CODICI SEGRETI: UN VIAGGIO NELLA CRITTOGRAFIA

Agostino Dovier

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

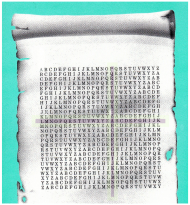
Febbraio 2017

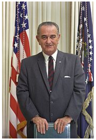
Preistoria e storia

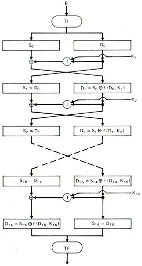
aleph	beth	gimel	daleth	he	waw	zayin	heth	teth	yod	kaph
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ
taw	sin shin	resh	qoph	sadhe	pe	ayin	samkeh	nun	mem	lamed
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל

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

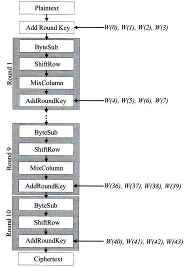
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L





B
TI
S_0
D_0
f
K_1
$S_1 = D_0$
$D_1 = S_0 \oplus f(D_0, K_1)$
K_2
$S_2 = D_1$
$D_2 = S_1 \oplus f(D_1, K_2)$
$S_{15} = D_{14}$
$D_{15} = S_{14} \oplus f(D_{14}, K_{15})$
K_{16}
$D_{16} = S_{15} \oplus f(D_{15}, K_{16})$
$S_{16} = D_{15}$
TF

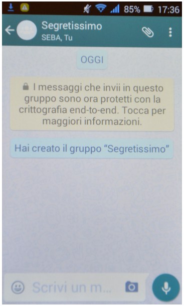


Plaintext
Add Round Key
W(0), W(1), W(2), W(3)
Round 1
ByteSub
ShiftRow
MixColumn
AddRoundKey
W(4), W(5), W(6), W(7)
Round 9
ByteSub
ShiftRow
MixColumn
AddRoundKey
W(36), W(37), W(38), W(39)
Round 10
ByteSub
ShiftRow
AddRoundKey
W(40), W(41), W(42), W(43)
Ciphertext

ALGORITMO RSA
Ron Rivest, Adi Shamir e Leonard Adleman
1977, Massachussets Institute of Technology (MIT), Cambridge


WikiLeaks


YOU HAVE
BEEN HACKED


85% 17:36
Segretissimo
SEBA, Tu
OGGI
I messaggi che invii in questo gruppo sono ora protetti con la crittografia end-to-end. Tocca per maggiori informazioni.
Hai creato il gruppo "Segretissimo"
Scrivi un m...

CODICI SEGRETI

La nostra storia è da sempre piena di esempi di utilizzo di *codici* per nascondere l'informazione a tutti tranne che al desiderato destinatario.

La profezia di Daniele
MENE TEKEL PERES
(V Libro del profeta Daniele)
$\Leftarrow$ Rembrand: il festino di Baldassarre

ATBASH (Ebraico)

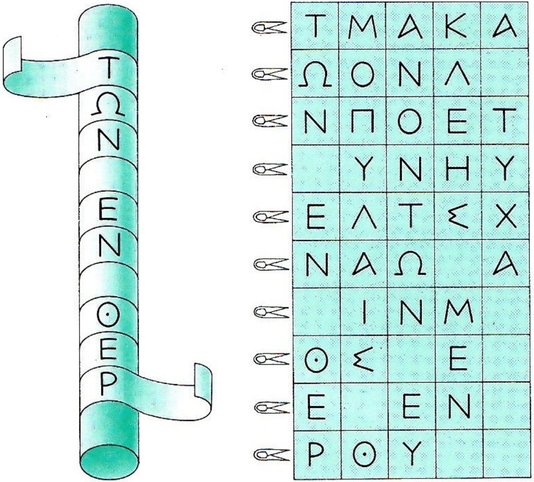
aleph	beth	gimel	daleth	he	waw	zayin	heth	teth	yod	kaph
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ
taw	sin shin	resh	qoph	sadhe	pe	ayin	samkeh	nun	mem	lamed
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל

בבל
Babel/Babilonia
ששכ
Sheschach

Il messaggio in chiaro viene trasformato in un messaggio in cifra (o crittogramma) mediante una operazione di cifratura usando un codice segreto (un algoritmo).

Codici Segreti

Scitala spartana (≈ 400 AC) — trasposizione



Codici Segreti

Steganografia (nascondere l'informazione)

- Scrivere in messaggio sotto la cera nuova delle tavolette di cera (block notes/tablet dell'epoca)
- Se non c'è fretta: radere i capelli, scrivere sul cuoio capelluto, attendere che ricrescano e inviare il messaggero col messaggio (Istiéo ad Aristagona di Mileto)
- Usare una miscela di allume e aceto per scrivere sul guscio d'uovo (sodo). Il messaggio si vedrà solo a uovo pelato (G.B. Della Porta)
- Inchiostri simpatici di vario tipo . . .

  Il messaggio non è cifrato, è solo nascosto. Se cade in mano del nemico viene compreso in poco tempo: non approfondiremo la steganografia!

- Scrivere in messaggio sotto la cera nuova delle tavolette di cera (block notes/tablet dell'epoca)
- Se non c'è fretta: radere i capelli, scrivere sul cuoio capelluto, attendere che ricrescano e inviare il messaggero col messaggio (Istiéo ad Aristagona di Mileto)
- Usare una miscela di allume e aceto per scrivere sul guscio d'uovo (sodo). Il messaggio si vedrà solo a uovo pelato (G.B. Della Porta)
- Inchiostri simpatici di vario tipo ...
  Il messaggio non è cifrato, è solo nascosto. Se cade in mano del nemico viene compreso in poco tempo: non approfondiremo la steganografia!

P	I	G	R	E	C	O
S	M	K	V	H	F	R

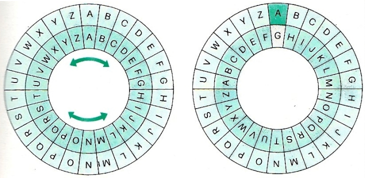
A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	A	B	C

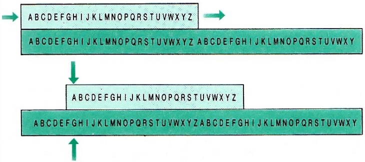
A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	A	B	C

- La “chiave” segreta è la lettera iniziale (la D per Cesare).
- Anche ammettendo che la spia conosca il tipo di codifica usata (Principio di Kerckhoffs 1835–1903)
  deve essere difficile per lei/lui identificare tale la chiave.
- Ci sono una ventina di chiavi: il codice è troppo debole.

Cifrari a sostituzione monoalfabetica

Macchine di cifra





L.B. Alberti (1404–1472)

G.B. Della Porta (1535–1615)

Regolo di Saint Cyr (fine 800)

- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.

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

- Quante sono le permutazioni di n elementi?
  - $n = 1$: $[1] \Rightarrow 1$
  - $n = 2$: [2,1], [1,2] $\Rightarrow 2$
  - $n = 3$: [3,2,1],[2,3,1],[2,1,3] [3,1,2], [1,3,2], [1,2,3] $\Rightarrow 6$
  - ...
  - n generico. Prendo una qualuque permutazione di $[1, \ldots, n-1]$. n lo posso inserire in n posizioni. E dunque le permutazioni di n elementi sono n moltipicato per le permutazioni di $n-1$ elementi. Ragiono a ritroso (o per induzione) e capisco che sono

$$n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$$

- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.

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

- Quante sono le permutazioni di n elementi?
  - $n = 1$: [1] $\Rightarrow$ 1
  - $n = 2$: [2,1], [1,2] $\Rightarrow$ 2
  - $n = 3$: [3,2,1],[2,3,1],[2,1,3] [3,1,2], [1,3,2], [1,2,3] $\Rightarrow$ 6
  - ...
  - n generico. Prendo una qualuque permutazione di $[1, \ldots, n-1]$. n lo posso inserire in n posizioni. E dunque le permutazioni di n elementi sono n moltipicato per le permutazioni di $n-1$ elementi. Ragiono a ritroso (o per induzione) e capisco che sono

$$n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$$

- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.

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

- Quante sono le permutazioni di n elementi?
  - $n = 1$: [1] $\Rightarrow$ 1
  - $n = 2$: [2,1], [1,2] $\Rightarrow$ 2
  - $n = 3$: [3,2,1],[2,3,1],[2,1,3] [3,1,2], [1,3,2], [1,2,3] $\Rightarrow$ 6
  - ...
  - n generico. Prendo una qualuque permutazione di $[1, \ldots, n-1]$. n lo posso inserire in n posizioni. E dunque le permutazioni di n elementi sono n moltipicato per le permutazioni di $n-1$ elementi. Ragiono a ritroso (o per induzione) e capisco che sono

$$n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$$

- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.

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

- Quante sono le permutazioni di n elementi?
  - $n = 1$: [1] $\Rightarrow$ 1
  - $n = 2$: [2,1], [1,2] $\Rightarrow$ 2
  - $n = 3$: [3,2,1],[2,3,1],[2,1,3] [3,1,2], [1,3,2], [1,2,3] $\Rightarrow$ 6
  - ...
  - n generico. Prendo una qualuque permutazione di $[1, \ldots, n-1]$. n lo posso inserire in n posizioni. E dunque le permutazioni di n elementi sono n moltipicato per le permutazioni di $n-1$ elementi. Ragiono a ritroso (o per induzione) e capisco che sono

$$n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$$

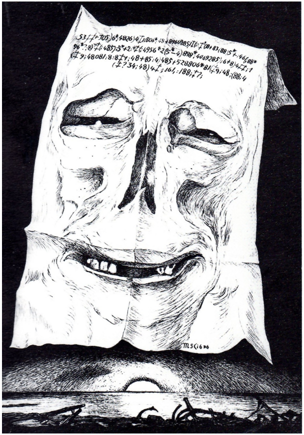
- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.

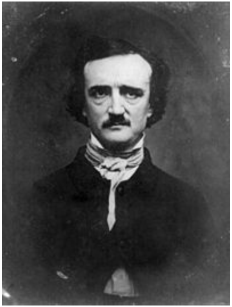
A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X
M	V	F	T	H	C	K	L	D	N	O	P	Q	R	A	G	E	X	S	B	I

- Le chiavi possibili diventano $21! = 21 \cdot 20 \cdot 19 \cdots 2 \cdot 1 \approx 5 \cdot 10^{19}$ (in realtà un po' meno ... non vogliamo troppe identità...) La chiave è l'intera sostituzione.
- Cominciano a diventare numeri pesanti per la *forza bruta*.
- Viene usata la statistica. In una data lingua le lettere assumono una frequenza tipica. Il codice si forza a partire da questa informazione aggiuntiva.

CIFRARI A SOSTITUZIONE MONOALFABETICA

DECRITTAZIONE





Lo scarabeo d'oro / The Gold-Bug (Edgar Allan Poe, 1843)

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	”

Confondere la statistica

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
0 0 0 1 1	1 0 1 0 1	0 1 0 0 1	0 0 0 1 0	0 0 0 1 0	0 1 0 0 1	0 1 1 1 1
I O N O N	D I C O P	A R O L A	C C E Q U	A N D O P	A R L O I	N A U L A

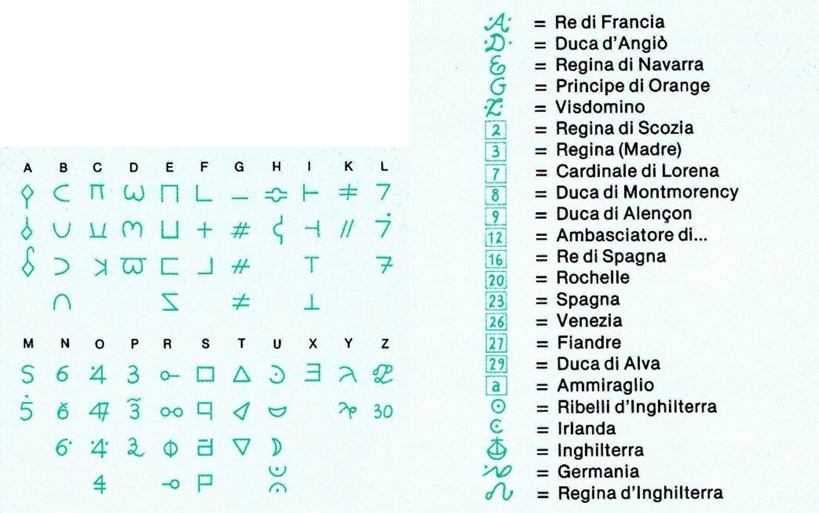
Crittogramma:

I O N o n	d I c O p	A r O L a	C C E q U	A N D o P	A r L O i	N a u l a

- 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 ...



Poi potevano essere ulteriormente cifrati.

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.

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.

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).

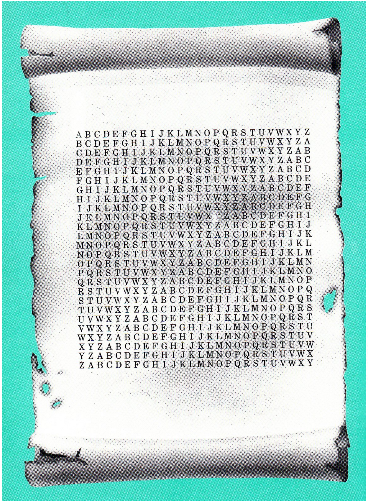
> *C'era una volta, tanto tempo fa, una principessa che non voleva uscire di casa per far le compere ma ordinare tutto senza alzarsi dalla scrivania utilizzando la connessione wifi a bassa protezione in hotel.*

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).

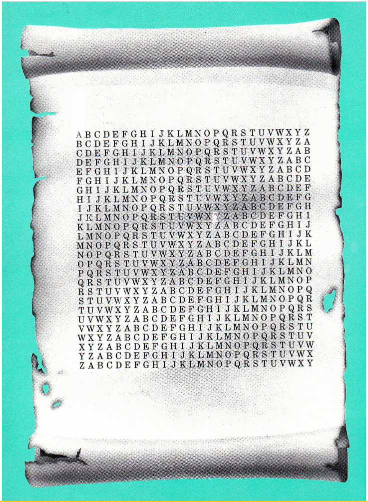


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z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

Cifrari a sostituzione polialfabetica

Cifrazione

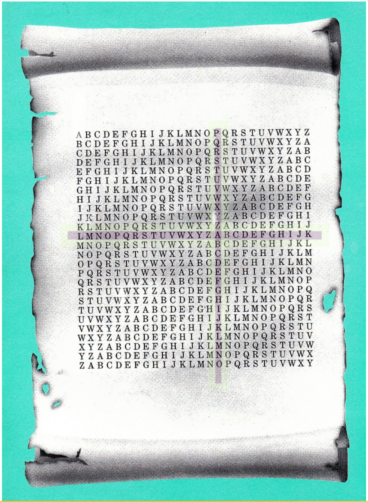
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



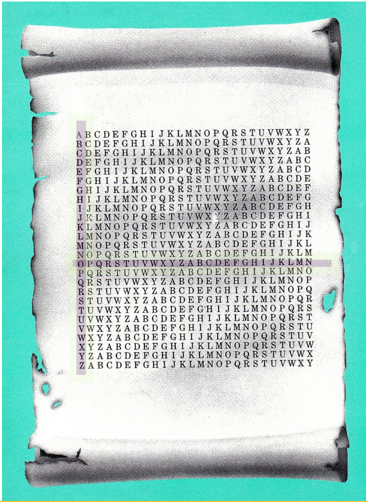
CIFRARI A SOSTITUZIONE POLIALFABETICA

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



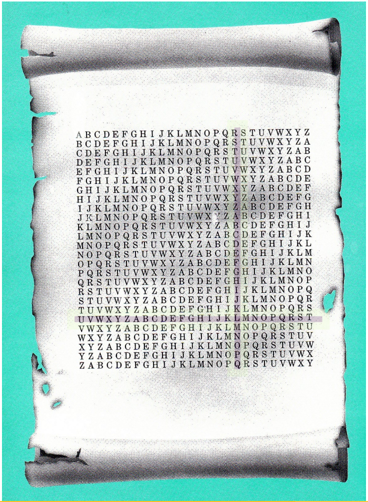
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L



Cifrari a sostituzione polialfabetica

Cifrazione

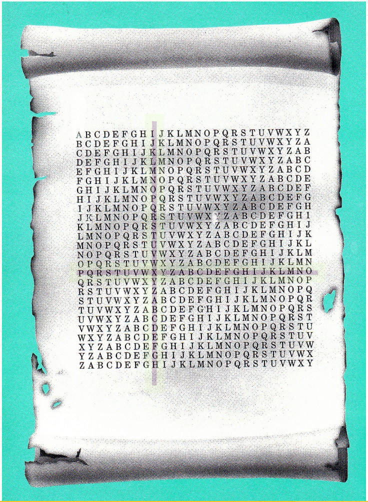
P	A	R	I	S	V	A	U	T	B	I	E	N	U	N	E	M	E	S	S	E
L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L	O	U	P	L

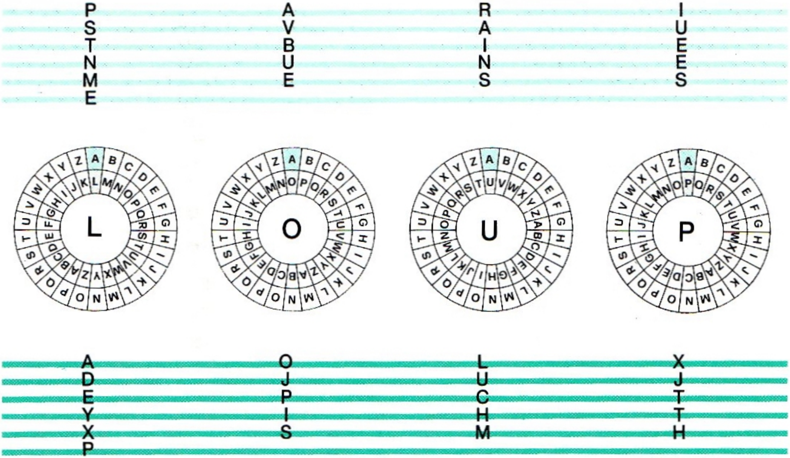


CIFRARI A SOSTITUZIONE POLIALFABETICA

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





PSTNME
AVBUE
RAINS
IUEES
L
O
U
P
ADEYXP
OJPIS
LUCHM
XJTTH

- È 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
$$f : \{A, \dots, Z\}^n \longrightarrow \{A, \dots, Z\}^n$$
- Anche se su ogni lettera della chiave ci sono solo 21 scelte, in tutto ce ne sono ben $21^n = \underbrace{21 \cdot 21 \cdot \dots \cdot 21}_{n}$.
- Inoltre la statistica sembra ingannata.
- E la spia non conosce nemmeno n.

Andrew Swanston. Il codice del traditore (The King's Spy). 2012

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

PETER	LEGRAND	IS	A	GOOD	FRIEND	OF	NAPOLEON	LEGRAND
EDGAR	EDGARED	GA	R	EDGA	REDGAR	ED	GAREDGAR	EDGARED
THZEI	PHMRRRG	OS	R	KRUD	WVLKNU	SI	TAGSOKOE	PHMRRRG

PETER	LEGRAND	IS	A	GOOD	FRIEND	OF	NAPOLEON	LEGRAND
EDGAR	EDGARED	GA	R	EDGA	REDGAR	ED	GAREDGAR	EDGARED
THZEI	PHMRRRG	OS	R	KRUD	WVLKNU	SI	TAGSOKOE	PHMRRRG

`tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp`

CIFRARI A SOSTITUZIONE POLIALFABETICA

DECRITTAZIONE

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

CIFRARI A SOSTITUZIONE POLIALFABETICA
DECRITTAZIONE

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
  tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
  tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
   tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
   tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
    tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsgtugrfnlbpdp
    tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

Perché succede?

Serve un po' di conoscenza di teoria della probabilità. Il punto chiave è il seguente. Supponete di avere n numeri positivi (per semplicità interi).

Ad esempio con $n = 3$ prendiamo (a caso) i numeri 2, 4, 5.

Supponete ora di moltiplicare ogni numero con esattamente un altro numero dell'elenco, anche sé stesso, però ogni numero può essere selezionato una volta sola, e di fare la somma. Come fate ad ottenere la somma massima?

Nell'esempio sopra avremmo, ad esempio
$2 \cdot 4 + 4 \cdot 5 + 5 \cdot 2 = 8 + 20 + 10 = 38$.
Ma anche $2 \cdot 2 + 4 \cdot 4 + 5 \cdot 5 = 4 + 16 + 25 = 45$.

E dunque? Applicando la proprietà ad una formula opportuna si dimostra che quando lo spostamento ha la lunghezza della chiave si massimizza la probabilità di affiancare lo stesso carattere.

Cifrari a sostituzione polialfabetica

Decrittazione (vedi appendice)

Perché succede?

Serve un po' di conoscenza di teoria della probabilità. Il punto chiave è il seguente. Supponete di avere n numeri positivi (per semplicità interi).

Ad esempio con $n = 3$ prendiamo (a caso) i numeri 2, 4, 5.

Supponete ora di moltiplicare ogni numero con esattamente un altro numero dell'elenco, anche sé stesso, però ogni numero può essere selezionato una volta sola, e di fare la somma. Come fate ad ottenere la somma massima?

Nell'esempio sopra avremmo, ad esempio
$2 \cdot 4 + 4 \cdot 5 + 5 \cdot 2 = 8 + 20 + 10 = 38$.
Ma anche $2 \cdot 2 + 4 \cdot 4 + 5 \cdot 5 = 4 + 16 + 25 = 45$.

E dunque? Applicando la proprietà ad una formula opportuna si dimostra che quando lo spostamento ha la lunghezza della chiave si massimizza la probabilità di affiancare lo stesso carattere.

Perché succede?

Serve un po' di conoscenza di teoria della probabilità. Il punto chiave è il seguente. Supponete di avere n numeri positivi (per semplicità interi).

Ad esempio con $n = 3$ prendiamo (a caso) i numeri 2, 4, 5.

Supponete ora di moltiplicare ogni numero con esattamente un altro numero dell'elenco, anche sé stesso, però ogni numero può essere selezionato una volta sola, e di fare la somma. Come fate ad ottenere la somma massima?

Nell'esempio sopra avremmo, ad esempio
$2 \cdot 4 + 4 \cdot 5 + 5 \cdot 2 = 8 + 20 + 10 = 38$.
Ma anche $2 \cdot 2 + 4 \cdot 4 + 5 \cdot 5 = 4 + 16 + 25 = 45$.

E dunque? Applicando la proprietà ad una formula opportuna si dimostra che quando lo spostamento ha la lunghezza della chiave si massimizza la probabilità di affiancare lo stesso carattere.

Perché succede?

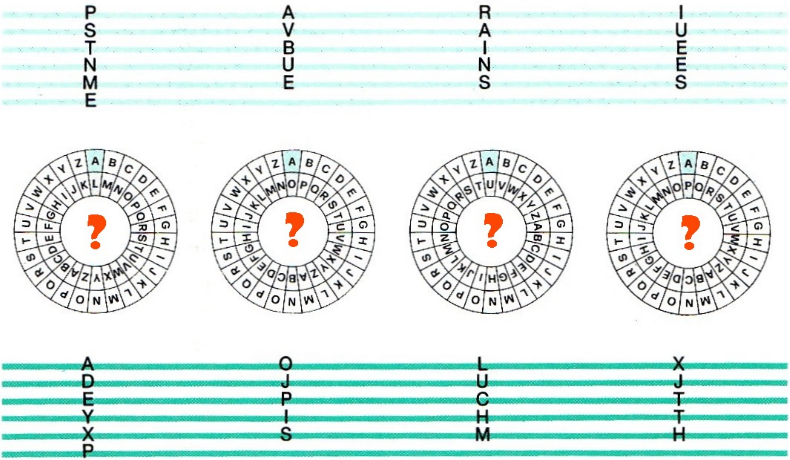
Serve un po' di conoscenza di teoria della probabilità. Il punto chiave è il seguente. Supponete di avere n numeri positivi (per semplicità interi).

Ad esempio con $n = 3$ prendiamo (a caso) i numeri 2, 4, 5.

Supponete ora di moltiplicare ogni numero con esattamente un altro numero dell'elenco, anche sé stesso, però ogni numero può essere selezionato una volta sola, e di fare la somma. Come fate ad ottenere la somma massima?

Nell'esempio sopra avremmo, ad esempio
$2 \cdot 4 + 4 \cdot 5 + 5 \cdot 2 = 8 + 20 + 10 = 38$.
Ma anche $2 \cdot 2 + 4 \cdot 4 + 5 \cdot 5 = 4 + 16 + 25 = 45$.

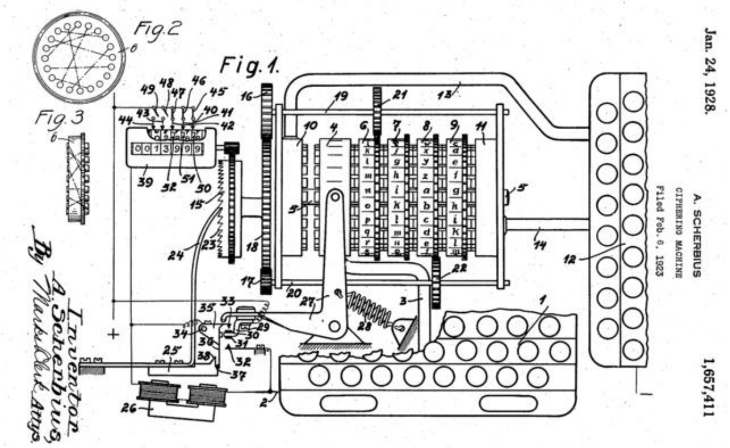
E dunque? Applicando la proprietà ad una formula opportuna si dimostra che quando lo spostamento ha la lunghezza della chiave si massimizza la probabilità di affiancare lo stesso carattere.


PSTNME
AVBUE
RAINS
IUEES
ADEYXP
OJPIS
LUCHM
XJTTH

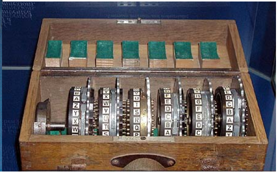
1. Con l'allineamento visto, si determina la lunghezza della parola chiave.
2. Congetturata la lunghezza, si partiziona il testo in n sottotesti e si cercano le n chiavi con la la statistica.

3. La cifratura polialfabetica non è praticamente decifrabile se la parola chiave è lunga quanto il testo (e non viene più utilizzata per alti testi). Se inoltre non ha senso compiuto (è scelta lanciando una moneta) diventa dimostrabilmente indecifrabile (cifrario perfetto/one time pad—Vernam)
4. In generale, se la chiave (il periodo) è molto lungo rispetto al testo la decodifica statistica non è effettiva.

Nel 1918 brevetta una macchina da cifra a rotori (multipli)



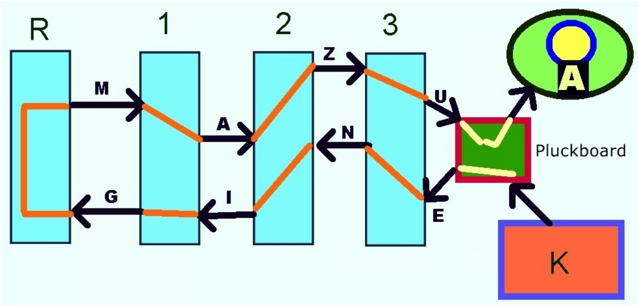
NEL 1923 SCHERBIUS COMMERCIALIZZA L'ENIGMA.



Enigma: funzionamento

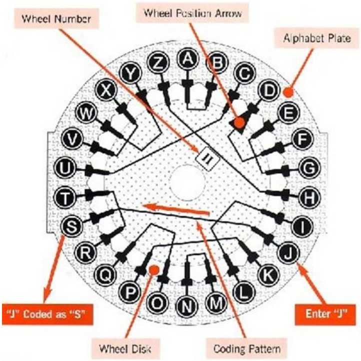
- Si tratta di un cifrario polialfabetico.
- Un punto di forza è che la lunghezza del periodo (o della chiave nel senso di Vigenère) è maggiore della lunghezza dei messaggi, il che rende apparentemente simile al one-time-pad.
- Le tecniche statistiche viste per Vigenère non si possono applicare.
- L'altro punto di forza (per l'epoca) era l'automazione elettrica della trasformazione (sia per cifrare che per decifrare) e la relativa semplicità d'uso (anche se mancava la stampante).
- Ci sono simulatori di Enigma per tutte le piattaforme (Windows, Linux, Mac, I-phone, Android). Quella forse più realistica e corredata di diverso materiale sulla crittografia si trova qui: `http://users.telenet.be/d.rijmenants/`

È una macchina a rotori non fissi che si muovono con moto odometrico dopo ogni lettera codificata—stepping motion (come i vecchi contachilometri o i contatori dell'acqua o del gas).



Ogni rotore ha 26 contatti su una faccia e 26 sull'altra e implementa una sostituzione monoalfabetica (completa).

Ritorna nella stessa posizione dopo $26^3 \simeq 17500$ caratteri!!!


Wheel Number
Wheel Position Arrow
Alphabet Plate
"J" Coded as "S"
Enter "J"
Wheel Disk
Coding Pattern

(DEMO)

Oltre ai 3 (o 4) rotori c'era una pluckboard (pannello elettrico) che permetteva un'ulteriore (e più libera) sostituzione:

Inoltre c'era una sostituzione iniziale tra tastiera e primo rotore (fissa, ma poteva cambiare cambiando il modello della macchina).

- Diverse varianti sono state usate. Concentriamoci su quelle a 3 rotori (per quella a 4, $\times 26$).
- Fissati i rotori, le possibili chiavi iniziali erano $26^3 = 17576$ (456976 per 4 rotori)
- Tale numero è anche la lunghezza del *periodo* (o della chiave nel senso di Vigenère—a dire il vero $26 \cdot 25 \cdot 26$)
- Erano possibili 6=3! posizioni per i 3 rotori.
- In versioni più evolute veniva fornita una scatola con 5 o, per la marina, 8 rotori da cui sceglierne 3 (o 4). Allora potevano esserci $6 \times \binom{8}{3} = 536$ posizioni.
- Inoltre c'erano i collegamenti sulla plugboard. Con 6 cavi ci sono $\sim 10^{11}$ possibilità.
- In generale, per k cavi ($k = 1, \ldots, 13$) abbiamo:

$$\binom{26}{2k} \frac{\binom{2k}{2}\binom{2k-2}{2}\cdots\binom{2}{2}}{k!}$$

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. Turing.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

In §§ 9, 10 I give some arguments with the intention of showing that the computable numbers include all numbers which could naturally be regarded as computable. In particular, I show that certain large classes of numbers are computable. They include, for instance, the real parts of all algebraic numbers, the real parts of the zeros of the Bessel functions, the numbers π, e, etc. The computable numbers do not, however, include all definable numbers, and an example is given of a definable number which is not computable.

ATHLETICS

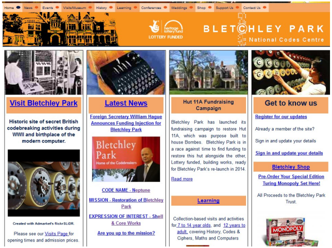
MARATHON AND DECATHLON CHAMPIONSHIPS

The Amateur Athletic Association championships for this year were concluded at Loughborough College Stadium, Leicestershire, on Saturday, with the second, and last, day of the Decathlon and the decision of the Marathon championship.

MARATHON CHAMPIONSHIP (26 miles 385 yds.) (record: 2hrs. 30min. 57 6sec., by H. W. Payne, Windsor to Stamford Bridge, on July 5, 1929; standard time: 3hrs. 5min.).—J. T. Holden (Tipton Harriers), 2hrs. 33min. 20 1-5sec., 1; T. Richards (South London Harriers), 2hrs. 36mni. 7sec., 2; D. McNab Robertson (Maryhill Harriers, Glasgow), 2hrs. 37min. 54 3-5sec., 3; J. E. Farrell (Maryhill Harriers), 2hrs. 39min. 46 2-5sec., 4; Dr. A. M. Turing (Walton A.C.), 2hrs. 46min. 3sec., 5; L. H. Griffiths (Reading A.C.), 2hrs. 47min. 50 2-5sec., 6.

DECATHLON CHAMPIONSHIP.—H. J. Moesgaard-Kjeldsen (Polytechnic Harriers, London), 5,965 points, 1; Captain H. Whittle (Army and Reading A.C.), 5,650, 2;

Nel 1948 (Olimpiadi di Londra) Delfo Cabrera vinse in 2h34'51"



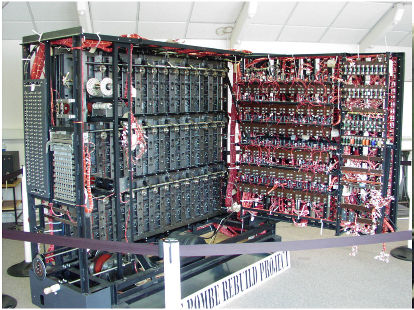
"The Government Code and Cypher School" originariamente di stanza a Londra aveva bisogno di un posto più sicuro dove lavorare e nel 1938 decise di installarsi a Bletchley Park. Nell'agosto 1939 divenne il centro operativo del controspionaggio inglese (Ora è un museo).

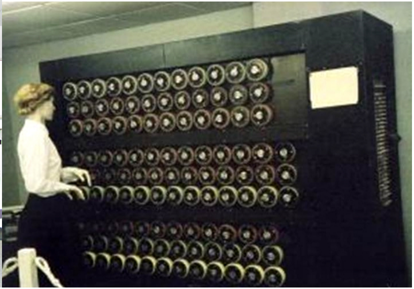
Alan Turing ebbe un ruolo cruciale nel team per la decrittazione dell'Enigma(e, in seguito, ad esportare in USA le tecniche sviluppate).

- Le configurazioni iniziali dell'Enigma venivano comunicate segretamente e duravano brevi intervalli di tempo (p.es. plugboard: trimestrale, ordine dei rotori: mensile, carattere di partenza: giornaliero).
- All'inizio del messaggio arrivava codice (in cifra) per modificare ordine rotori.
- L'obiettivo del team di Turing era quello di indovinare rotori/cavi in plugboard/chiave iniziale.
- Furono progettate le bombe che simulavano elettromeccanicamente molti Enigma contemporaneamente.
- La forza bruta, coi numeri visti, non era sufficiente.

ENIGMA: ATTACCO

Nel 1940 fu costruita la prima Bombe (attacco *forza bruta*)





Ne furono costruite 210 operate da circa 2000 WReNS (Women's Royal Naval Service).

Quando si fermano un operatore verifica se il msg ha senso o è un false stop.
Se conosciamo il messaggio (crib) allora l'arresto equivale all'identificazione della chiave.

Il ruolo di Turing per l'attacco all'Enigma

- Turing sfruttò le poche debolezze (1. una lettera non veniva mai crittata in sè stessa, 2. il funzionamento generale è sempre simmetrico, 3. le posizioni iniziali dei rotori (3 caratteri) venivano ripetute due volte a inizio messaggio)
- Utilizzò dei risultati di tre matematici polacchi del Cipher Bureau (Marian Rejewski, Henryk Zygalski e Jerzy Różycki) che ne studiarono a fondo le caratteristiche matematico-logiche
- Più alre informazioni che derivavano dalla cattura di macchine ENIGMA e di libri di utilizzo destinati agli ufficiali tedeschi e
- se ne servì per ridurre lo spazio di ricerca delle bombe, riuscendo a forzare anche "shark", l'ENIGMA a 4 rotori usato dai sommergibili.
- Oltre ad averci aperto il mondo dell'informatica che caratterizza la nostra vita quotidiana, Turing è stato fondamentale per la vittoria degli alleati nella seconda guerra mondiale che ha permesso l'attuale civiltà.

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 (=20,3,8,13,4).
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
20 3 8 13 4	20 3 8 13 4	20 3 8 13 4	20 3 8 13 4

8 9 14 21 15	21 14 12 12 12	7 17 12 17 17	8 11 22 5 5
I J O V P	V O M M M	H R M R R	I L W F F

Testo in cifra: JJOVPWOMMMIRMRRJLWFF
(ovviamente non usiamo gli accenti!)

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= 20,3,8,13,4 = 10100, 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
10100	00011	01000	01101	00100	10100	00011	01000	01101	00100
11010	00101	01110	00101	01111	10101	01000	01100	10100	01100
♣	F	O	F	P	V	Q	M	U	M

O	N	E	E	N	O	I	O	S	A
01101	01110	00100	00100	01101	01110	01000	01110	01010	00001
10100	00011	01000	01101	00100	10100	00011	01000	01101	00100
01001	01101	01100	01001	01001	11010	01011	00110	00111	00101
J	N	M	J	J	♣	L	G	H	F

Testo in cifra: ♣FOFP VQMUM JNMJJ ♣LGHF

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. (cifrario perfetto–C. E. Shannon)
- 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. (cifrario perfetto–C. E. Shannon)
- 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. (cifrario perfetto–C. E. Shannon)
- Come comunichiamo la chiave?

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 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

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.

- 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.

CRITTOGRAFIA INFORMATICA

LA PROSSIMA VOLTA!

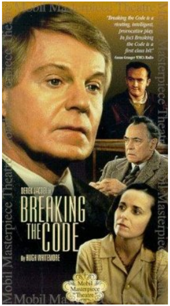
RIASSUNTO

- Gran parte di quanto visto oggi si basa sull'idea del Vigenère.
- Se la parola chiave ha lunghezza 1 siamo nel codice di Cesare
- Nel Vigenère tradizionale la chiave era una parola mnemonica corta (rispetto al testo). Attacco con allineamento e tecniche statistiche!!!
- Nell'Enigma la parola chiave era solo apparentemente corta (3 lettere—posizione iniziale rotori), ma dal punto di vista del Vigenère, era lunga 26^3: nessun attacco statistico è possibile per testi corti.
- Nel one-time pad la chiave è lunga quanto il testo. Inattaccabile, ma la chiave va distribuita prima.

FILMS 'SU' TURING

The Imitation Game
2014
Morten Tyldum

Enigma
2001
M. Adept



Breaking the Code
1996
Derek Jacobi

Un sito che rapporta meglio T.I.G. nella storia reale: `http://www.historyvshollywood.com/reelfaces/imitation-game/`

LIBRI DOVE APPROFONDIRE

Il ruolo di Turing. **Storico/scientifici:**

- M. Davis. Il calcolatore universale
- A. Hodges. The Enigma (da cui è tratto "The imitation game")

Romanzi:

- Robert Harris. ENIGMA (1995) (da cui è tratto il film "ENIGMA")
- Neal Stephenson. Cryptonomicon (1999)

Oltre ovviamente ai contributi scientifici scritti da Turing reperibili da:
`http://www.turingarchive.org/`

Generali sulla crittografia:

- Andrea Sgarro. Codici segreti. 1989 (Mondadori)
- Simon Singh. Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet. 2001. (BUR Biblioteca Univ. Rizzoli)

APPENDICE

- Sia $P = (p_0, \ldots, p_{25})$ la probabilità di ogni lettera (per semplicità supponiamo le lettere siano 0,...,25) nella lingua del messaggio.
- Prendiamo il testo in chiaro. Fissiamo una posizione. Per $x \in \{0, \ldots, 25\}$, 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 $P^0 = P$).

- 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.