Scambiarsi messaggi segreti: la matematica della crittografia

a cura di Alessandro Musesti

Università Cattolica del Sacro Cuore, Brescia

17 febbraio 2018

UNIVERSITÀ
CATTOLICA
del Sacro Cuore

Una citazione

La "vera" matematica dei "veri" matematici, quella di Fermat, di Eulero, di Gauss, di Abel e di Riemann, è quasi totalmente "inutile". [...]

G.H. Hardy, Apologia di un matematico

Parte I

L'inizio della storia: la sostituzione monoalfabetica

Il metodo Atbash

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

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	M	L	K	J	I	H	G	F	E	D	C	B	A

Il metodo Atbash

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

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	M	L	K	J	I	H	G	F	E	D	C	B	A

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

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

Il metodo Atbash

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

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	M	L	K	J	I	H	G	F	E	D	C	B	A

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

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

ILMXZWVOOV

Il metodo Atbash

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

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	M	L	K	J	I	H	G	F	E	D	C	B	A

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

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

roncadelle

Il cifrario di Cesare

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

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	D	E	F	G	H	I	J	K	L	M	N	O	P

Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caio Giulio Cesare usava questo metodo per comunicare con le truppe. Naturalmente può essere usata qualsiasi altra chiave (compresa tra 1 e 25).

Il cifrario di Cesare

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

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	D	E	F	G	H	I	J	K	L	M	N	O	P

Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caio Giulio Cesare usava questo metodo per comunicare con le truppe. Naturalmente può essere usata qualsiasi altra chiave (compresa tra 1 e 25).

Un algoritmo tuttora usato (per gioco) è il ROT13, in cui la chiave scelta è 13 (in questo modo per crittare e decrittare si usa lo stesso algoritmo):

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

Il cifrario di Cesare

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

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	D	E	F	G	H	I	J	K	L	M	N	O	P

Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caio Giulio Cesare usava questo metodo per comunicare con le truppe. Naturalmente può essere usata qualsiasi altra chiave (compresa tra 1 e 25).

Provate a decrittare la frase

```
GLHFLPLOD QHPLFL DO IURQWH
```

Il cifrario di Cesare

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

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrato	D	E	F	G	H	I	J	K	L	M	N	O	P

Chiaro	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caio Giulio Cesare usava questo metodo per comunicare con le truppe. Naturalmente può essere usata qualsiasi altra chiave (compresa tra 1 e 25).

Provate a decrittare la frase

```
diecimila nemici al fronte
```

Cifrari per sostituzione

Si possono anche usare alfabeti "mescolati" per la sostituzione, ad esempio

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

Cifrari per sostituzione

Si possono anche usare alfabeti "mescolati" per la sostituzione, ad esempio

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

In tutto ci sono

$$!26 = 148\,362\,637\,348\,470\,135\,821\,287\,825$$

possibilità (dismutazioni), cioè all'incirca 148 milioni di miliardi di miliardi di modi di scambiare tutte le lettere!

Cifrari per sostituzione

Si possono anche usare alfabeti "mescolati" per la sostituzione, ad esempio

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

In tutto ci sono

$$!26 = 148\,362\,637\,348\,470\,135\,821\,287\,825$$

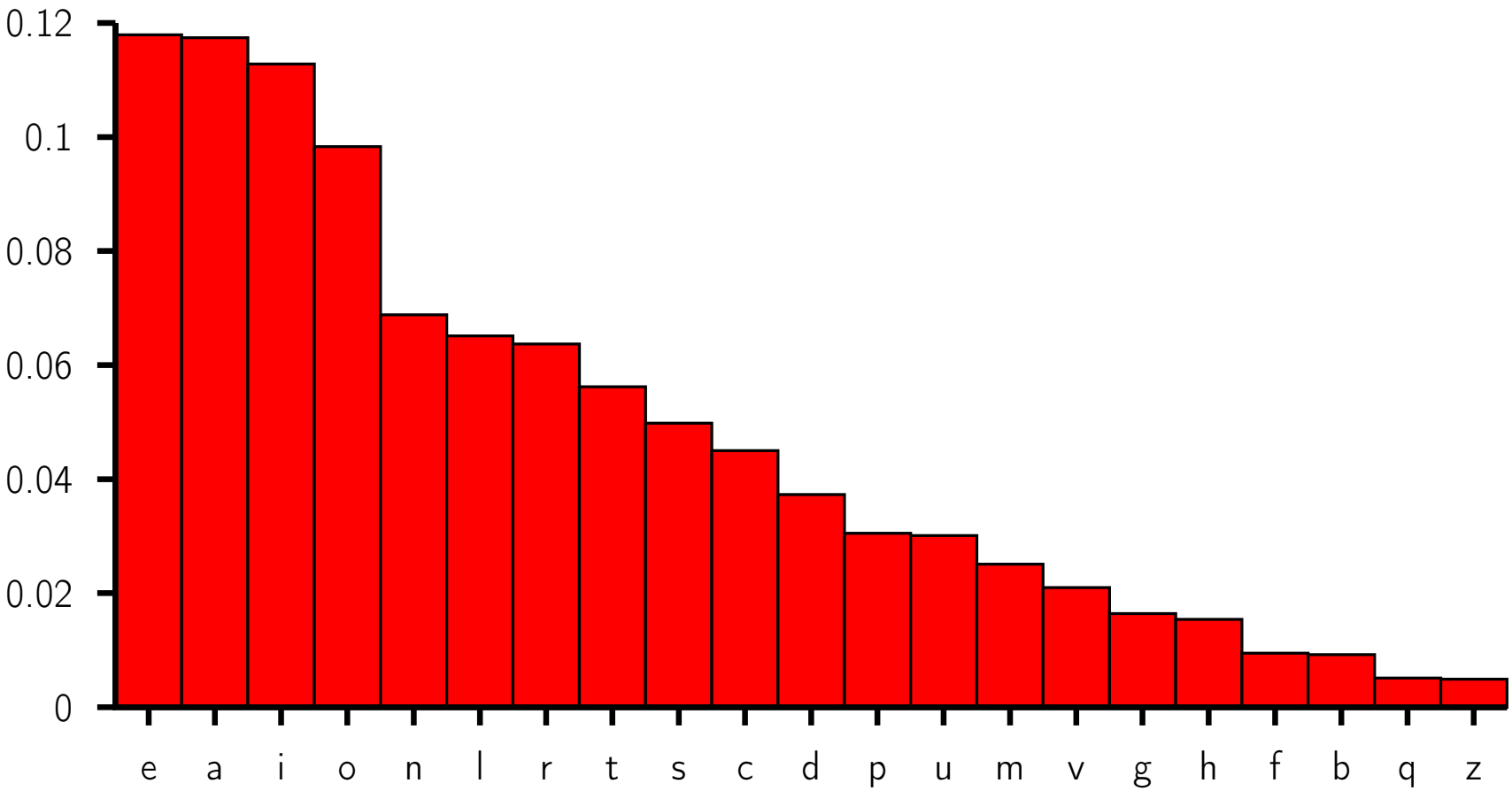
possibilità (dismutazioni), cioè all'incirca 148 milioni di miliardi di miliardi di modi di scambiare tutte le lettere!

Ma c'è un problema...

a simbolo uguale corrisponde lettera uguale

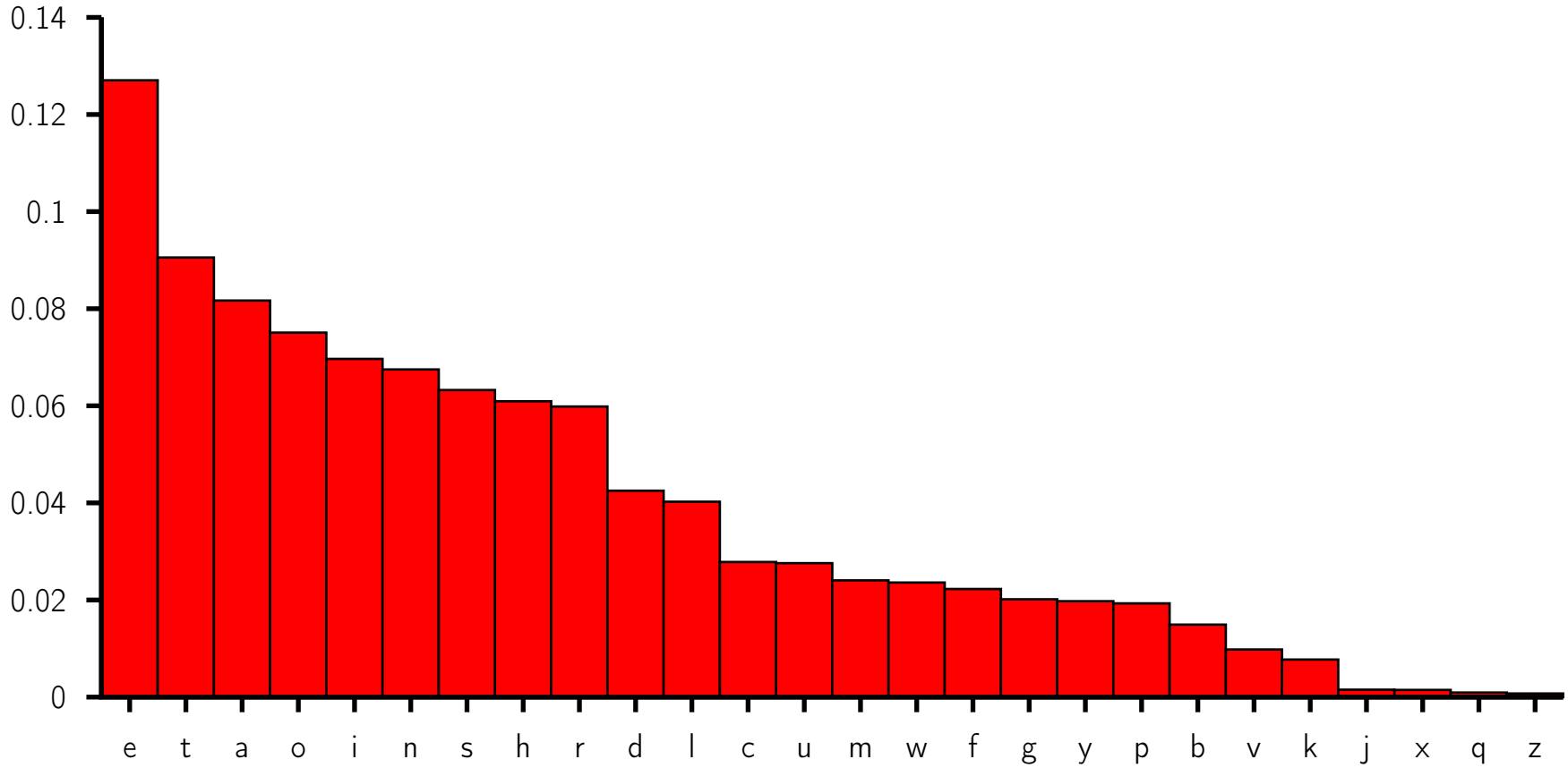
al-Kindi, scienziato arabo del IX secolo d.C, cominciò a studiare l'**analisi delle frequenze**.

Analisi delle frequenze



Frequenze delle lettere nella lingua italiana

Analisi delle frequenze



Frequenze delle lettere nella lingua inglese

I rischi di codici non sicuri

I rischi di codici non sicuri

Maria Stuarda (1542-1587), regina di Scozia, tradita da un cifrario troppo debole, decifrato da Thomas Phelippes.

Parte II

Sostituzione polialfabetica

Il cifrario di Vigenère (1586)

Storicamente è stato inventato da Giovan Battista Bellaso, nato a Brescia nel 1505.
In questo metodo bisogna stabilire una parola, o una frase (anche lunga) comune: questa sarà la chiave segreta del cifrario.
Per esempio, la chiave segreta sia la parola `RICERCA` e supponiamo di voler cifrare la frase "`la matematica è bella`". In una tabella scriviamo la frase da cifrare e sotto di essa, ripetutamente, la parola-chiave. Poi ad ogni lettera "sommiamo" il valore della lettera corrispondente della parola-chiave (da `A`=0 a `Z`=25), trovando una nuova lettera:

Il cifrario di Vigenère (1586)

Storicamente è stato inventato da Giovan Battista Bellaso, nato a Brescia nel 1505.
In questo metodo bisogna stabilire una parola, o una frase (anche lunga) comune: questa sarà la chiave segreta del cifrario.
Per esempio, la chiave segreta sia la parola `RICERCA` e supponiamo di voler cifrare la frase "`la matematica è bella`". In una tabella scriviamo la frase da cifrare e sotto di essa, ripetutamente, la parola-chiave. Poi ad ogni lettera "sommiamo" il valore della lettera corrispondente della parola-chiave (da `A`=0 a `Z`=25), trovando una nuova lettera:

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

Il cifrario di Vigenère (1586)

Storicamente è stato inventato da Giovan Battista Bellaso, nato a Brescia nel 1505.
In questo metodo bisogna stabilire una parola, o una frase (anche lunga) comune: questa sarà la chiave segreta del cifrario.
Per esempio, la chiave segreta sia la parola `RICERCA` e supponiamo di voler cifrare la frase "`la matematica è bella`". In una tabella scriviamo la frase da cifrare e sotto di essa, ripetutamente, la parola-chiave. Poi ad ogni lettera "sommiamo" il valore della lettera corrispondente della parola-chiave (da `A`=0 a `Z`=25), trovando una nuova lettera:

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

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

Il cifrario di Vigenère (1586)

Storicamente è stato inventato da Giovan Battista Bellaso, nato a Brescia nel 1505.
In questo metodo bisogna stabilire una parola, o una frase (anche lunga) comune: questa sarà la chiave segreta del cifrario.
Per esempio, la chiave segreta sia la parola `RICERCA` e supponiamo di voler cifrare la frase "`la matematica è bella`". In una tabella scriviamo la frase da cifrare e sotto di essa, ripetutamente, la parola-chiave. Poi ad ogni lettera "sommiamo" il valore della lettera corrispondente della parola-chiave (da `A`=0 a `Z`=25), trovando una nuova lettera:

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

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

Inoltre, bisogna prima condividere la chiave!

Tavola dell'addizione delle lettere

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	S
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

I blocchetti monouso (cifrario di Vernam, 1917)

Se nel cifrario di Vigenère prendiamo una parola-chiave lunga come il messaggio e formata da caratteri completamente casuali, otteniamo il cosiddetto cifrario di Vernam.
È stato dimostrato che questo è il modo più sicuro di scambiarsi un messaggio, ma ha una pecca: come condividere la chiave segreta, così lunga? Il serpente si morde la coda...

I blocchetti monouso (cifrario di Vernam, 1917)

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

I blocchetti monouso (cifrario di Vernam, 1917)

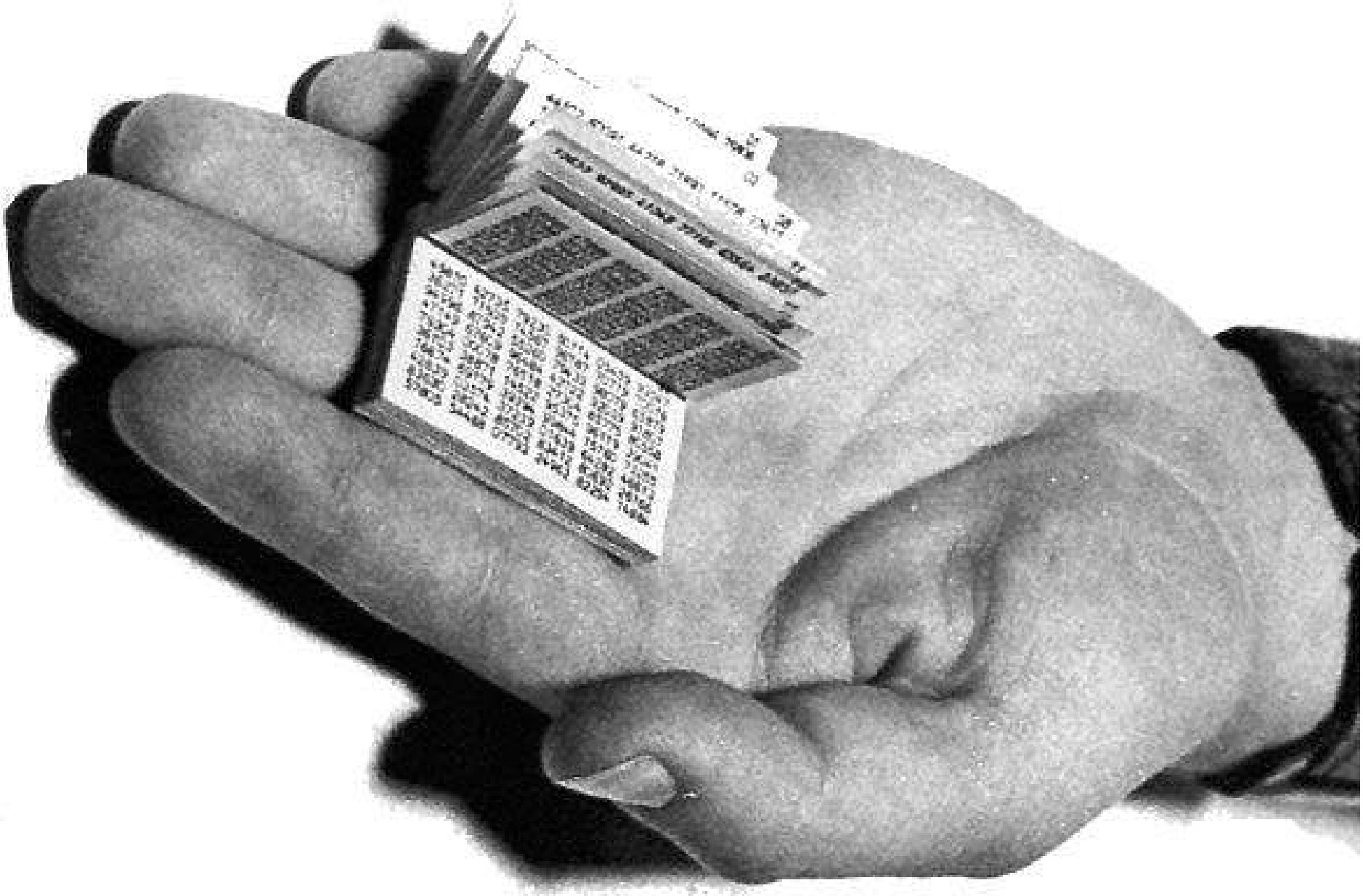
Se nel cifrario di Vigenère prendiamo una parola-chiave lunga come il messaggio e formata da caratteri completamente casuali, otteniamo il cosiddetto cifrario di Vernam.
È stato dimostrato che questo è il modo più sicuro di scambiarsi un messaggio, ma ha una pecca: come condividere la chiave segreta,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

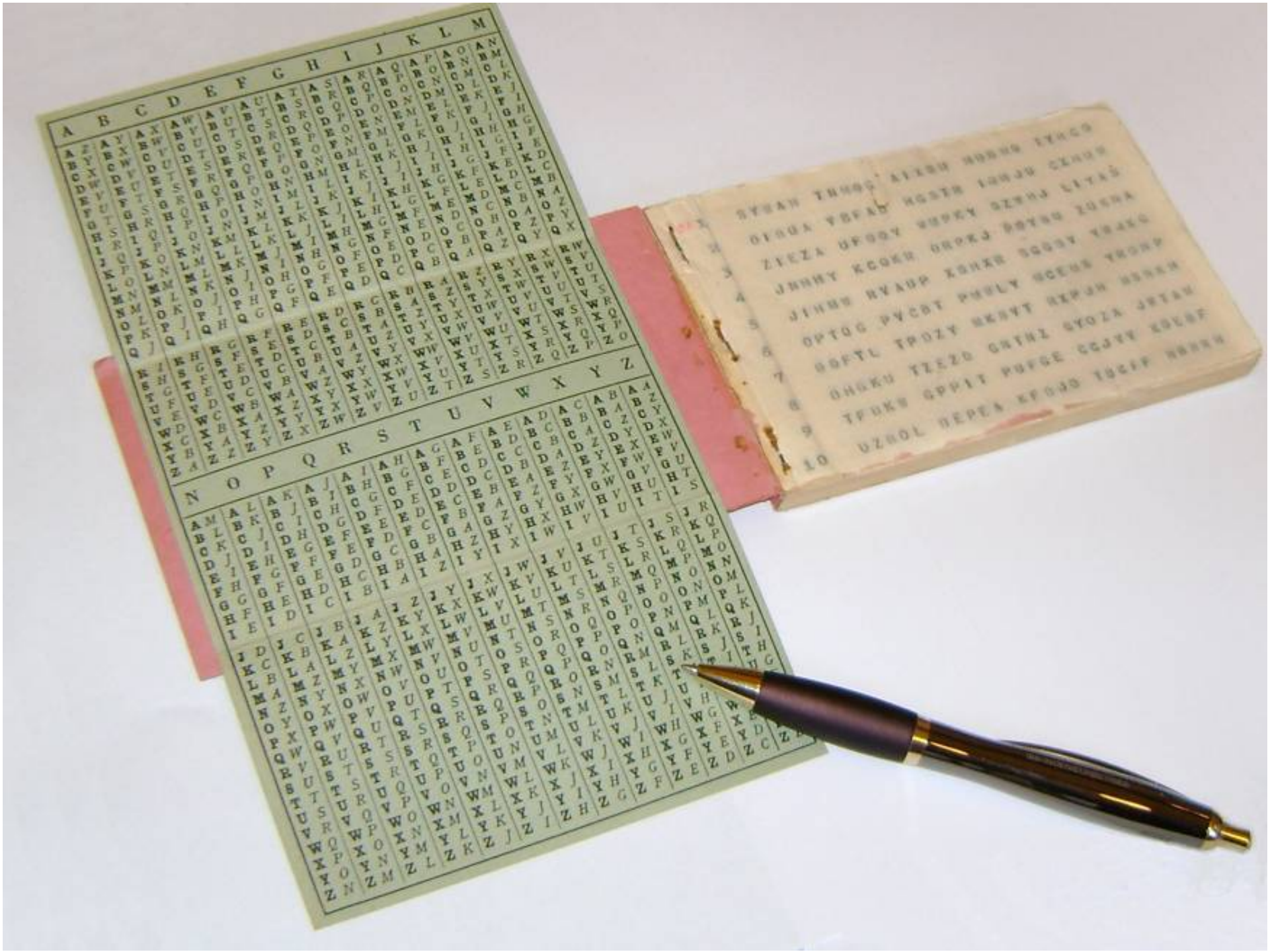
Blocchetto monouso 001

TSWVW	DMFTD	YWWZQ	BTRZB	YAYNI	HEJMH	PEORI	RWMDY	QDQZZ	BCAAI
OLYCA	VEIKK	LKAGR	PYTRX	AIDRO	XXMNG	RZETS	ZXCIZ	KBTCY	MABYZ
VCIAN	MGXXN	OJBQG	QQGWP	ZJWUB	RJSCZ	KUURU	XJFHP	TBVPK	SRPHI
XISFJ	CQWVG	IYPCY	ZHJSS	OQZDJ	SUIQQ	KOUAN	ZMDPT	SRRLK	FYIRM
EPQBH	JCRJG	LMBQG	WSNAH	BWFRO	WRYUB	VJGII	AFVIR	LBZHH	WZUKV
KOFAE	EZGNA	PSODB	LADJZ	YACKG	QPHMP	SHRZO	ROUFN	WCLVX	WQDIZ
FRYXI	DNZDE	XRPTE	NKOJF	BEUWW	BLDIG	KCLQW	RPBWR	AZCAM	XZGGP
BMPEM	CCLKC	YEWGS	ZWRYU	MMZRK	ICDRC	DYIHX	MKTKC	YFQEI	VYTYJ
NKJYG	MASBJ	NIIIH	WIQUZ	GOZJZ	ZCVSO	BVSOV	HVKYE	IBGHR	WQORS
ZDAPE	RCKPG	OUSTY	XFBKF	BSTXN	RSDIX	OOCMA	DSMRR	BFGLT	PXGDN
THWKF	IXOJY	UKXSO	TBDOS	SCWRC	ECERO	FIDQD	NAPBA	CXTFM	MPSAT
SBEHA	CWWUB	ORWZK	YWFMT	AMGEQ	ZTBPU	EBLWV	KTUXV	SEMZE	CSVIX
UIGLU	JLNAG	MSJXW	TCLYB	FQOXY	IPLWS	TYPMM	LKTFC	YLAKB	TSAVJ
KOEIT	OUETL	AWHOS	NJFAB	GLSHI	TZYXU	FWBZU	KLBHS	JGORI	YODKU
YKVQO	RTYDJ	COJWE	BBVGM	SOYLP	PZYZR	FWKNX	PBAFQ	YGASF	EUAOC
NKJID	PXMHE	FOIDY	YQZBY	MKVUA	AMZLH	GZNPJ	WCFNY	RBNAO	KXOKQ
AYIIF	NUXIO	FWIPE	YAZQB	KYZOH	KELCK	YGBFE	OXILJ	BZAZD	ZBHYA
ERHAB	UPUHO	AGOLO	LONUL	HXUNY	NKSOK	QGHXP	MFZEM	XCNJZ	ECEVW
JTTIA	FXUZI	EYOYY	VIDQN	WKWPX	DEKAN	CUEAQ	OFTDH	HYHCH	CKBBO
YUPEP	ZHPBE	QQVQG	XEFJZ	ATVHV	OAWYZ	OJOHK	YSFLF	ZWVGJ	HMFFJ
VOANG	QHBBX	QLUAI	LQDHQ	WPUON	TRFTQ	ZZFGI	JWGBW	QLGOJ	JCWVG
JOWID	PWIIB	WYRBI	EVYWN	KKRDI	KWNWF	ERLUV	RITUZ	TGXJV	EXQHA
IYLIU	OSQMX	HHZNY	URWTS	ZLDTU	PWSLS	UWXNJ	ITUUJ	VOIUY	KQSCF
CRWAV	QWLHQ	YCLNA	HNHUC	XVSVJ	NWHFR	WNRWM	CTGPP	FTYQY	OFFXV
IIATD	ALPTQ	SKDDU	IFHXD	NPHJY	RLITA	UOJOZ	KZOCR	VOLQC	EQUWW
IULMG	PIJWG	MVBMU	RZUSK	LGMQP	KVMDM	LQCON	QGSDU	FXDAA	LLDXR

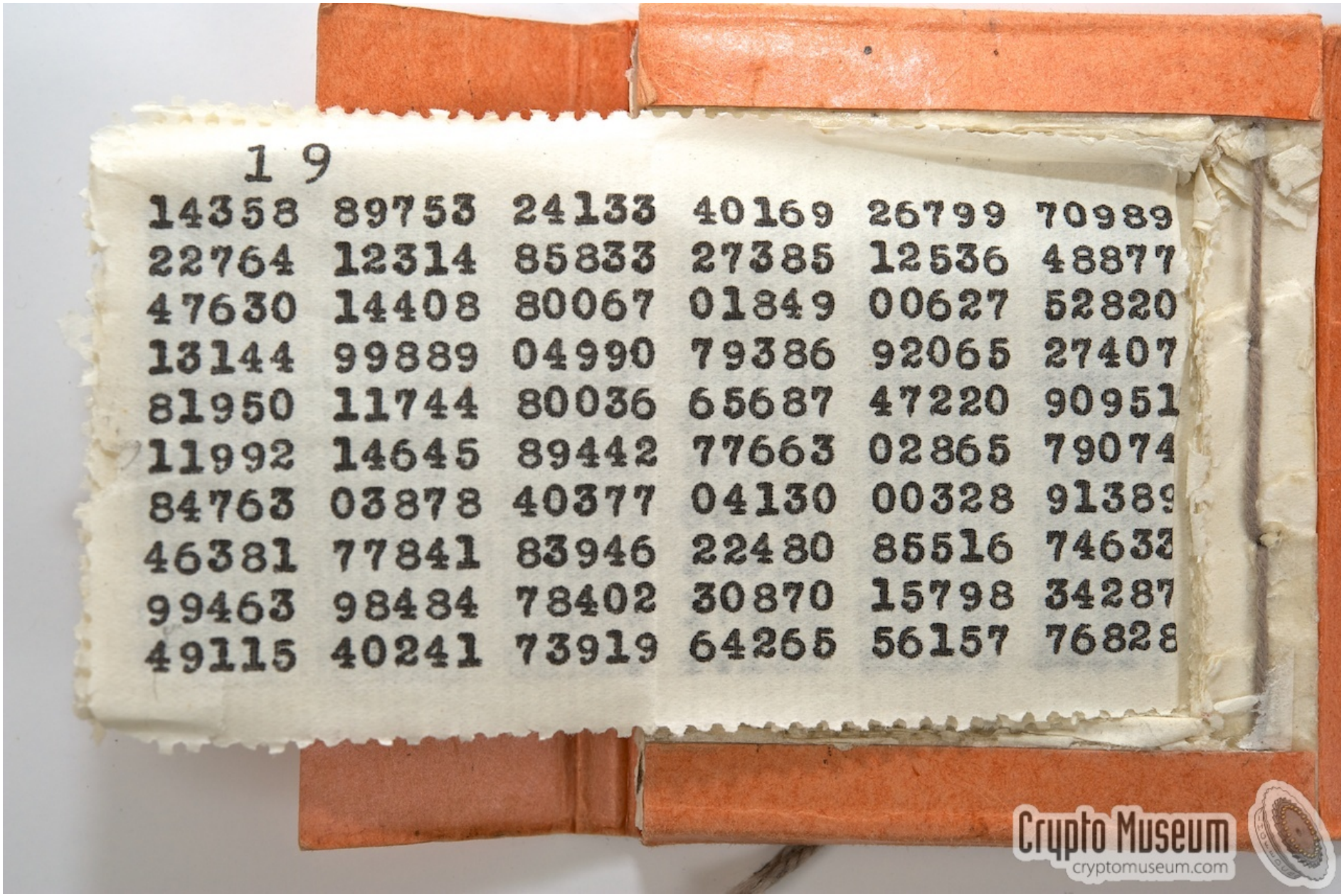
Blocchetto monouso 002

WJAEY	GDGVP	XEXQW	AEIQG	JKMSY	FUURS	OSXRL	FKQFA	WUYDE	ODOPJ
JPEVC	NCXIE	XJVKW	MQJQI	EQVIG	IJYVL	GMSIP	IAIPK	BLOFS	VZJJL
PDWRA	ZUXON	CLBGH	HIKFW	EGQFZ	BITKZ	TOEEK	HDBMF	OSZGL	QHSMQ
GURSR	WQENU	MMMQZ	NCGXC	ZXRXX	PIANL	SHDKT	RREOO	MQGGV	QFRJP
IFOZW	QDLTO	DVCWH	MWUDI	PCUZW	IQJGR	CWKNB	VFDGD	ICRPC	ZGRTO
RSCAI	RXWLL	FDPSQ	JKSDX	OVFNI	BUHYP	WCLRK	STOAN	TVINN	SEKTI
MFVDO	QEOUB	UNQKB	MWSSR	ZNGNJ	CKNOO	MTHGP	GJCLA	WPGSW	WJHHY
UJXLD	EUINU	DUBKI	TCAXB	USPMI	KKELN	VEMGP	FKYWG	AMHML	RDSGX
CNLFM	KHSJO	XOLNG	IVFVT	FWJBO	YQSSF	HTFBE	ZZVLX	DABCD	YOTPQ
DJEPF	CGHES	GWLUG	NJLCO	PHVIX	PFIJV	TXBWF	XVSBI	COFOZ	KLYYN
EPZEF	STWZV	CYHTO	XNBCV	SWJHE	DYMYF	MYKXV	EDAOG	MCFRP	GNJOI
CDOAP	NOCJK	CQXKJ	RCPXW	OFUEZ	OPNPX	BWVZP	ASWRQ	KPIWS	VXMGX
IJDCW	WTHTU	KQVAK	GVCFX	RBZCQ	NSEUJ	NOKYM	BEYJG	MLUGL	HMIUY
UZILO	QOTLQ	ESBQV	RJUWI	TICEJ	ULFMN	VNHBI	CGVRY	LSSGO	GMEZZ
NGOOA	RZNMN	MBLVU	QRZJC	LCSHD	LKQBV	KKFFR	YHFKM	NWVFT	NALJB
GSASU	GRJTA	KWYTO	KKZQN	ZLGCM	WBEAS	PCNGQ	VHLCU	CKPFR	NRGOJ
DTOJI	WOYAZ	GGOVP	CBFUA	MAZQM	AMEYX	FRKSJ	GNSWN	HIBBE	LAEVG
KSJEL	RVZFI	AAVQG	VHOHZ	PCABH	JBRYL	ZVMFB	CZGQD	FDCHR	AXOUV
QUHVR	MYADB	BGGSW	XMODX	CKBWU	GDHIY	NGZEX	PYIBN	ERHKY	PHMDF
WYAUN	JEPLC	ASECK	ZWHFF	DUZPA	ETIIB	RUCST	NVNCY	GAQHZ	PFZNZ
DXOGL	UKSXM	YCGRY	AQHRL	RDQCL	UVHUD	QWKWZ	CJKQG	NGQHM	SIACW
TBRGV	JNMGW	WXFLR	NXZKM	MEUFD	OGMGQ	SMUUF	HCVEO	FOXXV	XFKZH
JRNCV	XDCVD	KJUCI	XSJXS	HNRND	TRNJV	MKLNT	WWLAM	VXLXJ	OFKLJ
GAOVV	PTJRO	YYRQI	MBAIZ	FQKGN	WKMNV	LYETO	PFZLB	QHIVG	YTIPY
CQXZY	JCBQL	UCEIP	ULLCH	LYGKY	YUZQD	SZYGA	CQZWD	ELHPM	ZGKAO
NBBJC	SGTIM	XUQEF	HWHWS	INIKZ	EEZQQ	NPADW	RHBTX	VDXVF	KWJMO






Crypto Museum
cryptomuseum.com


19
14358 89753 24133 40169 26799 70989
22764 12314 85833 27385 12536 48877
47630 14408 80067 01849 00627 52820
13144 99889 04990 79386 92065 27407
81950 11744 80036 65687 47220 90951
11992 14645 89442 77663 02865 79074
84763 03878 40377 04130 00328 91389
46381 77841 83946 22480 85516 74633
99463 98484 78402 30870 15798 34287
49115 40241 73919 64265 56157 76828
Crypto Museum
cryptomuseum.com

La macchina ENIGMA

È una macchina tedesca usata per codificare i messaggi durante la II Guerra Mondiale. Basata su tre rotori (scelti tra cinque disponibili), posizionati all'inizio in una posizione concordata e che poi continuavano a ruotare ad ogni lettera, cambiando cifrario ogni volta.

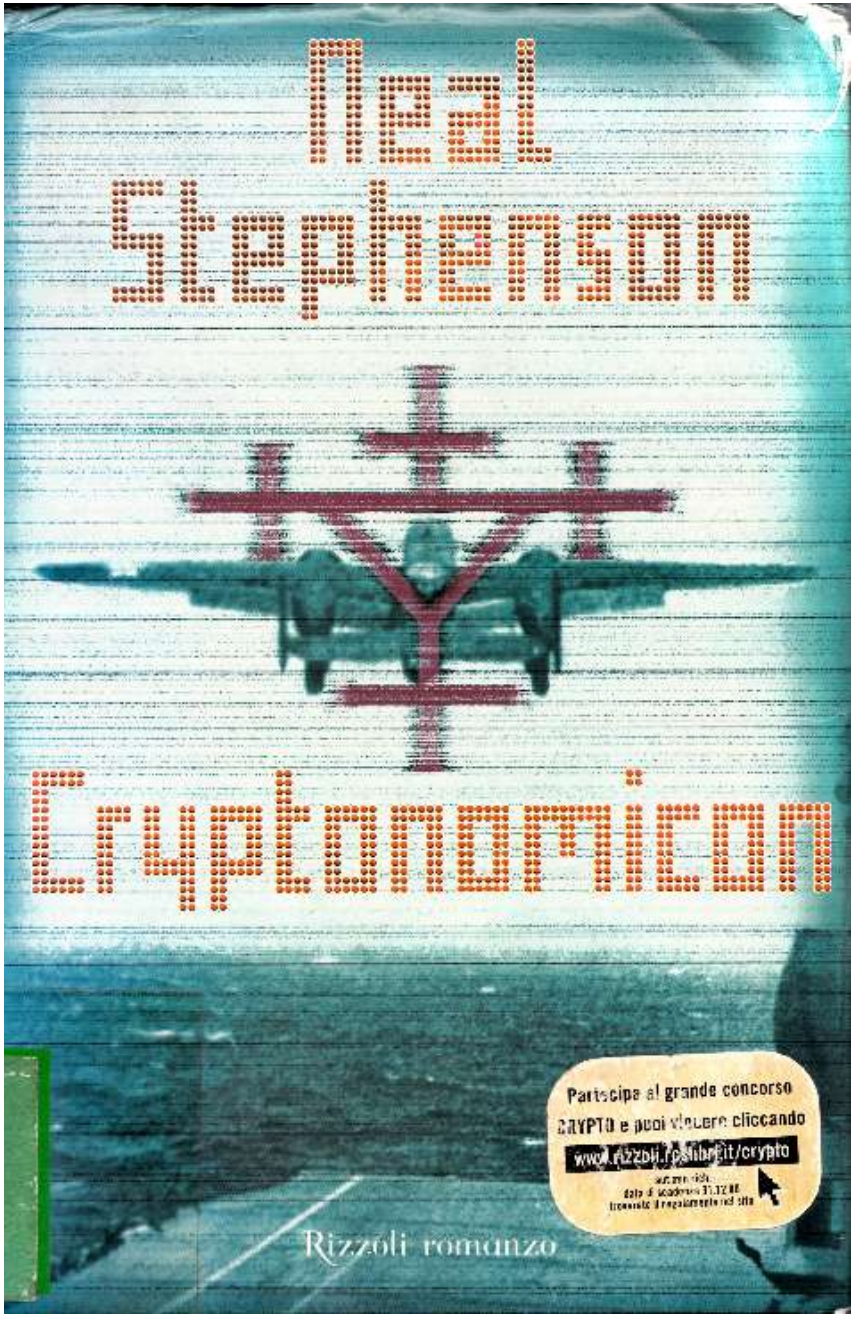

ENIGMA

Alan Turing

Alan Turing (1912–1954), tra i più grandi matematici del XX secolo, uno dei padri dell'informatica.
Inventa il concetto di **macchina di Turing** e il **test di Turing**.
Durante la II Guerra Mondiale lavora a Bletchley Park, dove risulta determinante nella decrittazione del codice Enigma, perfezionando il progetto della "Bomba", il capostipite dei calcolatori elettronici, progettato inizialmente in Polonia.
Turing era un ottimo corridore: aveva un personale sulla maratona di 2h46'3", un tempo di solo 11 minuti più alto del vincitore dei Giochi Olimpici di Londra del 1948 Delfo Cabrera.


THE TRUE ENIGMA
WAS THE MAN WHO CRACKED
THE CODE
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
THE IMITATION GAME


Unlock the secret
DOUGRAY SCOTT KATE WINSLET JEREMY NORTHAM SAFFRON BURROWS
FROM DIRECTOR MICHAEL APTED AND ACADEMY AWARD® WINNER WRITER TOM STOPPARD. BASED ON THE BEST SELLING NOVEL BY ROBERT HARRIS.
ENIGMA
15


Neal Stephenson
Cryptonomicon
Partecipa al grande concorso
CRYPTO e puoi vincere cliccando
Rizzoli romanzo


Simon Singh
CODICI & SEGRETI
La storia affascinante
dei messaggi cifrati
dall'antico Egitto a Internet
BUR
rizzoli
SAGGI

Verso i cifrari contemporanei: i cifrari poligrafici

Nei cifrari contemporanei non si usa più codificare una lettera alla volta, ma si suddivide il messaggio in blocchi di due o più lettere, e sono i blocchi ad essere codificati singolarmente. In questo modo la procedura si complica, poiché aumenta molto il numero dei simboli e si rende molto più difficile l'analisi delle frequenze.

Verso i cifrari contemporanei: i cifrari poligrafici

Nei cifrari contemporanei non si usa più codificare una lettera alla volta, ma si suddivide il messaggio in blocchi di due o più lettere, e sono i blocchi ad essere codificati singolarmente. In questo modo la procedura si complica, poiché aumenta molto il numero dei simboli e si rende molto più difficile l'analisi delle frequenze.

Ad esempio, esistono $26^2 = 676$ coppie di lettere possibili e $26^3 = 17576$ terne di lettere possibili.

Verso i cifrari contemporanei: i cifrari poligrafici

Nei cifrari contemporanei non si usa più codificare una lettera alla volta, ma si suddivide il messaggio in blocchi di due o più lettere, e sono i blocchi ad essere codificati singolarmente. In questo modo la procedura si complica, poiché aumenta molto il numero dei simboli e si rende molto più difficile l'analisi delle frequenze.

Ad esempio, esistono $26^2 = 676$ coppie di lettere possibili e $26^3 = 17576$ terne di lettere possibili.
Gli attuali cifrari (DES, AES) si basano su questo principio.

Verso i cifrari contemporanei: i cifrari poligrafici

Nei cifrari contemporanei non si usa più codificare una lettera alla volta, ma si suddivide il messaggio in blocchi di due o più lettere, e sono i blocchi ad essere codificati singolarmente. In questo modo la procedura si complica, poiché aumenta molto il numero dei simboli e si rende molto più difficile l'analisi delle frequenze.

Ad esempio, esistono $26^2 = 676$ coppie di lettere possibili e $26^3 = 17576$ terne di lettere possibili.
Gli attuali cifrari (DES, AES) si basano su questo principio.

Ma rimane sempre il problema di scambiarsi la chiave!

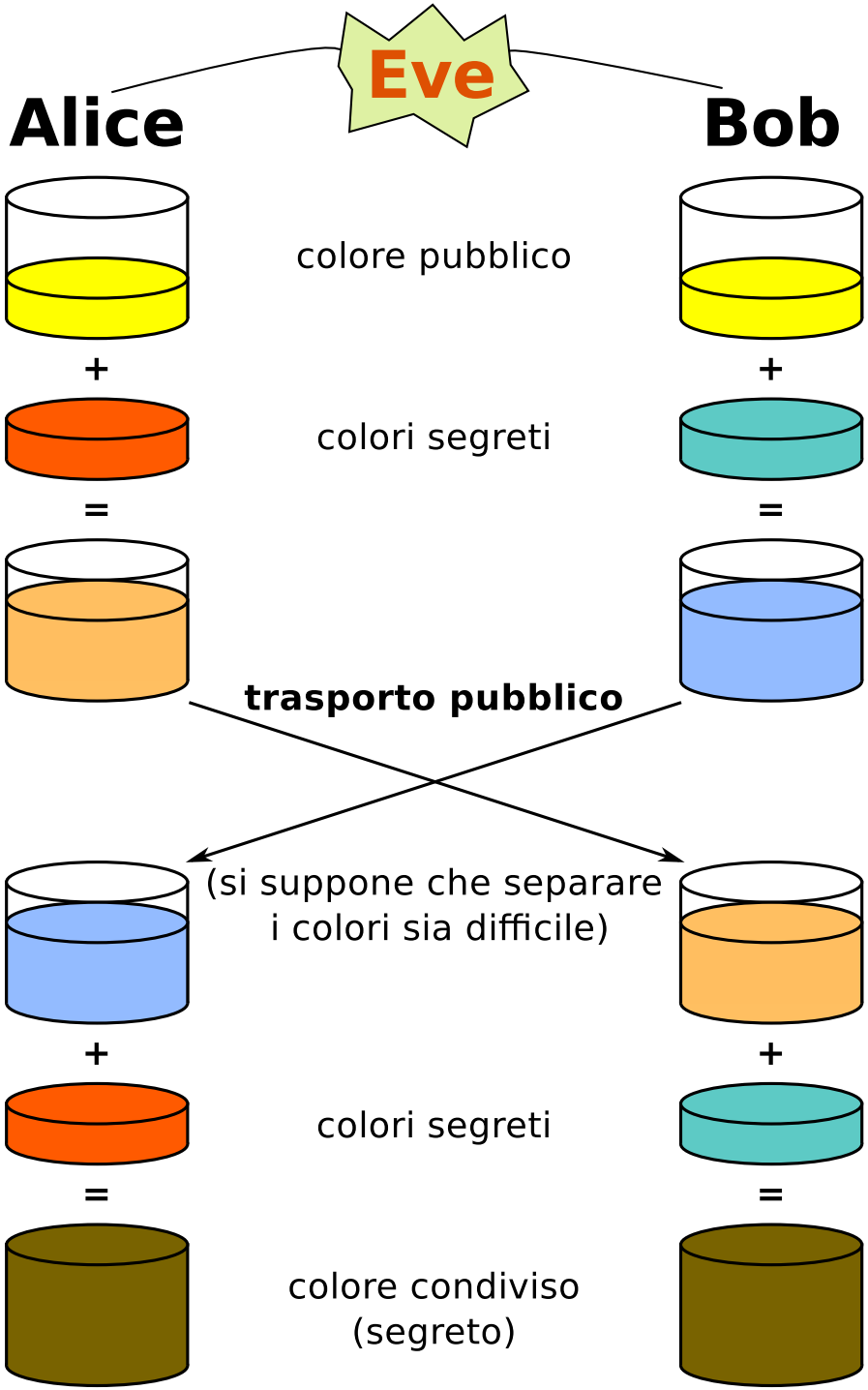
Parte III

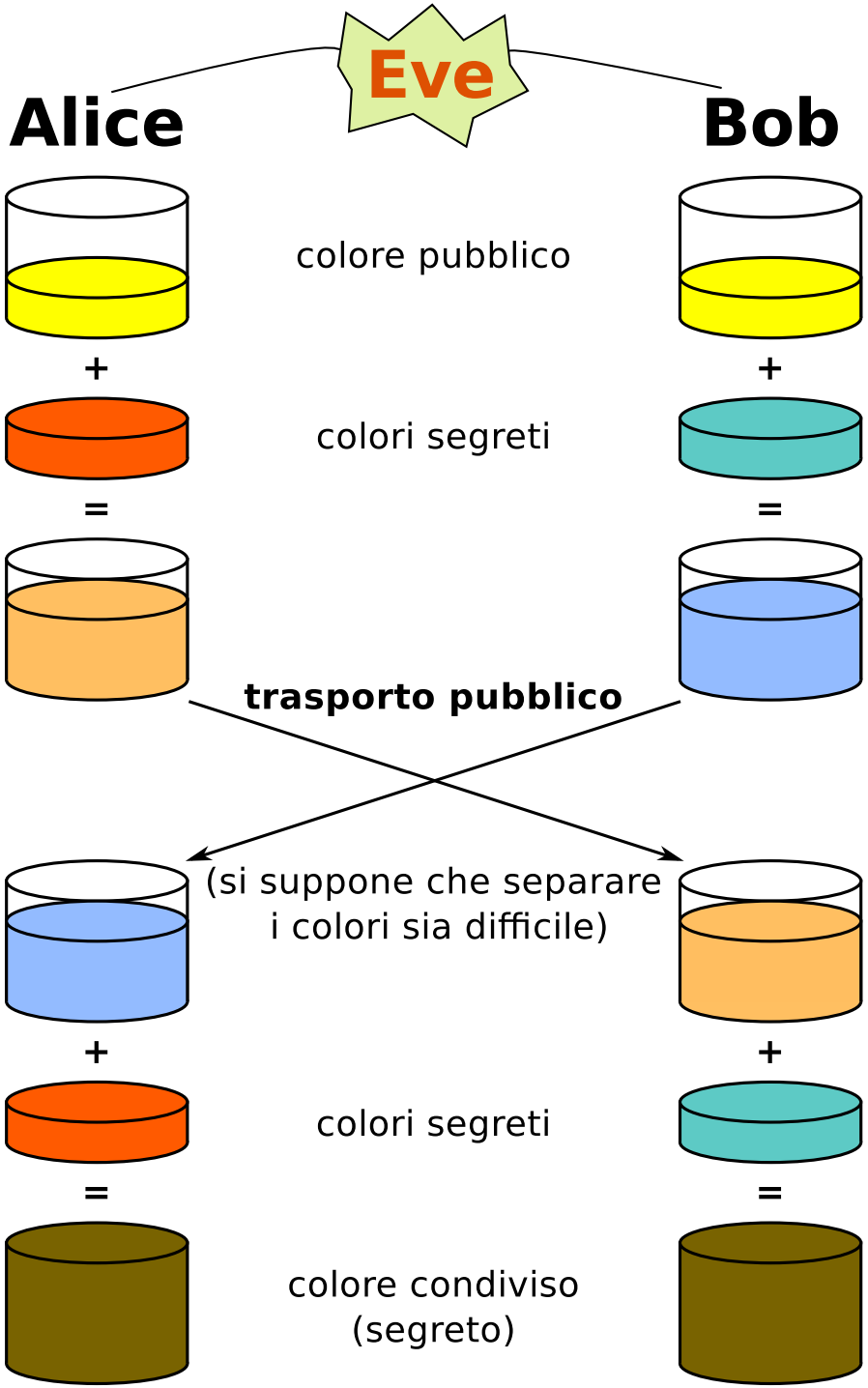
La matematica della crittografia

Condivisione di una chiave: l'esempio con i colori

Alice e Bob vogliono poter scambiare messaggi senza che altri (rappresentati da Eve, il malvagio) li capiscano. Per fare questo devono entrambi avere una "chiave" che apra lo stesso lucchetto. Come possono fare a condividere questa chiave?

Vediamo un esempio, fatto coi colori, che si basa su un colore segreto (la chiave privata) e un colore noto a tutti (la chiave pubblica). Entrambi giungono a condividere un colore senza che Eve ne sia a conoscenza.


Eve
Alice
Bob
colore pubblico
+
colori segreti
=
trasporto pubblico
(si suppone che separare
i colori sia difficile)
+
colori segreti
=
colore condiviso
(segreto)



È **facile** mescolare i colori, ma è **difficile** capire quali colori formano una miscela.

Si parla di
funzione unidirezionale

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.
Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.
Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.
Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

Provate a fattorizzare il numero 390900163...

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.
Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

Provate a fattorizzare il numero 390900163...
E invece verificate, con la calcolatrice, quanto fa

$$14087 \times 27749$$

Come fare nella realtà?

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire.
Esempio importante: è facile (magari con una calcolatrice!) calcolare

$$59 \times 31 = 1829$$

ma è **mooolto** più difficile (perché ci vuole tanto tempo!) scoprire che 1829 è composto da 59 e 31.

Provate a fattorizzare il numero 390900163...
E invece verificate, con la calcolatrice, quanto fa

$$14087 \times 27749$$

Nelle attuali applicazioni informatiche si usano numeri di 1024 bit, che superano le 300 cifre decimali, e addirittura di 2048 bit!

RSA Factoring Challenge

Nel 1991 fu lanciato un concorso che chiedeva di fattorizzare alcuni numeri grandi, per stimolare la ricerca sulla sicurezza dell'algoritmo RSA, che si basa sulla fattorizzazione. Nel 2007 il concorso si è ufficialmente chiuso, ma tuttora alcuni gruppi stanno tentando di risolvere alcune delle sfide proposte.
Nel settembre del 2013 è stato fattorizzato il numero RSA-210, composto da 210 cifre decimali!

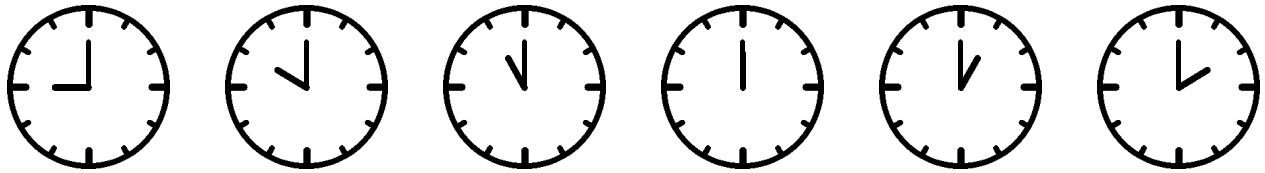
$$
\begin{aligned}
&2452466449002782119765176635730880184670267876783327597434144517150616\\
&0083003858721695220839933207154910362682719167986407977672324300560059\\
&2035631246561218465817904100131859299619933817012149335034875870551067 = \\
&\\
&\quad 435958568325940791799951965387214406385470910265220 19\\
&\quad 631870548214452408534527599974024462525542845594457 9 \quad \times\\
&\quad 562545761726884103756277007304447481743876944007510 54\\
&\quad 510494685109454839657747947347214622855079932293927 3
\end{aligned}
$$

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

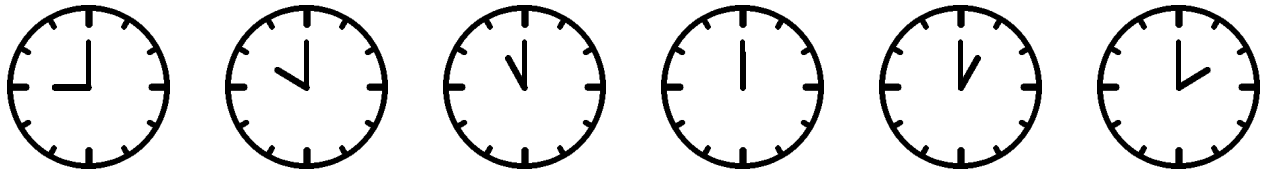
Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?



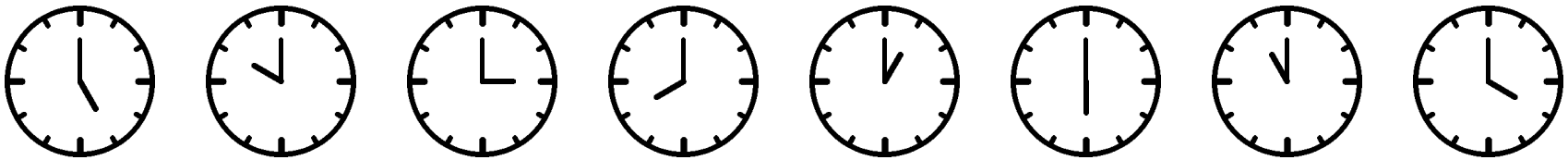
Ovviamente, le 2.

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?



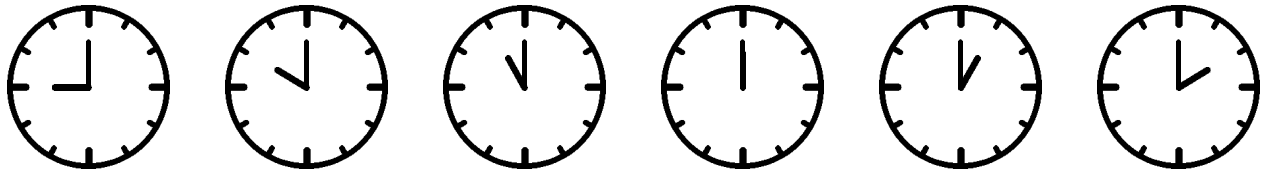
Ovviamente, le 2.
Se l'orologio segna le 5 si "moltiplica" quest'ora per 8, che ora risulterà?



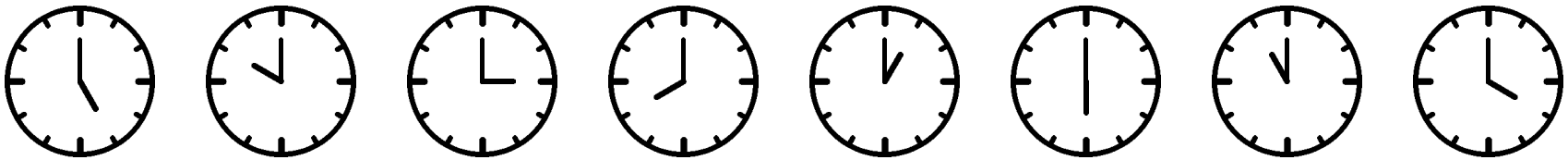
Le 4, poiché $5 \times 8 = 40 = 12 \times 3 + 4$. Quindi la lancetta delle ore fa tre giri e finisce sulle 4.

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?



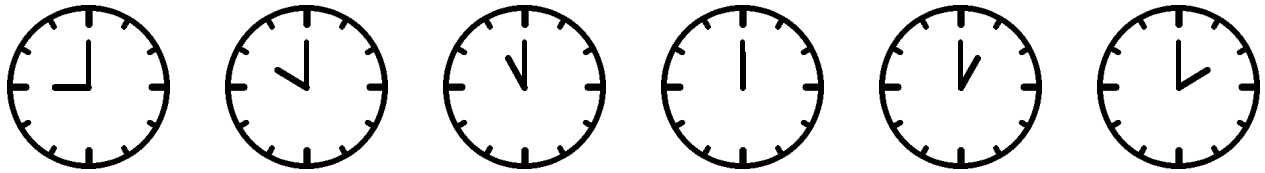
Ovviamente, le 2.
Se l'orologio segna le 5 si "moltiplica" quest'ora per 8, che ora risulterà?



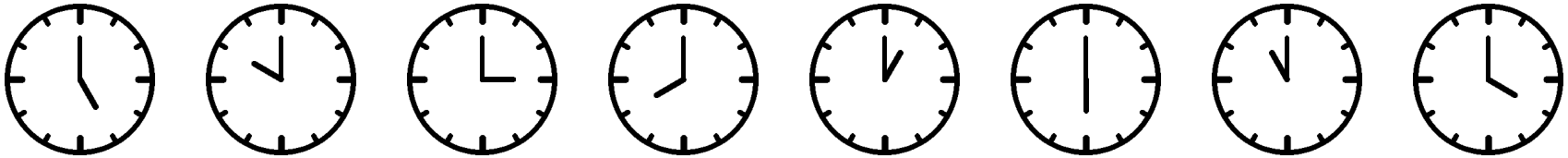
Le 4, poiché $5 \times 8 = 40 = 12 \times 3 + 4$. Quindi la lancetta delle ore fa tre giri e finisce sulle 4.
Nell'aritmetica "dell'orologio" non interessa il numero dei giri, ma solo quello che avanza alla fine (il **resto** della divisione).

Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se un orologio segna le 9 e si aggiungono 5 ore, che ora segnerà?



Ovviamente, le 2.
Se l'orologio segna le 5 si "moltiplica" quest'ora per 8, che ora risulterà?



Le 4, poiché $5 \times 8 = 40 = 12 \times 3 + 4$. Quindi la lancetta delle ore fa tre giri e finisce sulle 4.
Nell'aritmetica "dell'orologio" non interessa il numero dei giri, ma solo quello che avanza alla fine (il **resto** della divisione).
Questa si chiama **aritmetica modulare**.

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).
Scrivere $(\mathrm{mod}\, p)$ significa che delle operazioni che si fanno bisogna tenere solo il resto della divisione per p.

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).
Scrivere $(\mathrm{mod}\, p)$ significa che delle operazioni che si fanno bisogna tenere solo il resto della divisione per p.

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5(\mathrm{mod}11),$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).
Scrivere $(\mathrm{mod}\, p)$ significa che delle operazioni che si fanno bisogna tenere solo il resto della divisione per p.

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5(\mathrm{mod}11), \quad 5 \times 8 = 7(\mathrm{mod}11),$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).
Scrivere $(\mathrm{mod}\, p)$ significa che delle operazioni che si fanno bisogna tenere solo il resto della divisione per p.

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5(\mathrm{mod}11), \quad 5 \times 8 = 7(\mathrm{mod}11), \quad 2^6 = 9(\mathrm{mod}11)$$

L'aritmetica modulare con numeri primi

Risulta particolarmente utile usare "orologi" con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "$(\mathrm{mod}\, p)$" (si legge **modulo** p).
Scrivere $(\mathrm{mod}\, p)$ significa che delle operazioni che si fanno bisogna tenere solo il resto della divisione per p.

Ad esempio, scegliendo $p = 11$, avremo

$$7 + 9 = 5(\mathrm{mod}11), \quad 5 \times 8 = 7(\mathrm{mod}11), \quad 2^6 = 9(\mathrm{mod}11)$$

L'insieme dei numeri $\{0, 1, \ldots, p-1\}$ dotato di queste operazioni particolari si denota con $\mathbb{Z}_p$.

Generatori di $\mathbb{Z}_p$

Un **generatore** g in $\mathbb{Z}_p$ è un numero più piccolo di p tale che calcolando

$$g, g^2, g^3, \ldots, g^{p-2}, g^{p-1} (\mathrm{mod}\, p)$$

si esauriscano tutti i numeri tra 1 e $p-1$. Ad esempio, si può verificare che 2 è un generatore per $p = 11$, poiché

n	1	2	3	4	5	6	7	8	9	10
$2^n (\mathrm{mod} 11)$	2	4	8	5	10	9	7	3	6	1

Generatori di $\mathbb{Z}_p$

Un **generatore** g in $\mathbb{Z}_p$ è un numero più piccolo di p tale che calcolando

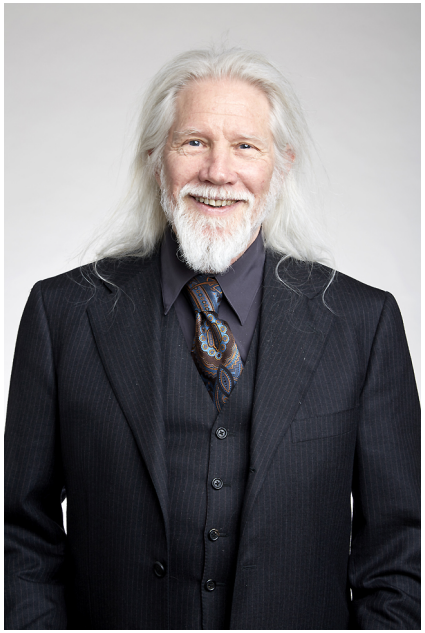
$$g, g^2, g^3, \ldots, g^{p-2}, g^{p-1} (\mathrm{mod}\, p)$$

si esauriscano tutti i numeri tra 1 e $p-1$. Ad esempio, si può verificare che 2 è un generatore per $p = 11$, poiché

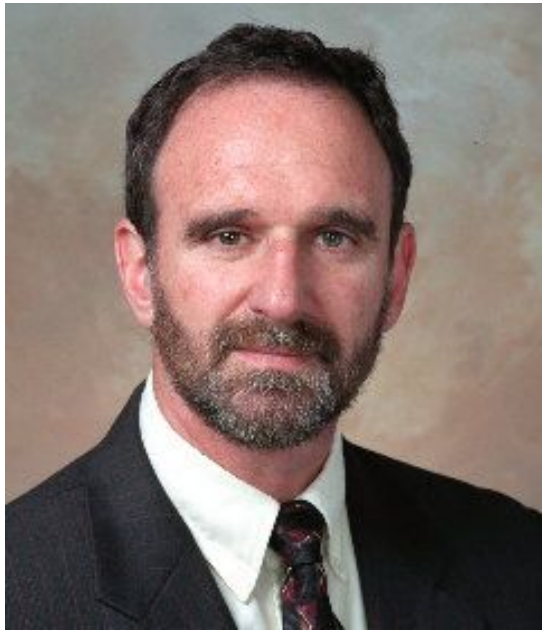
n	1	2	3	4	5	6	7	8	9	10
$2^n (\mathrm{mod} 11)$	2	4	8	5	10	9	7	3	6	1

Se p è primo, esiste sempre almeno un generatore in $\mathbb{Z}_p$, anche se potrebbe non essere semplice trovarlo.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)



Whitfield Diffie



Martin Hellman

Ralph Merkle

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.
È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.
È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.
Ad esempio, si verifica che 6 è un generatore per $p = 17$, poiché

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6^n	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.
È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.
Ad esempio, si verifica che 6 è un generatore per $p = 17$, poiché

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6^n	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Questi numeri p e g sono noti a tutti e decisi una volta per tutte. Nella pratica p è un numero molto grande (1024 bit), mentre g può anche essere piccolo.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo per condividere un numero tra due persone, in modo che solo loro due lo conoscano. Questo numero potrà poi servire a scambiarsi messaggi in codice.
È basato sull'elevamento a potenza e sull'aritmetica dell'orologio. Si prende un numero primo p, ad esempio $p = 17$, e un generatore g di $\mathbb{Z}_{17}$.
Ad esempio, si verifica che 6 è un generatore per $p = 17$, poiché

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6^n	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Questi numeri p e g sono noti a tutti e decisi una volta per tutte. Nella pratica p è un numero molto grande (1024 bit), mentre g può anche essere piccolo.

Poi si esegue la procedura seguente:

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) =$

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) =$

6^n:	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$ e Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod} 17) = 9$.

6^n:	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$ e Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod} 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

6^n:	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$ e Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod} 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

3) Infine Alice prende la chiave pubblica di Bob, $B = 9$, e calcola $B^a (\mathrm{mod}\, p) = 9^{10} (\mathrm{mod} 17) = 13$.

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod} 17) = 15$ e Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod} 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

3) Infine Alice prende la chiave pubblica di Bob, $B = 9$, e calcola $B^a (\mathrm{mod}\, p) = 9^{10} (\mathrm{mod} 17) = 13$.
Bob prende la chiave pubblica di Alice, $A = 15$, e calcola $A^b (\mathrm{mod}\, p) = 15^{14} (\mathrm{mod} 17) = 13$.

1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e vanno tenuti **segreti**.
Nel nostro esempio, scegliamo $a = 10$ e $b = 14$.

2) Alice calcola il numero $A = g^a (\mathrm{mod}\, p) = 6^{10} (\mathrm{mod}\, 17) = 15$ e Bob calcola il numero $B = g^b (\mathrm{mod}\, p) = 6^{14} (\mathrm{mod}\, 17) = 9$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.

3) Infine Alice prende la chiave pubblica di Bob, $B = 9$, e calcola $B^a (\mathrm{mod}\, p) = 9^{10} (\mathrm{mod}\, 17) = 13$.
Bob prende la chiave pubblica di Alice, $A = 15$, e calcola $A^b (\mathrm{mod}\, p) = 15^{14} (\mathrm{mod}\, 17) = 13$.

È un caso che sia risultato lo stesso numero? Certamente no: si ha **sempre** $A^b = (g^a)^b = g^{ab} = (g^b)^a = B^a (\mathrm{mod}\, p)$.
Quindi Alice e Bob hanno una chiave in comune: il numero $\boxed{13}$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Scegliamo (a caso) le chiavi private: $a = 32359975$, $b = 6431846$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Scegliamo (a caso) le chiavi private: $a = 32359975$, $b = 6431846$.

Allora le chiavi pubbliche sono $A = g^a = 19135999$, $B = g^b = 5444512$.

Un esempio con numeri più grandi

$p = 34121249$ è un numero primo e $g = 5$ è un generatore di $\mathbb{Z}_{34121249}$.

Scegliamo (a caso) le chiavi private: $a = 32359975$, $b = 6431846$.

Allora le chiavi pubbliche sono $A = g^a = 19135999$, $B = g^b = 5444512$.

E si ha $A^b = B^a = 18352668$, che è la chiave condivisa.

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Nel nostro esempio, sapendo che $p = 17$, $g = 6$ e $A = g^a = 15$, si può scoprire a: scorrendo tutta la tabella delle potenze del generatore si va a cercare quale potenza di 6 risulta 15 (modulo 17), e si trova $n = 10$. Quindi la chiave segreta di Alice è 10.

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Nel nostro esempio, sapendo che $p = 17$, $g = 6$ e $A = g^a = 15$, si può scoprire a: scorrendo tutta la tabella delle potenze del generatore si va a cercare quale potenza di 6 risulta 15 (modulo 17), e si trova $n = 10$. Quindi la chiave segreta di Alice è 10.

Ma allora dove sta la sicurezza della procedura? Nella realtà si usano numeri primi molto grandi, fatti da almeno 300 cifre, e la lista da scorrere per individuare l'esponente a a partire dalla conoscenza di g^a è molto, molto lunga!

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$? L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.

Nel nostro esempio, sapendo che $p = 17$, $g = 6$ e $A = g^a = 15$, si può scoprire a: scorrendo tutta la tabella delle potenze del generatore si va a cercare quale potenza di 6 risulta 15 (modulo 17), e si trova $n = 10$. Quindi la chiave segreta di Alice è 10.

Ma allora dove sta la sicurezza della procedura? Nella realtà si usano numeri primi molto grandi, fatti da almeno 300 cifre, e la lista da scorrere per individuare l'esponente a a partire dalla conoscenza di g^a è molto, molto lunga!

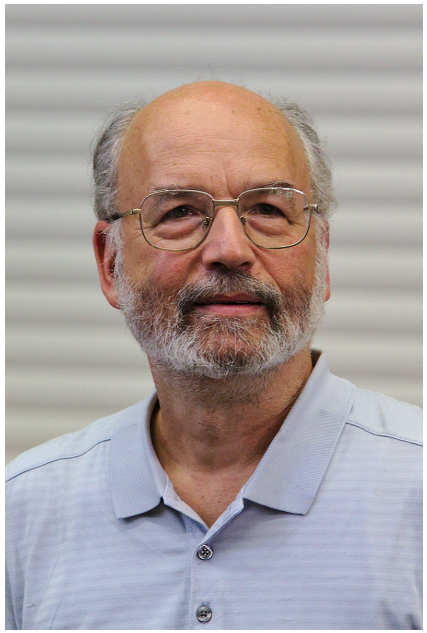
Questa operazione si chiama **logaritmo discreto**, ed è una funzione unidirezionale: è abbastanza facile calcolare $A = g^a$, ma è molto difficile scoprire l'esponente a conoscendo g e A. Anche i computer attualmente più potenti impiegherebbero centinaia di anni.

Utilizzo della chiave condivisa

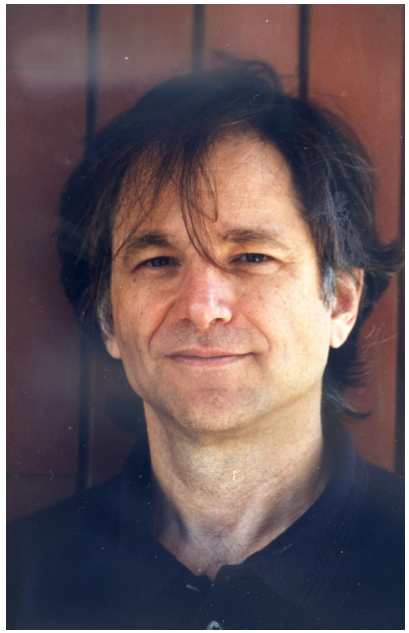
Una volta ottenuta una chiave condivisa, si può procedere a crittografare un messaggio in vari modi. Ad esempio, se Alice vuole comunicare a Bob un numero segreto, per esempio il numero della sua carta di credito 2442 4243 5089 4523, può moltiplicarlo per la chiave comune $\boxed{13}$, ottenendo 3175151656162879 9. Bob, ricevuto il numero, lo divide per 13 riottenendo il numero di partenza.
Il malvagio Eve, sempre in ascolto, vedrebbe passare il numero 3175151656162879 9, ma non potrebbe collegarlo al numero di carta di credito di Alice (a meno che non conosca la chiave comune). Oppure la chiave comune potrebbe essere il punto di partenza per un cifrario di Cesare, significando uno spostamento di 13 lettere: il nome ALESSANDRO diventerebbe NYRFFNAQEB (nell'alfabeto a 26 lettere) e Bob potrebbe facilmente decodificarlo.
Attualmente il metodo più usato per codificare messaggi con una chiave condivisa è l'algoritmo AES (Advanced Encryption Standard).

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

Ronald Rivest



Adi Shamir



Leonard Adleman

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ e che non abbia fattori in comune con r

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ e che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ e che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- Si rende pubblica la coppia (N, e) (chiave pubblica) e si tiene segreto il numero d (chiave privata).

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ e che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- Si rende pubblica la coppia (N, e) (chiave pubblica) e si tiene segreto il numero d (chiave privata).

Ad esempio: scegliendo $p = 3$, $q = 19$, si ha $N = 57$ e $r = 36$.

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ e che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- Si rende pubblica la coppia (N, e) (chiave pubblica) e si tiene segreto il numero d (chiave privata).

Ad esempio: scegliendo $p = 3$, $q = 19$, si ha $N = 57$ e $r = 36$.
Scegliamo $e = 5$, che non ha fattori in comune con 36.

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ e che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- Si rende pubblica la coppia (N, e) (chiave pubblica) e si tiene segreto il numero d (chiave privata).

Ad esempio: scegliendo $p = 3$, $q = 19$, si ha $N = 57$ e $r = 36$.
Scegliamo $e = 5$, che non ha fattori in comune con 36.
Si verifica che $5 \cdot 29 = 1 (\mathrm{mod} 36)$, quindi prendiamo $d = 29$.

L'algoritmo RSA (Rivest, Shamir, Adleman, 1977)

È tuttora usato in quasi tutte le transazioni sicure online (https).

- Si prendono due numeri primi grandi p, q e si calcolano $N = p \cdot q$ e $r = (p-1) \cdot (q-1)$
- Si sceglie un numero e tale che $1 < e < r$ e che non abbia fattori in comune con r
- Si cerca quel numero d tale che $e \cdot d = 1 (\mathrm{mod}\, r)$
- Si rende pubblica la coppia (N, e) (chiave pubblica) e si tiene segreto il numero d (chiave privata).

Ad esempio: scegliendo $p = 3$, $q = 19$, si ha $N = 57$ e $r = 36$.
Scegliamo $e = 5$, che non ha fattori in comune con 36.
Si verifica che $5 \cdot 29 = 1 (\mathrm{mod} 36)$, quindi prendiamo $d = 29$.
Ora teniamo segreta la chiave privata 29 e rendiamo pubblica la coppia $(57, 5)$, ad esempio scrivendola su un sito.

Chiave pubblica: $(57, 5)$, chiave privata 29

Supponiamo ora che qualcuno voglia comunicarci segretamente un numero m, ad esempio $m = 10$. Deve procedere così:

Chiave pubblica: $(57, 5)$, chiave privata 29

Supponiamo ora che qualcuno voglia comunicarci segretamente un numero m, ad esempio $m = 10$. Deve procedere così:

prende $(57, 5)$, che è pubblica, e calcola

$$10^5 (\mathrm{mod} 57) = 22;$$

poi ci comunica il risultato 22.

Chiave pubblica: $(57, 5)$, chiave privata 29

Supponiamo ora che qualcuno voglia comunicarci segretamente un numero m, ad esempio $m = 10$. Deve procedere così:

prende $(57, 5)$, che è pubblica, e calcola

$$10^5 (\mathrm{mod} 57) = 22;$$

poi ci comunica il risultato 22.

Noi poi calcoliamo $22^{29} (\mathrm{mod} 57)$ usando la nostra chiave privata.

Chiave pubblica: $(57, 5)$, chiave privata 29

Supponiamo ora che qualcuno voglia comunicarci segretamente un numero m, ad esempio $m = 10$. Deve procedere così:

prende $(57, 5)$, che è pubblica, e calcola

$$10^5 (\mathrm{mod} 57) = 22;$$

poi ci comunica il risultato 22.

Noi poi calcoliamo $22^{29} (\mathrm{mod} 57)$ usando la nostra chiave privata.

Risulta

$$22^{29} (\mathrm{mod} 57) = 10$$

che è proprio il numero di partenza.

Se vuole comunicarci il numero 13, calcola $13^5 (\mathrm{mod} 57) = 52$, ce lo comunica e noi poi calcoliamo $52^{29} (\mathrm{mod} 57) = 13$.

Sicurezza dell'RSA

In teoria, conoscendo $(57, 5)$ è possibile trovare la chiave privata 29:

Sicurezza dell'RSA

In teoria, conoscendo $(57, 5)$ è possibile trovare la chiave privata 29: basta fattorizzare $57 = 3 \cdot 19$, poi calcolare $r = 2 \cdot 18 = 36$, e infine cercare d tale che

$$5 \cdot d = 1 (\mathrm{mod} 36).$$

Sicurezza dell'RSA

In teoria, conoscendo $(57, 5)$ è possibile trovare la chiave privata 29: basta fattorizzare $57 = 3 \cdot 19$, poi calcolare $r = 2 \cdot 18 = 36$, e infine cercare d tale che

$$5 \cdot d = 1 (\mathrm{mod} 36).$$

Ma per fattorizzare N bisogna andare per tentativi!

Nelle transazioni si usano di solito numeri primi di più di 300 cifre!

Sarebbero richieste centinaia di anni di calcoli con un super-computer...

Sicurezza dell'RSA

In teoria, conoscendo $(57, 5)$ è possibile trovare la chiave privata 29: basta fattorizzare $57 = 3 \cdot 19$, poi calcolare $r = 2 \cdot 18 = 36$, e infine cercare d tale che

$$5 \cdot d = 1 (\mathrm{mod} 36).$$

Ma per fattorizzare N bisogna andare per tentativi!

Nelle transazioni si usano di solito numeri primi di più di 300 cifre!

Sarebbero richieste centinaia di anni di calcoli con un super-computer...

a meno di non trovare un metodo alternativo

Sicurezza dell'RSA

In teoria, conoscendo $(57, 5)$ è possibile trovare la chiave privata 29: basta fattorizzare $57 = 3 \cdot 19$, poi calcolare $r = 2 \cdot 18 = 36$, e infine cercare d tale che

$$5 \cdot d = 1 (\mathrm{mod} 36).$$

Ma per fattorizzare N bisogna andare per tentativi!

Nelle transazioni si usano di solito numeri primi di più di 300 cifre!

Sarebbero richieste centinaia di anni di calcoli con un super-computer...

a meno di non trovare un metodo alternativo (che nessuno ha ancora scoperto!)