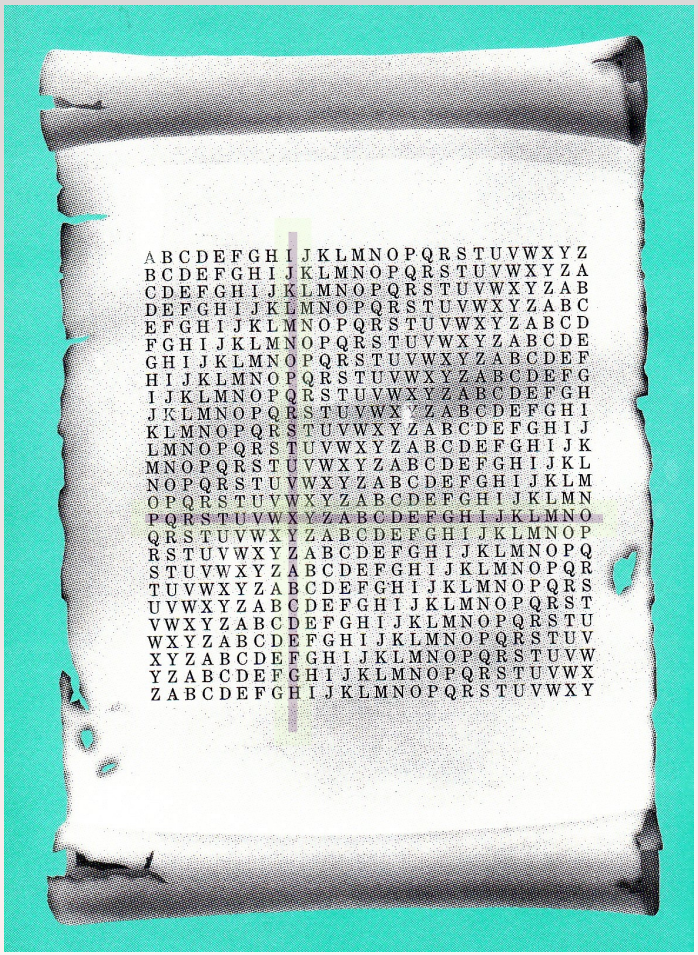
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

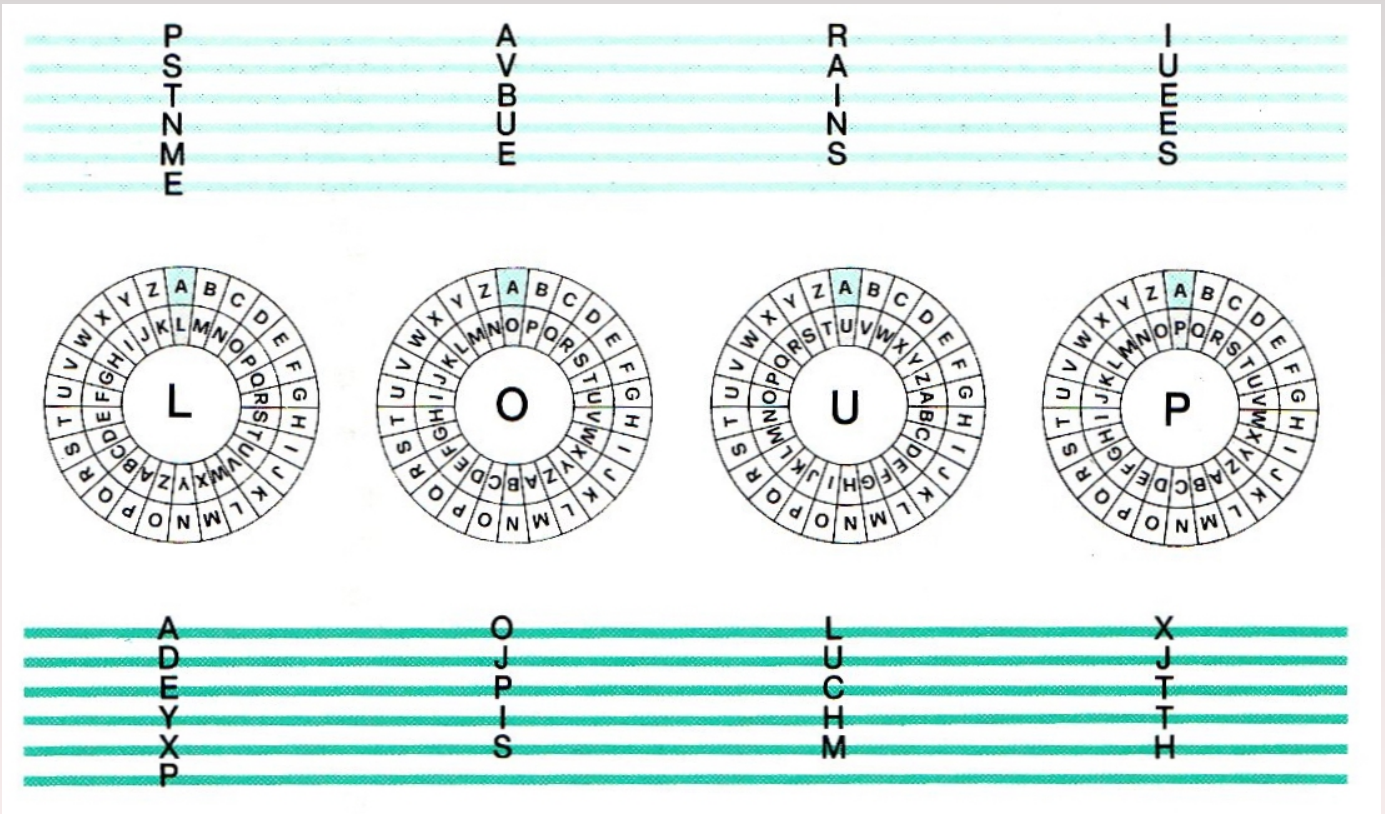
Cifrazione

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

Cifrazione



Cifrari a sostituzione polialfabetica

- E' 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

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

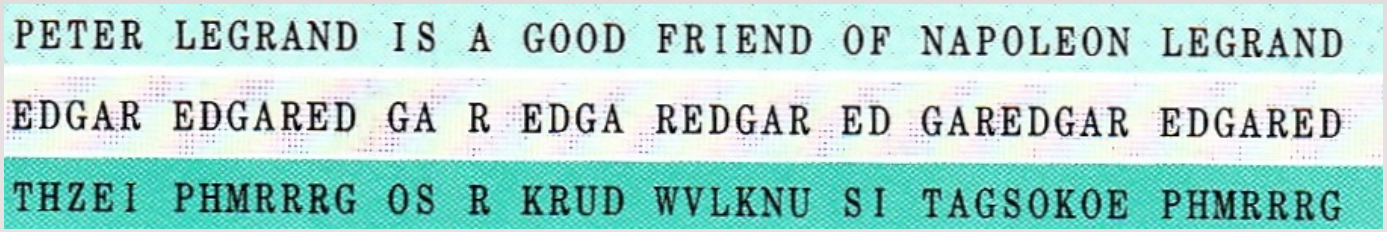
- Anche se su ogni lettera della chiave ci sono solo 21 scelte, in tutto ce ne sono ben 21^n.
- Inoltre la statistica sembra ingannata.
- E la spia non conosce nemmeno n (anche se potrebbe, in base a Kerchoffs).

Cifrari a sostituzione polialfabetica

Friedrich Kasiski (1805–1881): decrittatura (Babbage?)

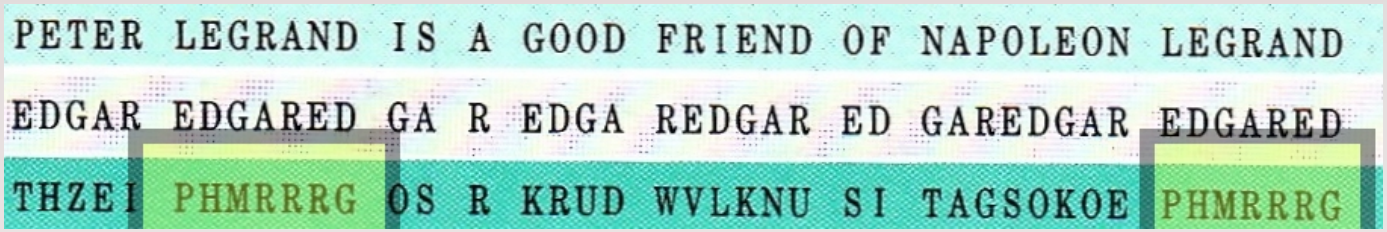
Cifrari a sostituzione polialfabetica

Friedrich Kasiski (1805–1881): decrittatura (Babbage?)



Cifrari a sostituzione polialfabetica

Friedrich Kasiski (1805–1881): decrittatura (Babbage?)



Cifrari a sostituzione polialfabetica

Altre vie

1. Per $i = 1, 2, \ldots,$ allineiamo il testo cifrato con sè stesso (spostato di i passi). Conta il numero di simboli coincidenti. Prendiamo i che massimizza tale numero e congetturiamo che i sia un multiplo della lunghezza della chiave.
2. Nell'esempio di prima viene trovata $i = 30$ con 7 contatti.
3. Nell'altro esempio invece il migliore era $i = 7$ ma anche 5,6, e 8 erano papabili (stringa troppo breve, comunque).
4. Congetturata la lunghezza, si cerca la chiave con la statistica.

Cifrari a sostituzione polialfabetica

Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Cifrari a sostituzione polialfabetica

Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```


Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

Cifrari a sostituzione polialfabetica

Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Cifrari a sostituzione polialfabetica

Metodo più generale

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

Cifrari a sostituzione polialfabetica

Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```


Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

Cifrari a sostituzione polialfabetica

Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

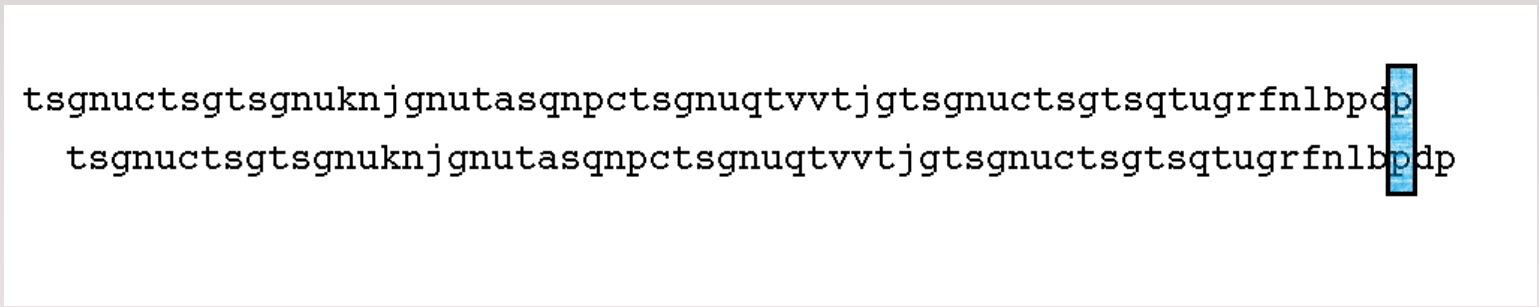
Cifrari a sostituzione polialfabetica

Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
  tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Cifrari a sostituzione polialfabetica

Metodo più generale



Cifrari a sostituzione polialfabetica

Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```


Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

Cifrari a sostituzione polialfabetica

Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Cifrari a sostituzione polialfabetica

Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
  tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

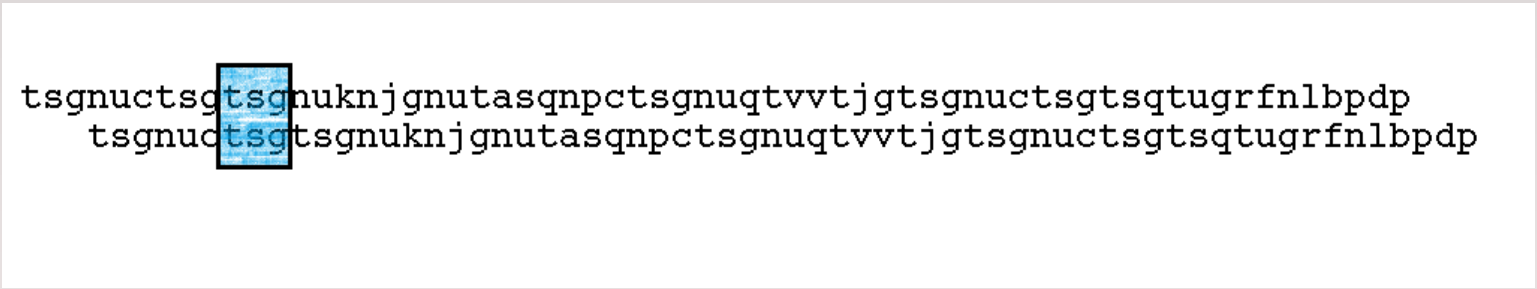
Cifrari a sostituzione polialfabetica

Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
   tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

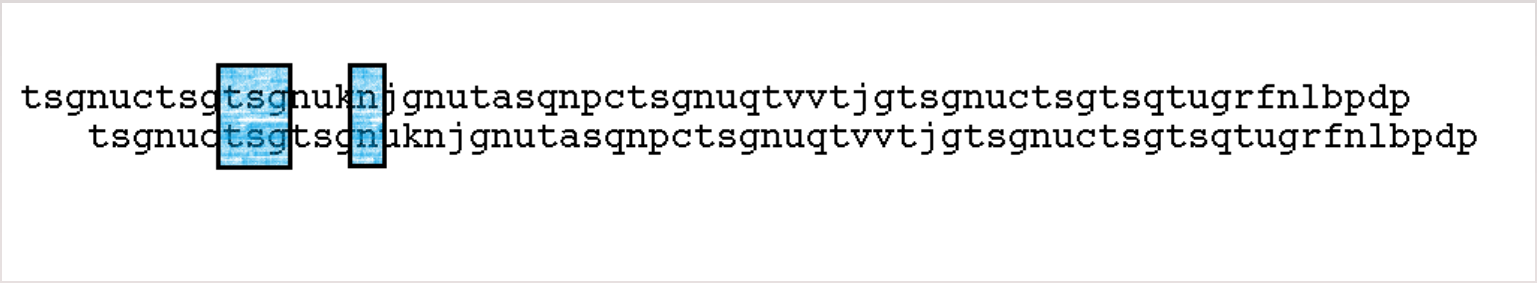
Cifrari a sostituzione polialfabetica

Metodo più generale



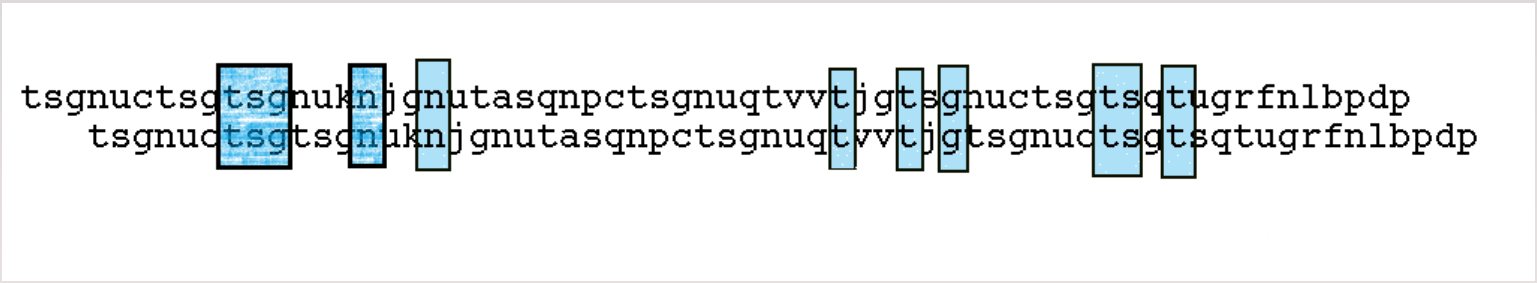
Cifrari a sostituzione polialfabetica

Metodo più generale



Cifrari a sostituzione polialfabetica

Metodo più generale



Cifrari a sostituzione polialfabetica

Metodo più generale

Per $i = 1, 2, \ldots,$ allineiamo il testo cifrato con sè stesso (spostato di i passi). Contiamo il numero di simboli coincidenti. Prendiamo i che massimizza tale numero e congetturiamo che i sia un multiplo della lunghezza della chiave.

Introduzione

Cifrari monoalfabetici

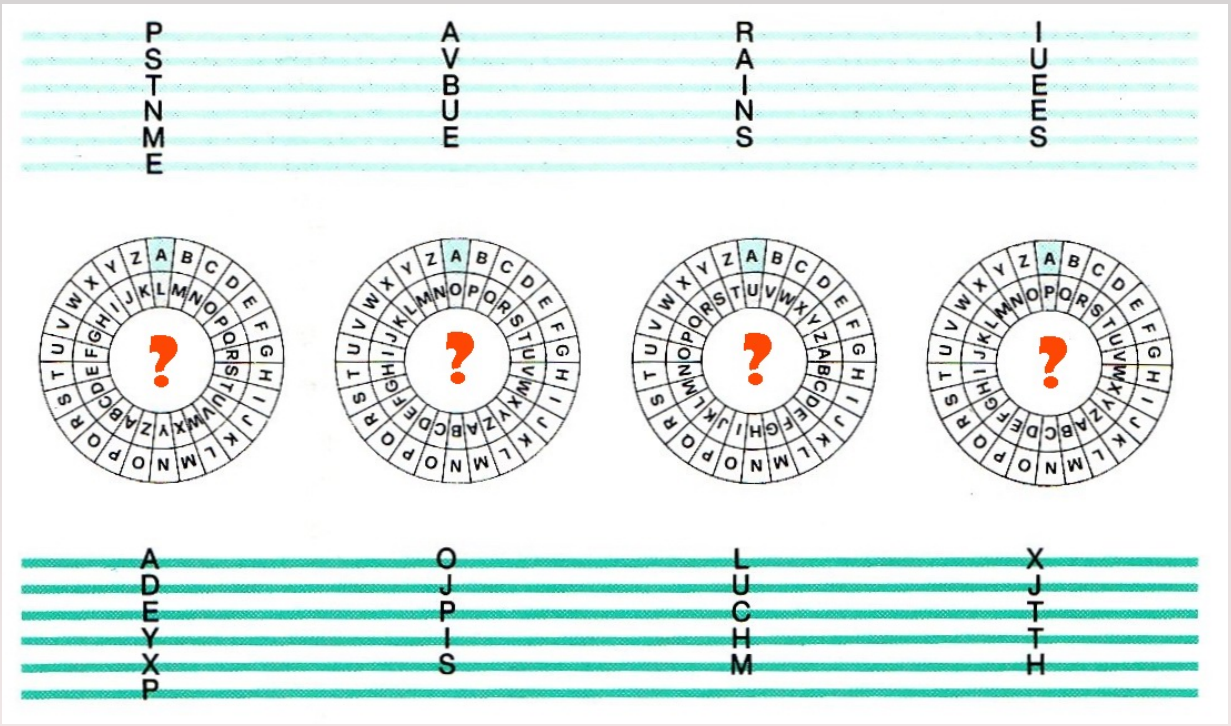
Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

Cifrari a sostituzione polialfabetica

Decrittazione

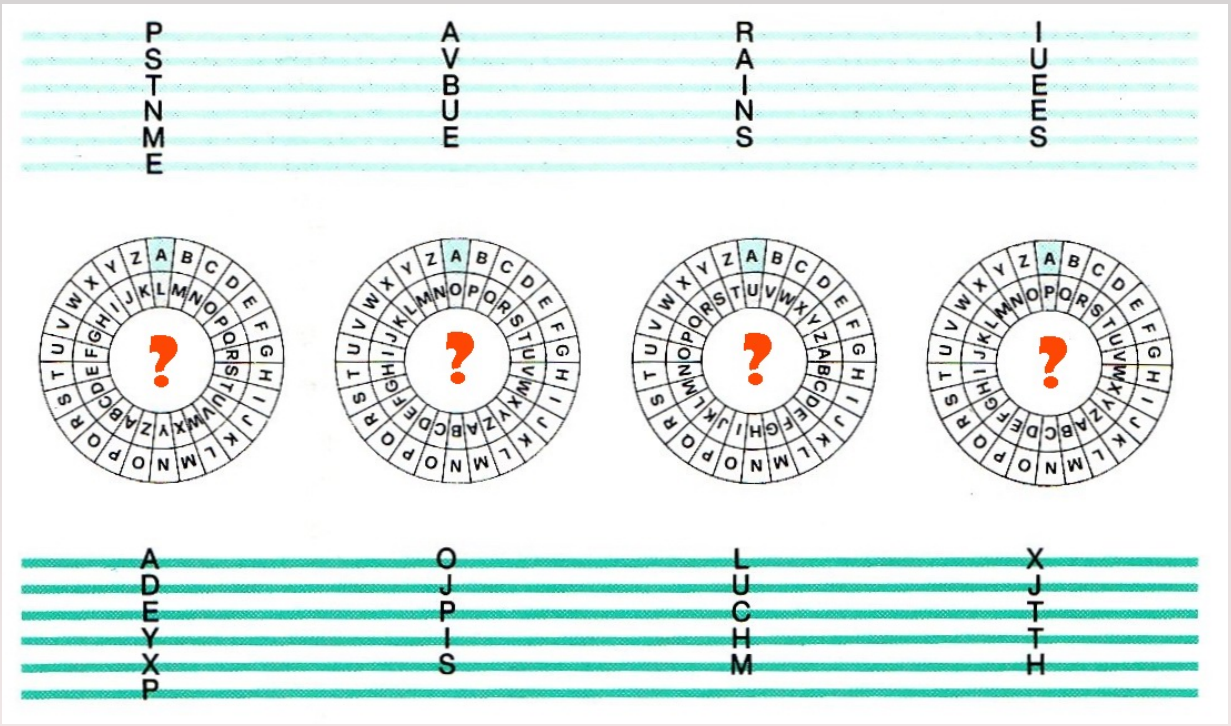


Partiziono il testo usando la lunghezza della chiave e applico la statistica ad ogni partizione.

Capiamo ora (1) perchè funziona e (2) vediamo un programmino che automatizza il task.

Cifrari a sostituzione polialfabetica

Decrittazione



Partiziono il testo usando la lunghezza della chiave e applico la statistica ad ogni partizione.

Capiamo ora (1) perchè funziona e (2) vediamo un programmino che automatizza il task.

Cifrari a sostituzione polialfabetica

Decrittazione

- Sia $P = (p_0, \ldots, p_{25})$ la probabilità di ogni lettera (per semplicità supponiamo le lettere siano 0,. . . ,25) nella lingua in cui è scritto il messaggio.
- Prendo il testo in chiaro. Fissiamo una posizione. Avremo che $P(X = x) = p_x$.
- Supponiamo di usare uno shift di 1 ($a \mapsto b$), allora nella stessa posizione,

$$\underbrace{P(Y = b)}_{\textit{msg in codice}} = \underbrace{P(X = a)}_{\textit{msg in chiaro}}$$

- E' come se ci fosse ora un vettore di probabilità $P^1 = (p_{25}, p_0, p_1, \ldots, p_{24})$.
- In generale, se vi è stato shift di $j > 0$, ci sarà un vettore: $P^j = (p_{26-j}, \ldots, p_{25}, p_0, p_1, \ldots, p_{25-j})$ (e $P^0 = P$).

Cifrari a sostituzione polialfabetica

Decrittazione

- Ora consideriamo il crittogramma allineato con sè stesso. Prendiamo una cella. Nella prima riga sarà X che avrà subito una sostituzione δ, nella seconda sarà Y una sostituzione γ (entrambe ignote)
- Avremo che

$$\begin{array}{llll} P(X=0)=P_0^\delta & P(X=1)=P_1^\delta & \dots & P(X=25)=P_{25}^\delta \\ P(Y=0)=P_0^\gamma & P(Y=1)=P_1^\gamma & \dots & P(Y=25)=P_{25}^\gamma \end{array}$$

- Pertanto

$$P(X=Y)=P_0^\delta P_0^\gamma + P_1^\delta P_1^\gamma + \cdots + P_{25}^\delta P_{25}^\gamma = \vec{P}^\delta \cdot \vec{P}^\gamma$$

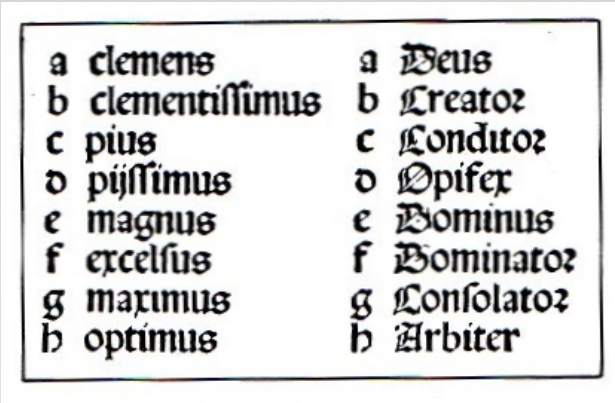
- Proprietà (esercizio). Se $\vec{V}$ è un vettore di numeri non negativi, e $\vec{V}'$ è una sua permutazione, allora $\vec{V}\vec{V} \geq \vec{V}\vec{V}'$.
- $P(X=Y)=\vec{P}^\delta \cdot \vec{P}^\gamma$ dipende solo da $|\delta-\gamma|$ ed è max se $\delta=\gamma$
- La probabilità di avere accoppiamenti è massima se lo shift della seconda stringa è tale da allineare le chiavi.

Codici Segreti

Johannes Trithemius (1462–1516)

Codici Segreti

Johannes Trithemius (1462–1516)



a clemens	a Deus
b clementiſſimus	b Creator
c pius	c Conditor
d piiſſimus	d Opifex
e magnus	e Dominus
f excelſus	f Dominator
g maximus	g Conſolator
h optimus	h Arbiter

- Usa steganografia con significati magici/religiosi (vedi cifrario Ave Maria—Steganographia)
- Usa il quadro di Vigenère (anzi, l'ha inventato lui in Polygraphiae libri sex).
- Lo usa ciclando le righe (senza chiave, o meglio con chiave fissa ABCDE . . .).

Gronsfeld: Vigenère “ridotto”.

0	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
1	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	A
2	C	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
3	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
4	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	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Étienne Bazeries (1892) lo decritta facendo arrestare un gruppo di anarchici francesi.

CODICI SEGRETI

A. DOVIER

INTRODUZIONE

CIFRARI MONOALFABETICI

CONFONDERE LA STATISTICA

CIFRARI POLIALFABETICI

IL CIFRARIO PERFETTO

Gronsfeld: Vigenère “ridotto”.

0	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
1	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	A
2	C	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
3	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
4	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	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Étienne Bazeries (1892) lo decritta facendo arrestare un gruppo di anarchici francesi.

CODICI SEGRETI
A. DOVIER
INTRODUZIONE
CIFRARI MONOALFABETICI
CONFONDERE LA STATISTICA
CIFRARI POLIALFABETICI
IL CIFRARIO PERFETTO

Codici Segreti

Il cifrario del Porta

AB	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
ED	A	B	C	D	E	F	G	H	I	J	K	L	M
	Z	N	O	P	Q	R	S	T	U	W	V	X	Y
EF	A	B	C	D	E	F	G	H	I	J	K	L	M
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
GH	A	B	C	D	E	F	G	H	I	J	K	L	M
	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
IJ	A	B	C	D	E	F	G	H	I	J	K	L	M
	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
KL	A	B	C	D	E	F	G	H	I	J	K	L	M
	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
MN	A	B	C	D	E	F	G	H	I	J	K	L	M
	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
OP	A	B	C	D	E	F	G	H	I	J	K	L	M
	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
QR	A	B	C	D	E	F	G	H	I	J	K	L	M
	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
ST	A	B	C	D	E	F	G	H	I	J	K	L	M
	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
UV	A	B	C	D	E	F	G	H	I	J	K	L	M
	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
WX	A	B	C	D	E	F	G	H	I	J	K	L	M
	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
YZ	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	N

- Si creano 13 permutazioni cicliche delle seconde 13 lettere come a lato.
- Le lettere A e B sono codificate usando un cifrario a sostituzione che parte dalla N
- Le lettere E e D sono codificate usando un cifrario a sostituzione che parte dalla Z
- . . .

Codici Segreti
A. Dovier
Introduzione
Cifrari monoalfabetici
Confondere la statistica
Cifrari polialfabetici
Il cifrario perfetto

Codici Segreti

Il cifrario del Porta

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

Codici Segreti

Francis Beaufort (1774–1857)

- In Vigenere: crittogramma = chiave + messaggio
- In Beaufort n. 1: crittogramma = chiave - messaggio,
- In Beaufort n. 2: crittogramma = messaggio + chiave.
- Si va verso l'algebrizzazione della crittografia.

Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

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: JJOVPWOMMMIRMRRJLWFF
(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

Codici Segreti
A. Dovier
Introduzione
Cifrari monoalfabetici
Confondere la statistica
Cifrari polialfabetici
Il cifrario perfetto

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.
- Come comunichiamo la chiave?

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.
- Come comunichiamo la chiave?

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.
- Come comunichiamo la chiave?

Il cifrario perfetto

C. E. Shannon: Communication Theory of Secrecy Systems (1949)

- Il crittografo sa quasi tutto:
  - sistema di cifratura,
  - elenco $m_1, \ldots, m_\ell$ dei messaggi in chiaro possibili,
  - loro probabilità $P(M = m)$ a priori,
  - elenco di chiavi possibili,
  - elenco $e_1, \ldots, e_\ell$ di messaggi crittati possibili e,
  - la probabilità a posteriori $P(M = m|E = e)$ (la calcola usando ogni chiave possibile).
- Non sa la chiave.

Definition

Un cifrario è *perfetto* se per ogni coppia e, m

$$P(M = m|E = e) = P(M = m)$$

Il cifrario perfetto

C. E. Shannon: Communication Theory of Secrecy Systems (1949)

Theorem

Il cifrario one-time-pad è un cifrario perfetto.

- Sappiamo che $P(M = m|E = e) = \frac{P(E=e|M=m)P(M=m)}{P(E=e)}$
- Sappiamo che nel one-time-pad la monetina fa sí che $P(E = e|M = m) = P(E = e)$
- Dunque $P(M = m|E = e) = P(M = m)$: il cifrario è perfetto

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

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.

Introduzione

Cifrari monoalfabetici

Confondere la statistica

Cifrari polialfabetici

Il cifrario perfetto

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.

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.