CODICI SEGRETI

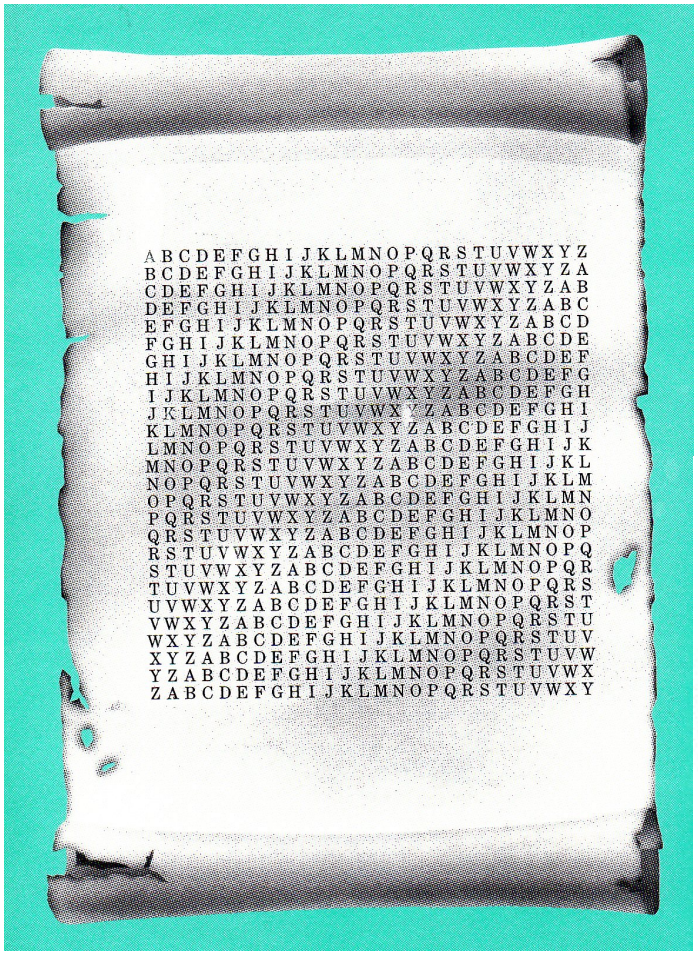
Agostino Dovier

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

Cifrari a sostituzione polialfabetica

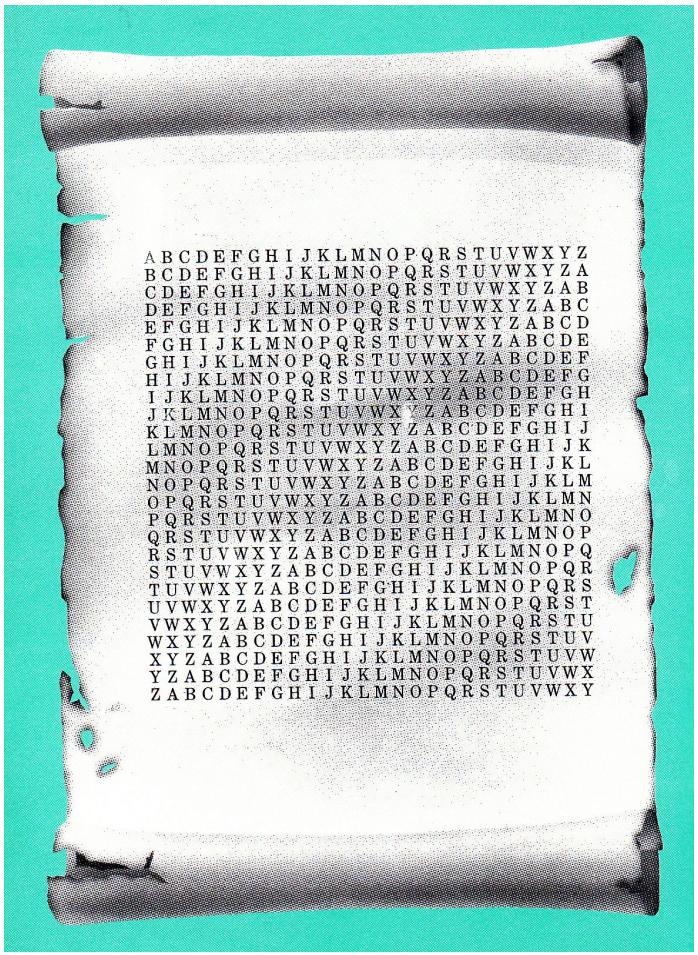
Blaise de Vigenère (1523–1596)



Cifrari a sostituzione polialfabetica

Cifrazione

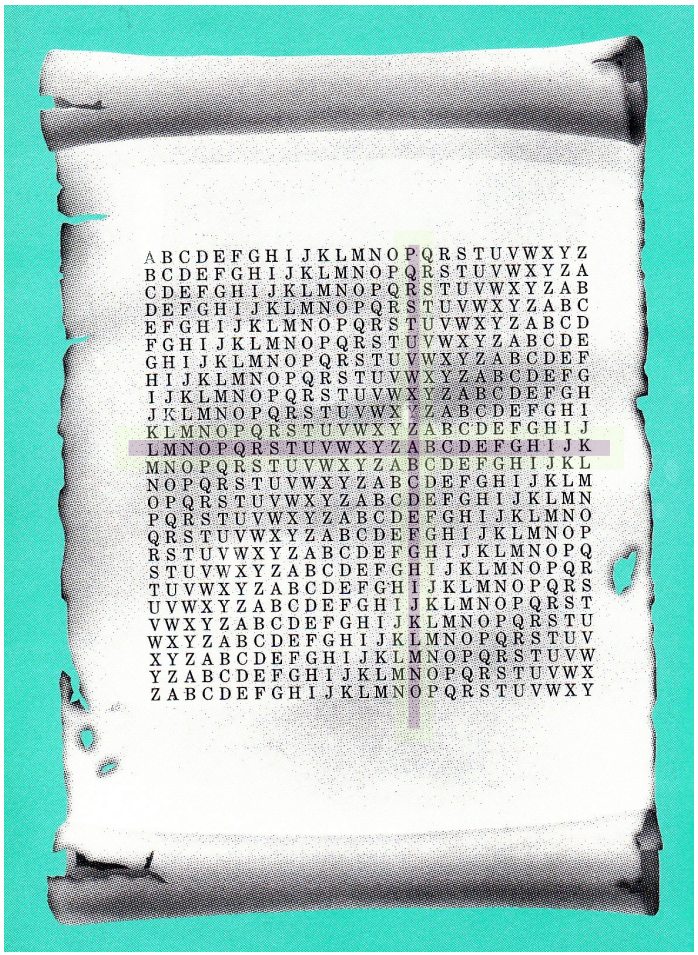
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

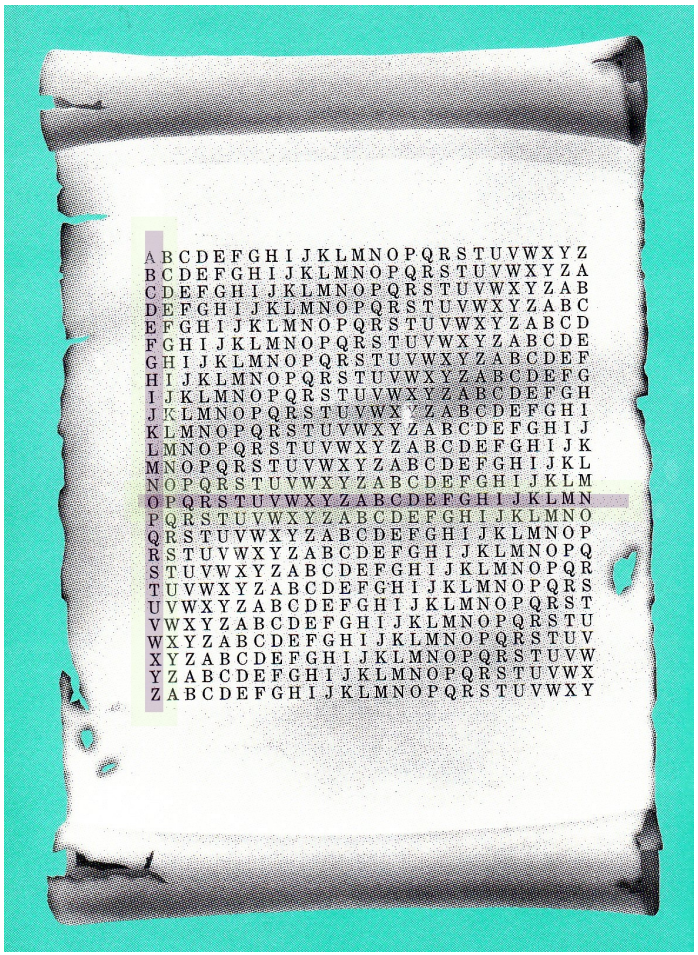
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

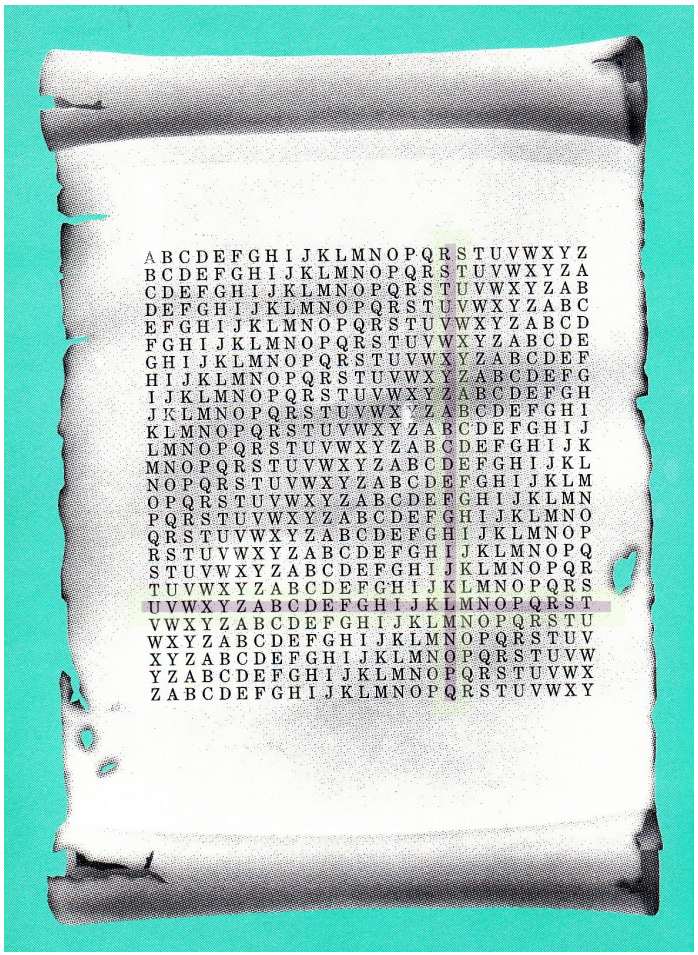
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

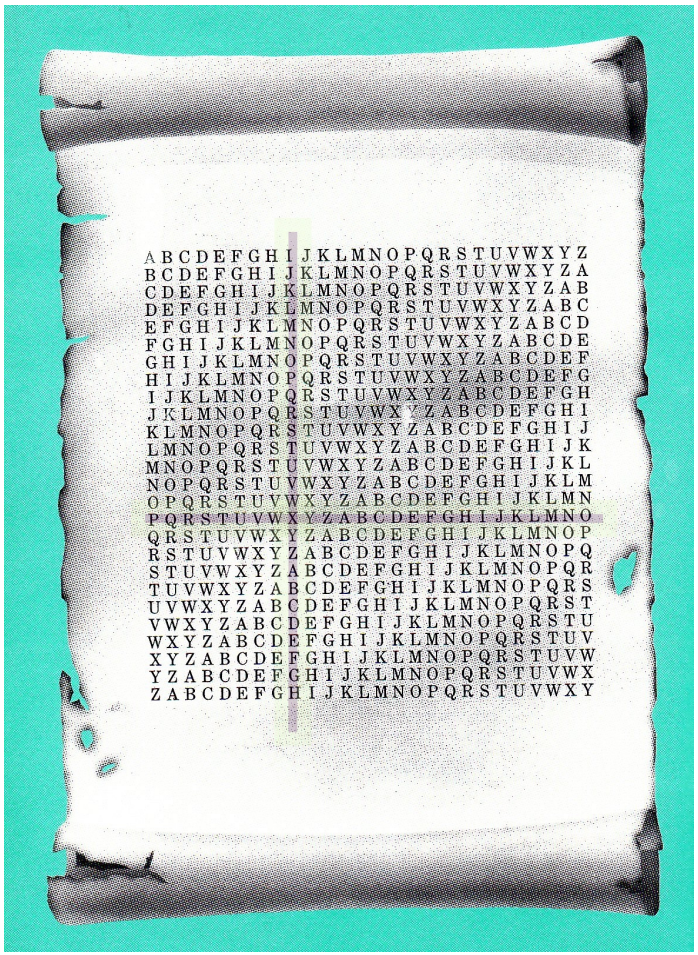
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

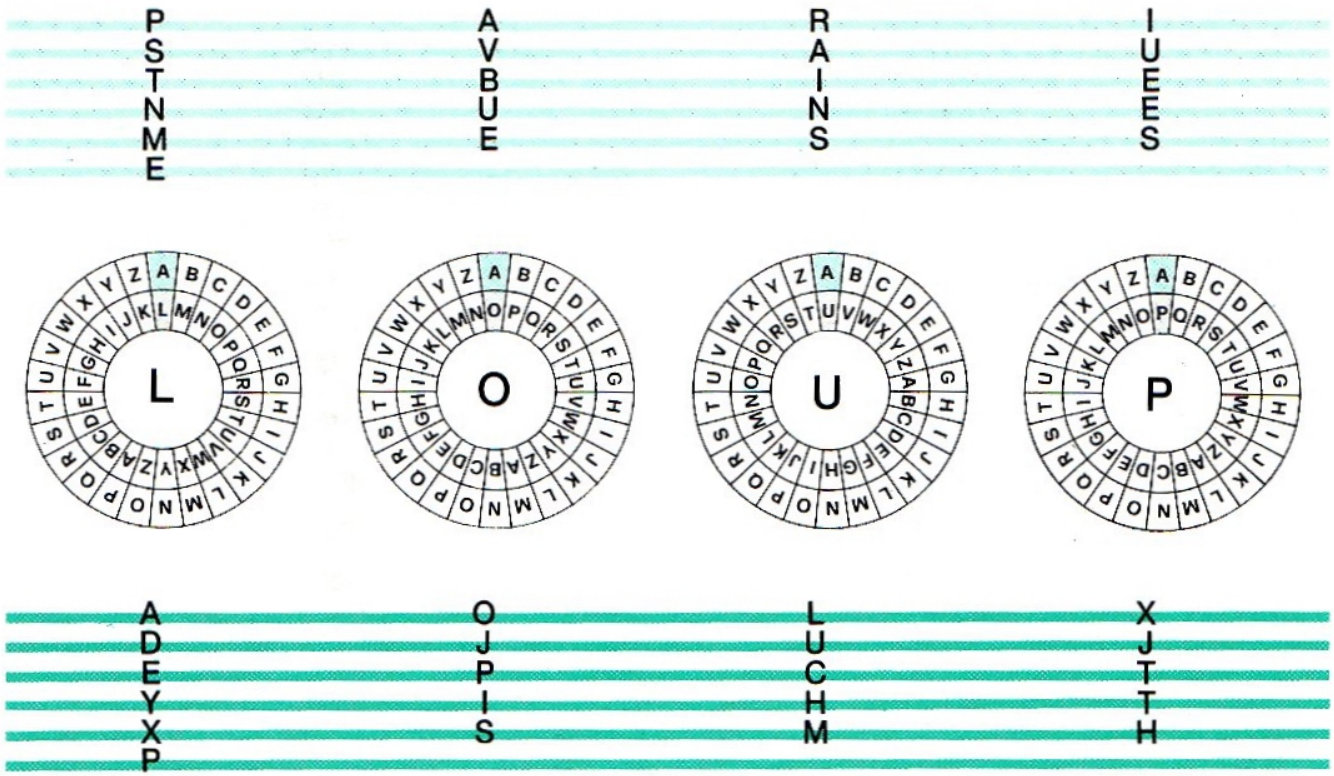
Cifrazione

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.

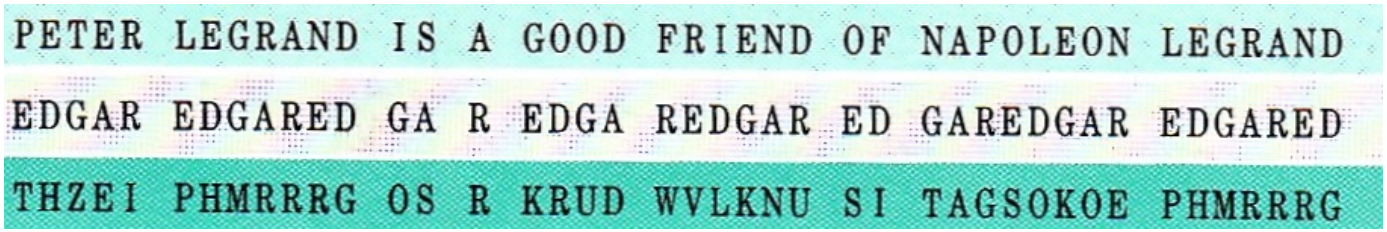
Cifrari a sostituzione polialfabetica

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

```
PETER LEGRAND IS A GOOD FRIEND OF PAUL LEGRAND
EDGAR EDGARED GA R EDGA REDGAR ED GARE DGAREDG
THZEI PHMRRRG OS R KRUD WVLKNU SI VALP OKGIEQJ
```

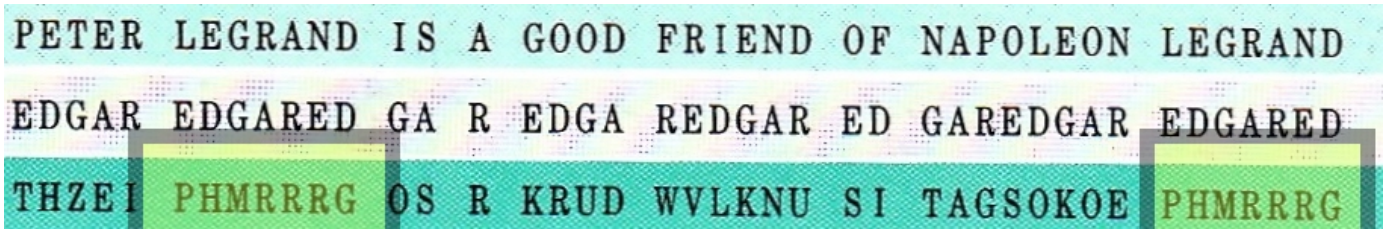
Cifrari a sostituzione polialfabetica

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



Cifrari a sostituzione polialfabetica

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



Cifrari a sostituzione polialfabetica

Metodo più generale


```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Cifrari a sostituzione polialfabetica

Metodo più generale

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

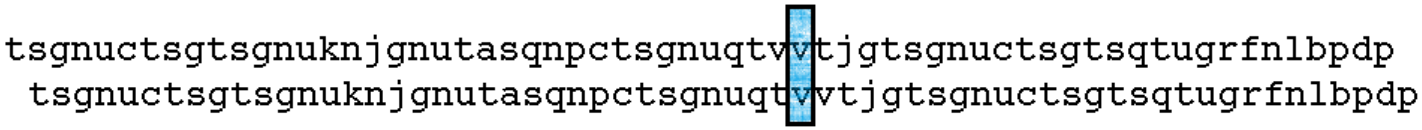
Cifrari a sostituzione polialfabetica

Metodo più generale


```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Cifrari a sostituzione polialfabetica

Metodo più generale



Cifrari a sostituzione polialfabetica

Metodo più generale

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

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


```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
  tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

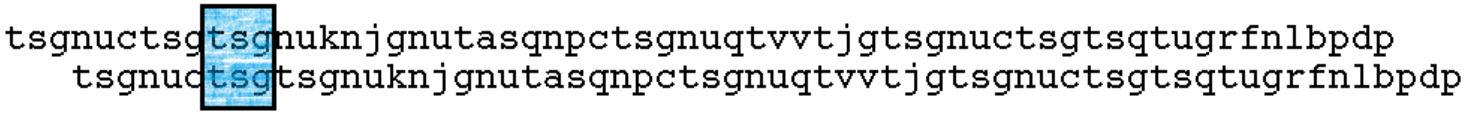
Cifrari a sostituzione polialfabetica

Metodo più generale


```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
   tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

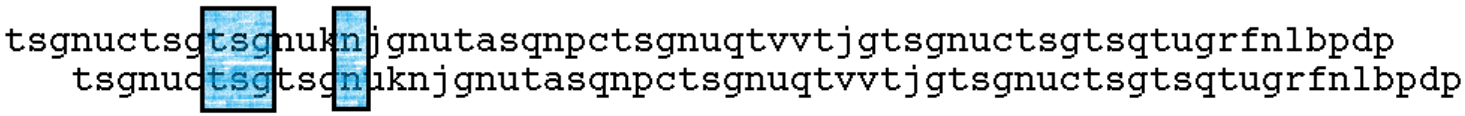
Cifrari a sostituzione polialfabetica

Metodo più generale



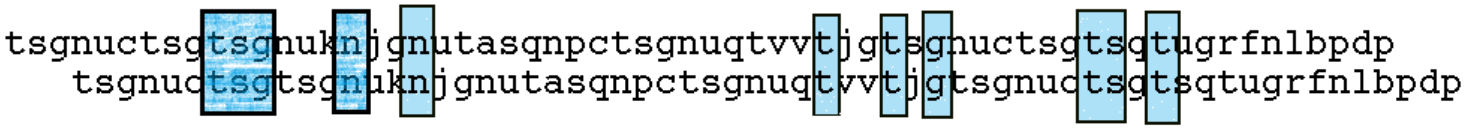
Cifrari a sostituzione polialfabetica

Metodo più generale



Cifrari a sostituzione polialfabetica

Metodo più generale



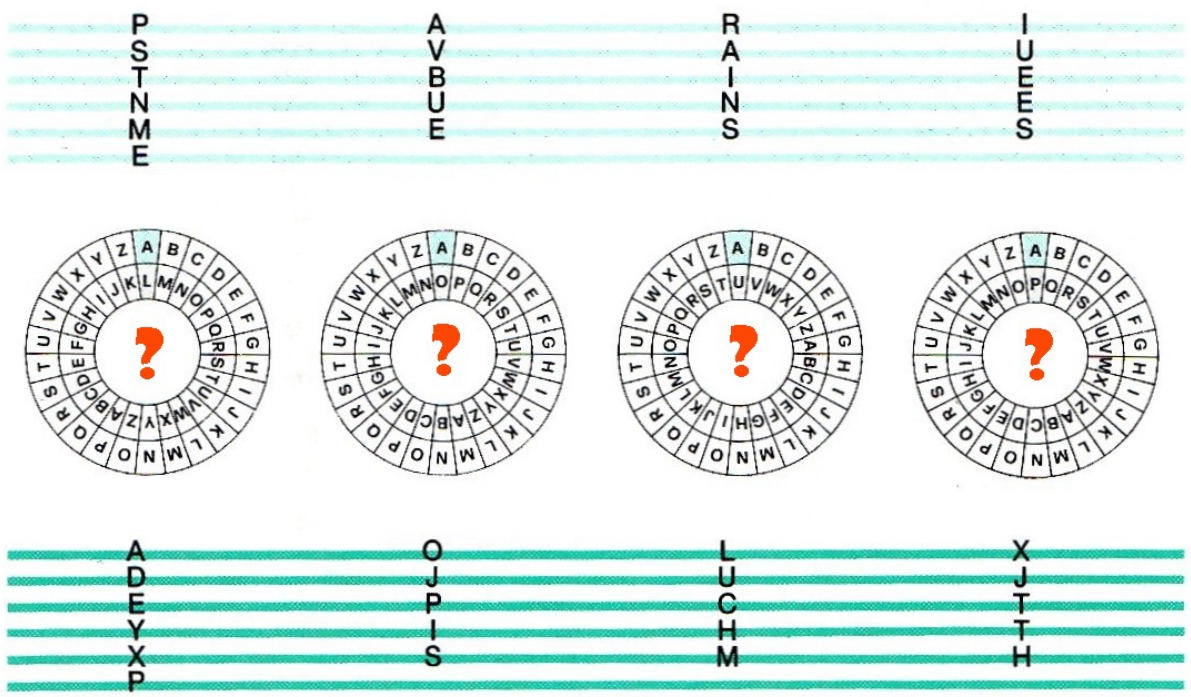
Cifrari a sostituzione polialfabetica

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.

Cifrari a sostituzione polialfabetica

Decrittazione

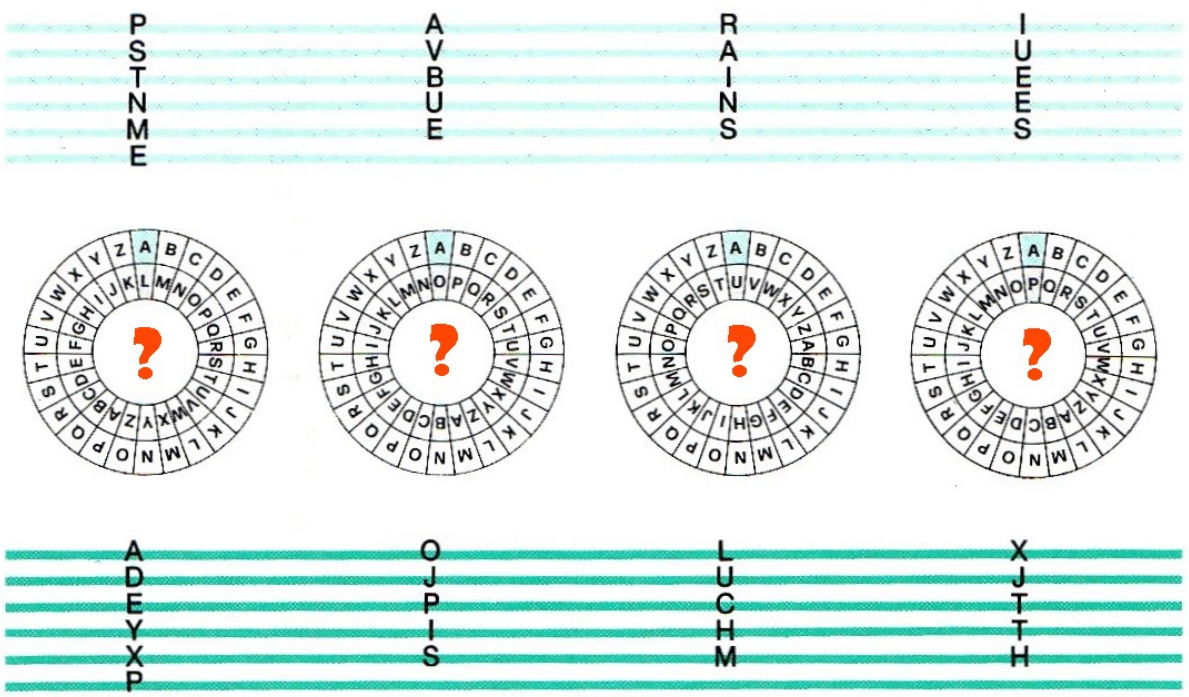


Partiziono il testo usando la lunghezza della chiave e applico la statistica ad ogni partizione.

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

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

- Pertanto

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

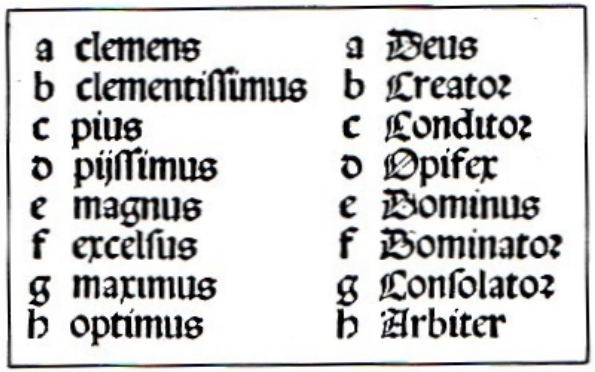
- Proprietà (esercizio). Se $\vec{V}$ è un vettore di numeri non negativi, e $\vec{V}'$ è una sua permutazione, allora $\vec{V}\vec{V} \geq \vec{V}\vec{V}'$.
- $P(X=Y)=\vec{P}^\delta \cdot \vec{P}^\gamma$ dipende solo da $|\delta-\gamma|$ ed è max se $\delta=\gamma$
- La probabilità di avere accoppiamenti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

CODICI SEGRETI

VARIANTI DI VIGENÈRE

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.

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

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

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