Crittografia Quantistica:

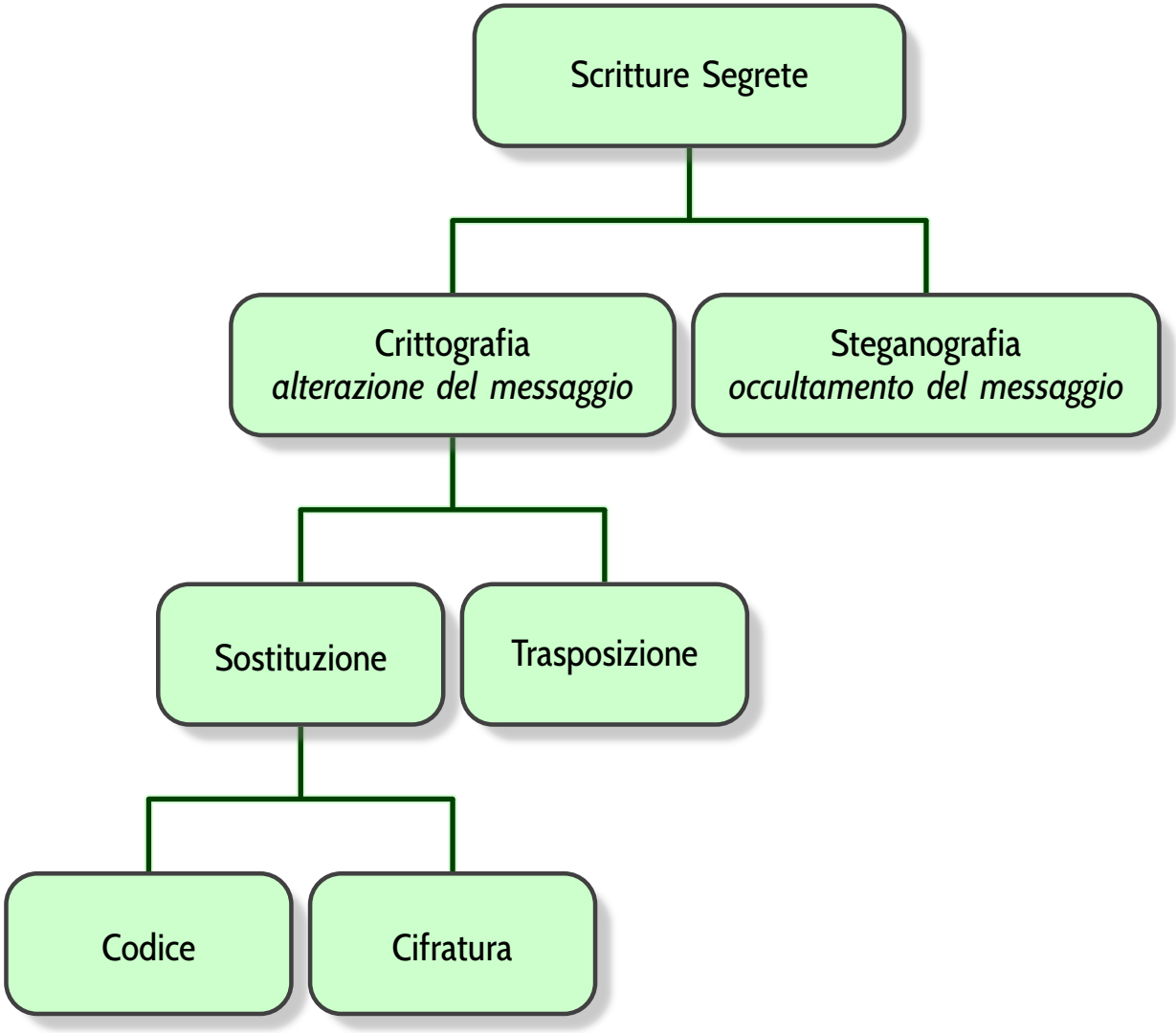
Quando la fisica dell'infinitamente piccolo entra nella vita di tutti i giorni

Mauro Orlandini
INAF/OAS Bologna

Rev: 1.7 (2023/02/02)

Parte I
Fondamenti di Crittografia

Le Scritture Segrete



Le Scritture Segrete

- **Steganografia:** da στεγανός (*steganòs,* coperto) e γραφία (*gràphein,* scrittura);
- **Crittografia:** da κρυπτός (*kryptos,* nascosto) e γραφία (*gràphein,* scrittura);
  - **Trasposizione:** le lettere sono spostate, mantenendo la propria identità (anagramma);
  - **Sostituzione:** le lettere vengono sostituite con altre, mantenendo il proprio posto;
    - **Codice:** alle parole viene dato un significato diverso;
    - **Cifratura:** le lettere vengono mescolate per mezzo di un algoritmo crittografico, invertibile con una *chiave.*

❑ Le tavolette raccontate da Erodoto (V secolo A.C.)

Racconta Erodoto (484–425 A.C.), nelle sue *Storie,* (Libro VII, 239) di Demarato, un esule greco stabilitosi nella città persiana di Susa:

❑ Le tavolette raccontate da Erodoto (V secolo A.C.)

Infatti, il pericolo di essere scoperti era grande; gli venne in mente un solo modo di far giungere in patria l'avviso: grattar via la cera da un paio di tavolette per scrittura, annotare sul legno sottostante le intenzioni di Serse, e ricoprire il messaggio con cera nuova. In tal modo le tavolette, che sembravano vergini, furono recapitate senza insospettire le guardie. Quando il messaggio giunse a destinazione, mi risulta che nessuno immaginò la sua esistenza, finché Gorgo, moglie di Leonida, ebbe una premonizione che, grattando via la cera , sul legno sarebbe apparsa una scritta. Fu fatto così, il messaggio fu trovato e letto, poi riferito agli altri greci.

Steganografia

❑ Steganografia su formati digitali: bmp, wav, gif, jpg

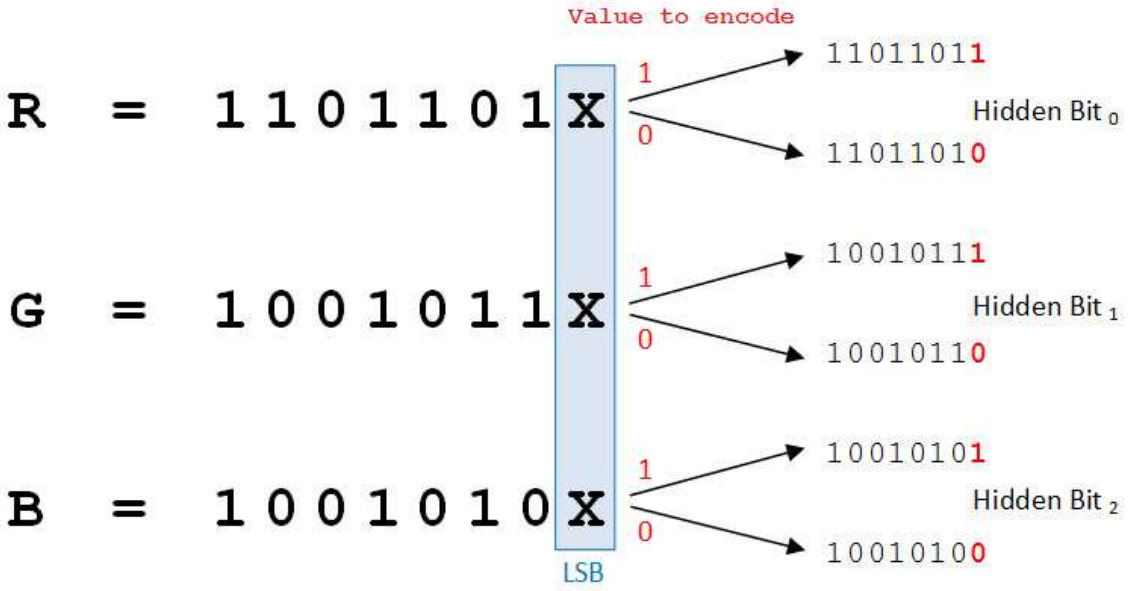
Si basa sulla teoria secondo la quale l'aspetto di un'immagine digitale ad alta definizione non cambia se i colori vengono modificati in modo impercettibile.

Immagine originale

Immagine steganografica

Steganografia su formati digitali: bmp, wav, gif, jpg

Si basa sulla teoria secondo la quale l'aspetto di un'immagine digitale ad alta definizione non cambia se i colori vengono modificati in modo impercettibile.



Crittografia per Trasposizione

Le lettere del messaggio sono mutate di posto generando un *anagramma.*

Per messaggi brevi non dà alcuna sicurezza, ma per messaggi lunghi il numero di anagrammi "esplode".

Se una parola contiene n simboli senza ripetizioni, il numero dei suoi anagrammi, cioè il numero delle permutazioni di n oggetti è n fattoriale, cioè

$$n! = n(n-1)(n-2)\ldots 1$$

Crittografia per Trasposizione

Le lettere del messaggio sono mutate di posto generando un *anagramma.*

Gli anagrammi della parola CANE ($n = 4$) sono $4! = 4 \times 3 \times 2 \times 1 = 24$

ENAC	NEAC	EANC	AENC	NAEC	ANEC
ENCA	NECA	ECNA	CENA	NCEA	CNEA
EACN	AECN	ECAN	CEAN	ACEN	CAEN
NACE	ANCE	NCAE	CNAE	ACNE	CANE

Crittografia per Trasposizione

Le lettere del messaggio sono mutate di posto generando un *anagramma.*

Il fattoriale è una funzione che cresce **MOLTO** velocemente, come si può vedere dalla seguente tabella

1	1
2	2
3	6
4	24
5	120
6	720
7	5,040
8	40,320
9	362,880
10	3,628,800
11	39,916,800
12	479,001,600
13	6,227,020,800
14	87,178,291,200
15	1,307,674,368,000
16	20,922,789,888,000
17	3.55687428096E+14
18	6.402373705728E+15
19	1.2164510040883E+17
20	2.432902008176 6E+18

Crittografia per Trasposizione

Le lettere del messaggio sono mutate di posto generando un *anagramma.*

La trasposizione casuale del messaggio fornisce la massima inviolabilità... ma è inutilizzabile anche per il destinatario!

Per essere efficace la ricombinazione deve ubbidire ad un criterio fissato tra i corrispondenti ed ignoto (si spera!) al nemico.

Crittografia per Trasposizione

Uno dei metodi più antichi di trasposizione è detto *ad inferriata*:

```
UN SEGRETO È IL TUO PRIGIONIERO; SE LO LASCI ANDARE, SARAI IL SUO PRIGIONIERO

U S G E O I T O R G O I R S L L S I N A E A A I S O R G O I R
N E R T E L U P I I N E O E O A C A D R S R I L U P I I N E O

USGEOITORGOIRSLLSINAEAAISORGOIRNERTELUPIINEOEOACADRSRILUPIINEO
```

Varianti: invece che due linee se ne possono utilizzare tre; il passaggio da una linea ad un'altra avviene dopo due caratteri invece che dopo ogni singolo carattere, ecc.

Crittografia per Trasposizione

Uno dei metodi più antichi di trasposizione è detto *ad inferriata*:

Scitale: asticciola di legno attorno alla quale veniva arrotolata una striscia di pelle (poteva essere camuffata da cintura: steganografia) su cui il mittente aveva scritto il messaggio.

Crittografia per Sostituzione

Il primo esempio documentato di impiego militare di cifratura per sostituzione si trova nel *De Bello Gallico* di Giulio Cesare.

La cifratura comportava l'uso dei caratteri dell'alfabeto greco al posto di quelli latini.

Crittografia per Sostituzione

Il primo esempio documentato di impiego militare di cifratura per sostituzione si trova nel *De Bello Gallico* di Giulio Cesare.

La cifratura comportava l'uso dei caratteri dell'alfabeto greco al posto di quelli latini.

Cesare utilizzava un'altra scrittura segreta per sostituzione. Si tratta del semplice scambio di ogni lettera con quella tre posti più avanti nell'alfabeto.

Alfabeto chiaro:	`abcdefghilmnopqrstuvz`
Alfabeto cifrante:	`DEFGHILMNOPQRSTUVZABC`
Testo chiaro:	`veni vidi vici`
Testo cifrato:	`BHQN BNGN BNFN`

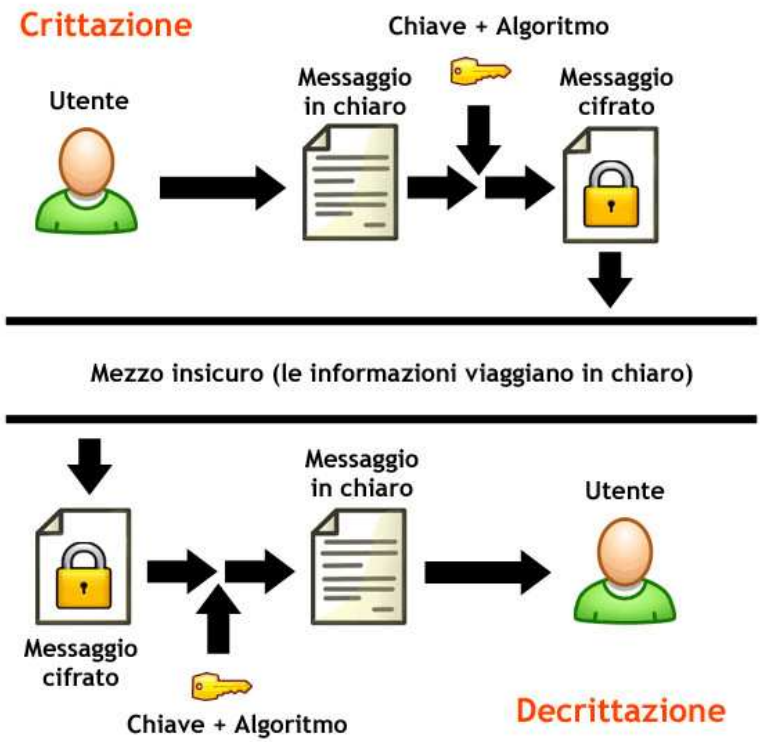
Crittografia per Sostituzione

Invece di usare uno spostamento di tre lettere possiamo utilizzare uno spostamento tra 1 e 20 lettere, ed avere quindi 20 diverse cifrature.
Se poi riorganizziamo l'alfabeto cifrante tramite trasposizione, possiamo ottenere $20 \times 21!$ (1000 miliardi di miliardi) diverse cifrature!

Algoritmo e Chiave

Qualsiasi scrittura segreta può essere analizzata in termini di *algoritmo* e di *chiave.*

Applicando insieme algoritmo e chiave ad un testo in chiaro questo è trasformato in un testo cifrato, o crittogramma.



Algoritmo e Chiave

La netta separazione concettuale tra algoritmo e chiave è uno dei principi della crittografia, e fu formulata nel 1883 da Kerckhoffs von Nieuwenhof nel trattato *"La Cryptographie Militaire":*

> *La sicurezza di un critto-sistema non deve dipendere dal tener celato il critto-algoritmo. La sicurezza dipenderà solo dal tener celata la chiave.*
>
> *Legge di Kerckhoffs*

Algoritmo e Chiave

Un buon sistema crittografico deve inoltre permettere di scegliere la chiave tra un numero molto grande di chiavi potenziali.

Ad esempio, utilizzando la cifratura di Cesare le chiavi sono solo 21. Ma se si utilizza l'algoritmo generale che ammette qualunque alfabeto cifrante, le chiavi possibili diventano 50 miliardi di miliardi:

Alfabeto chiaro:	`abcdefghilmnopqrstuvz`
Alfabeto cifrante:	`LPAIQBCTRZDSEGFHUONVM`
Testo chiaro:	`et tu brute`
Testo cifrato:	`QO ON PHNOQ`

Algoritmo e Chiave

Il pregio di questa cifratura consiste nel fatto che è semplice da eseguire ma garantisce un elevato grado di sicurezza.

Si può disporre di una chiave ancora più comoda se si utilizza una *frase chiave* per generare l'alfabeto cifrante. Se vogliamo usare **IULIUS CAESAR** come frase chiave, l'alfabeto cifrante diventa:

Alfabeto chiaro:	`abcdefghilmnopqrstuvz`
Alfabeto cifrante:	`IULSCAERTVZBDFGHMNOPQ`

Testo chiaro:	`et tu brute`
Testo cifrato:	`CN NO UHONC`

Il vantaggio è che bisogna memorizzare solo una frase e non una sequenza priva di senso.

Algoritmo e Chiave

Il pregio di questa cifratura consiste nel fatto che è semplice da eseguire ma garantisce un elevato grado di sicurezza.

Si può disporre di una chiave ancora più comoda se si utilizza una *frase chiave* per generare l'alfabeto cifrante. Se vogliamo usare **IULIUS CAESAR** come frase chiave, l'alfabeto cifrante diventa:

Alfabeto chiaro:	`abcdefghilmnopqrstuvz`
Alfabeto cifrante:	`IULSCAERTVZBDFGHMNOPQ`

Testo chiaro:	`et tu brute`
Testo cifrato:	`CN NO UHONC`

Se oltre alle lettere, l'alfabeto cifrante contiene anche simboli, la cifratura per sostituzione viene detta *monoalfabetica.*

Algoritmo e Chiave

Tecnicamente abbiamo che

codice sostituzione a livello di parole o frasi.
Codificare significa rendere un messaggio incomprensibile mettendolo in codice;
cifra sostituzione a livello di lettere.
Cifrare significa rendere un messaggio incomprensibile mettendolo in cifra.

I verbi *crittare* e *decrittare* sono invece più generali, dato che indicano l'operazione di rendere oscuro e chiaro un messaggio indipendentemente dal fatto che che sia stato cifrato o codificato.

Sostituzione Polialfabetica

Tra il 1460 e 1470 Leon Battista Alberti propose di usare due o più alfabeti cifranti:

Alfabeto chiaro:	`abcdefghilmnopqrstuvz`
Alfabeto cifrante I:	`EUFAVODNPHSGTMILBRZCQ`
Alfabeto cifrante II:	`CMUNBIPLOVATGSDRHQFZE`

Se volessimo cifrare la parola **LEONE** usando il primo alfabeto cifrante per la prima, terza e quinta lettera, ed il secondo alfabeto cifrante per la seconda e quarta lettera, otterremmo:

LEONE $\Rightarrow$ HBTTV

L'idea di Alberti venne sviluppata da Blaise de Vigenère (1523–1596)

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Sostituzione Polialfabetica

Supponiamo di voler cifrare il messaggio

“incontriamoci alla specola alle sedici”

adoperando la chiave **CONFERENZASPECOLA**.

Sostituzione Polialfabetica

Supponiamo di voler cifrare il messaggio

“incontriamoci alla specola alle sedici”

adoperando la chiave **CONFERENZASPECOLA**.

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 1 (i)
L	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	L
M	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	M
N	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	N
O	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	O
P	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	P
Q	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	Q
R	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	R
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	S
T	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	T
U	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	U
V	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	V
W	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	W
X	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	X
Y	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	Y
Z	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	Z

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `K`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 1 (i)
L	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	L
M	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	M
N	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	N
O	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	O
P	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	P
Q	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	Q
R	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	R
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	S
T	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	T
U	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	U
V	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	V
W	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	W
X	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	X
Y	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	Y
Z	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	Z

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KB`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 1 (i)
L	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	L
M	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	M
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R
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	S
T	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	T
U	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	U
V	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	V
W	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	W
X	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	X
Y	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	Y
Z	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	Z

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBP`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 1 (i)
L	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	L
M	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	M
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R
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	S
T	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	T 1 (o)
U	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	U
V	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	V
W	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	W
X	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	X
Y	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	Y
Z	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	Z

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPT`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 1 (i)
L	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	L
M	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	M
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 1 (n)
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	S
T	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	T 1 (o)
U	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	U
V	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	V
W	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	W
X	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	X
Y	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	Y
Z	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	Z

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTR`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 1 (i)
L	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	L
M	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	M
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 1 (n)
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	S
T	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	T 1 (o)
U	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	U
V	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	V
W	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	W
X	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	X
Y	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	Y
Z	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	Z

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRK`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 1 (n)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 1 (r)
W	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	W
X	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	X
Y	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	Y
Z	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	Z

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKV`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 1 (n)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 2 (ri)
W	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	W
X	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	X
Y	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	Y
Z	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	Z

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVV`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 1 (n)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 2 (ri)
W	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	W
X	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	X
Y	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	Y
Z	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	Z 1 (a)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZ`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 1 (m)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 1 (n)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 2 (ri)
W	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	W
X	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	X
Y	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	Y
Z	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	Z 1 (a)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZM`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 1 (m)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 1 (n)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 2 (ri)
W	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	W
X	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	X
Y	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	Y
Z	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	Z 1 (a)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMG`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 1 (m)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 2 (nc)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 2 (ri)
W	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	W
X	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	X
Y	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	Y
Z	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	Z 1 (a)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGR`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C
D	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	D
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 2 (nc)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 2 (ri)
W	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	W
X	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	X
Y	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	Y
Z	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	Z 1 (a)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRM`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C 1 (a)
D	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	D
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 2 (nc)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 2 (ri)
W	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	W
X	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	X
Y	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	Y
Z	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	Z 1 (a)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMC`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C 1 (a)
D	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	D
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 2 (nc)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 2 (ri)
W	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	W
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZ`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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
B	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	B 1 (n)
C	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	C 1 (a)
D	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	D
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 2 (nc)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZW`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 1 (a)
D	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	D
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 2 (nc)
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	S
T	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	T 1 (o)
U	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	U
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWA`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 1 (a)
D	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	D
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 2 (nc)
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	S
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAU`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 1 (a)
D	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	D
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 2 (nc)
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	S
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUD`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 1 (a)
D	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	D 1 (p)
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDR`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 1 (a)
D	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	D 1 (p)
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H 1 (c)
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRH`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 1 (a)
D	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	D 1 (p)
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H 1 (c)
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHS`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 1 (a)
D	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	D 1 (p)
E	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	E
F	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	F
G	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	G 1 (o)
H	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	H 1 (c)
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSC`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F
G	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	G 1 (o)
H	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	H 1 (c)
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCE`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F
G	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	G 1 (o)
H	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	H 1 (c)
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N 1 (a)
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCEN`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F
G	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	G 1 (o)
H	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	H 1 (c)
I	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	I
J	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	J
K	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	K 2 (it)
L	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	L
M	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	M 2 (mi)
N	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	N 1 (a)
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCENK`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F
G	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	G 1 (o)
H	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	H 1 (c)
I	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	I
J	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	J
K	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	K 3 (itl)
L	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	L 1 (l)
M	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	M 2 (mi)
N	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	N 1 (a)
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 1 (l)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCENKL`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F
G	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	G 1 (o)
H	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	H 1 (c)
I	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	I
J	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	J
K	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	K 3 (itl)
L	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	L 1 (l)
M	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	M 2 (mi)
N	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	N 1 (a)
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 2 (le)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCENKLW`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F
G	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	G 1 (o)
H	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	H 1 (c)
I	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	I
J	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	J
K	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	K 3 (itl)
L	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	L 1 (l)
M	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	M 2 (mi)
N	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	N 1 (a)
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 2 (le)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCENKLWH`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F
G	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	G 1 (o)
H	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	H 2 (cs)
I	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	I 1 (e)
J	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	J
K	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	K 3 (itl)
L	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	L 1 (l)
M	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	M 2 (mi)
N	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	N 1 (a)
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 2 (le)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCENKLWHI`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F 1 (d)
G	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	G 1 (o)
H	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	H 2 (cs)
I	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	I 1 (e)
J	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	J
K	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	K 3 (itl)
L	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	L 1 (l)
M	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	M 2 (mi)
N	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	N 1 (a)
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 2 (le)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCENKLWHIF`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F 1 (d)
G	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	G 1 (o)
H	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	H 2 (cs)
I	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	I 1 (e)
J	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	J
K	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	K 3 (itl)
L	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	L 1 (l)
M	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	M 2 (mi)
N	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	N 1 (a)
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 3 (lei)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCENKLWHIFW`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F 1 (d)
G	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	G 1 (o)
H	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	H 2 (cs)
I	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	I 1 (e)
J	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	J
K	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	K 3 (itl)
L	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	L 1 (l)
M	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	M 2 (mi)
N	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	N 2 (ac)
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 3 (lei)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCENKLWHIFWN`

Sostituzione Polialfabetica

	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	*Analisi Frq.*
A	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 1 (a)
B	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	B 1 (n)
C	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	C 2 (al)
D	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	D 1 (p)
E	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	E 1 (a)
F	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	F 1 (d)
G	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	G 1 (o)
H	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	H 2 (cs)
I	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	I 2 (ei)
J	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	J
K	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	K 3 (itl)
L	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	L 1 (l)
M	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	M 2 (mi)
N	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	N 2 (ac)
O	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	O
P	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	P 1 (c)
Q	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	Q
R	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	R 3 (nce)
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	S 1 (o)
T	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	T 1 (o)
U	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	U 1 (s)
V	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	V 2 (ri)
W	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	W 3 (lei)
X	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	X
Y	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	Y
Z	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	Z 2 (al)

Parola chiave: `CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro: `incontriamociallaspecolaallesedici`
Testo cifrato: `KBPTRKVVZMGRMCZWAUDRHSCENKLWHIFWNI`

Sostituzione Polialfabetica

Supponiamo di voler cifrare il messaggio

“incontriamoci alla specola alle sedici”

adoperando la chiave **CONFERENZASPECOLA**.

Parola chiave:	`CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro:	`incontriamociallaspecolaallesedici`
Testo cifrato:	`KBPTRKVVZMGRMCZWAUDRHSCENKLWHIFWNI`

Analisi delle frequenze: i simboli **K**, **R** e **W** che appaiono con maggiore frequenza, dovrebbero corrispondere ad una vocale. **K** e **R** cifrano una vocale e due consonanti, **W** due vocali e una consonante.

Inoltre la doppia **l** viene rappresentata da **ZW** e la doppia **e** da **EN**.

Sostituzione Polialfabetica

Supponiamo di voler cifrare il messaggio

“incontriamoci alla specola alle sedici”

adoperando la chiave **CONFERENZASPECOLA**.

Parola chiave:	`CONFERENZASPECOLACONFERENZASPECOLA`
Testo chiaro:	`incontriamociallaspecolaallesedici`
Testo cifrato:	`KBPTRKVVZMGRMCZWAUDRHSCENKLWHIFWNI`

Analisi delle frequenze: i simboli **K**, **R** e **W** che appaiono con maggiore frequenza, dovrebbero corrispondere ad una vocale. **K** e **R** cifrano una vocale e due consonanti, **W** due vocali e una consonante.

Inoltre la doppia **l** viene rappresentata da **ZW** e la doppia **e** da **EN**.

La cifratura di Vigenère ammette un numero enorme di chiavi.

Sostituzione Polialfabetica

Con l'avvento del telegrafo ci si accorse che bisognava cifrare il messaggio *prima* di inviarlo. La cifratura polialfabetica di Vigenère fu considerata la più adatta allo scopo.

Sostituzione Polialfabetica

Con l'avvento del telegrafo ci si accorse che bisognava cifrare il messaggio *prima* di inviarlo. La cifratura polialfabetica di Vigenère fu considerata la più adatta allo scopo.

Fu Charles Babbage (1791–1871) a trovare il punto debole della cifratura di Vigenère: la lunghezza della chiave determina il ciclo di ripetizioni delle cifre.

Sostituzione Polialfabetica

Con l'avvento del telegrafo ci si accorse che bisognava cifrare il messaggio *prima* di inviarlo. La cifratura polialfabetica di Vigenère fu considerata la più adatta allo scopo.

Fu Charles Babbage (1791–1871) a trovare il punto debole della cifratura di Vigenère: la lunghezza della chiave determina il ciclo di ripetizioni delle cifre.

Per esempio, se la chiave è **SOLE**, ogni lettera del testo chiaro può essere cifrata in quattro modi diversi. Se la parola **non** compare più volte nel messaggio originale, è molto probabile che una delle versioni di **non** compaia più di una volta. Se poi nel messaggio ci sono più di quattro **non**, almeno una ripetizione è inevitabile.

Sostituzione Polialfabetica

Con l'avvento del telegrafo ci si accorse che bisognava cifrare il messaggio *prima* di inviarlo. La cifratura polialfabetica di Vigenère fu considerata la più adatta allo scopo.

Fu Charles Babbage (1791–1871) a trovare il punto debole della cifratura di Vigenère: la lunghezza della chiave determina il ciclo di ripetizioni delle cifre.

Parola chiave:	`SOLESOLESOLESOLESOLESOL`
Testo chiaro:	`nonvedononsentononparlo`
Testo cifrato:	`FCYZWRZRGBDIFHZRGBAEJZZ`

Sostituzione Polialfabetica

Con l'avvento del telegrafo ci si accorse che bisognava cifrare il messaggio *prima* di inviarlo. La cifratura polialfabetica di Vigenère fu considerata la più adatta allo scopo.

Fu Charles Babbage (1791–1871) a trovare il punto debole della cifratura di Vigenère: la lunghezza della chiave determina il ciclo di ripetizioni delle cifre.

Parola chiave:	SOLESOLESOLESOLESOLESOL
Testo chiaro:	nonvedononsentononparlo
Testo cifrato:	**FCY**ZWRZ**RGB**DIFHZ**RGB**AEJZZ

Sostituzione Polialfabetica

Con l'avvento del telegrafo ci si accorse che bisognava cifrare il messaggio *prima* di inviarlo. La cifratura polialfabetica di Vigenère fu considerata la più adatta allo scopo.

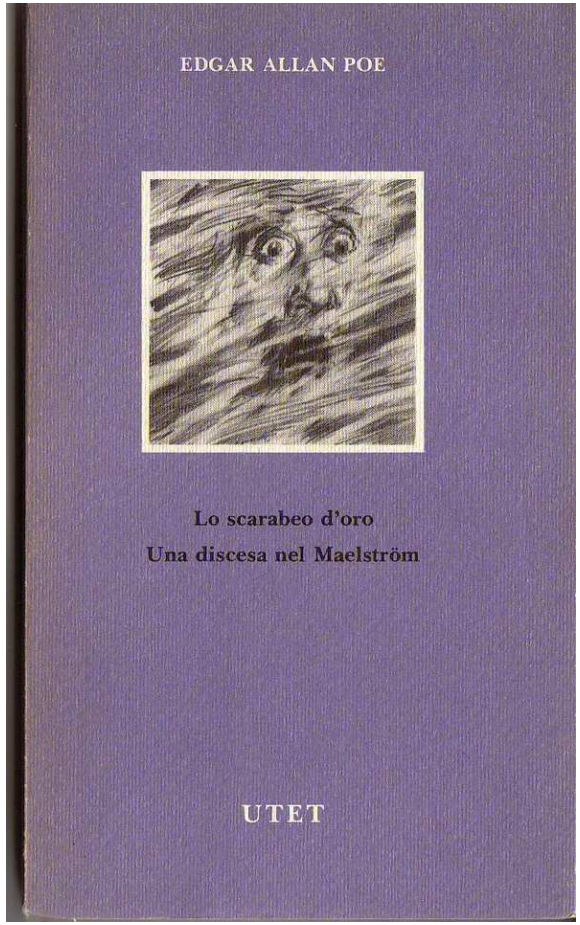
Fu Charles Babbage (1791–1871) a trovare il punto debole della cifratura di Vigenère: la lunghezza della chiave determina il ciclo di ripetizioni delle cifre.

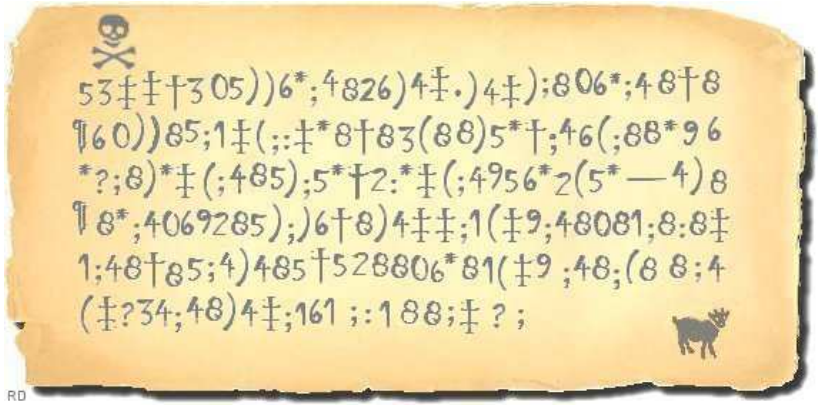
Parola chiave:	SOLESOLESOLESOLESOLESOL
Testo chiaro:	nonvedononsentononparlo
Testo cifrato:	**FCY**ZWRZ**RGB**DIFHZ**RGB**AEJZZ

Purtroppo Babbage non pubblicò il suo risultato, che fu riscoperto in modo indipendente da un ufficiale in pensione dell'esercito prussiano: Friedrich Wilhelm Kasiski (1805–1881).

Sostituzione Polialfabetica

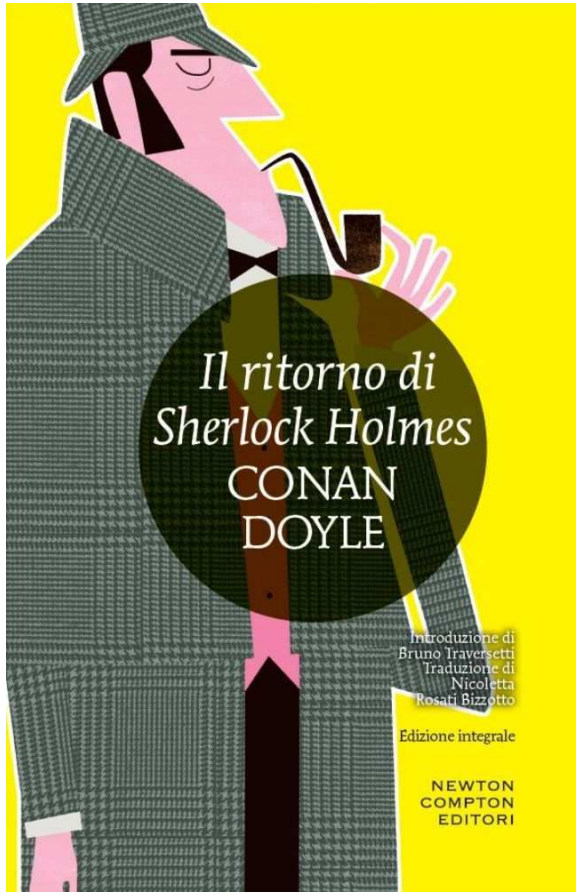
A causa del suo uso per le trasmissioni commerciali via telegrafo, la crittografia divenne un argomento molto popolare:





Sostituzione Polialfabetica

A causa del suo uso per le trasmissioni commerciali via telegrafo, la crittografia divenne un argomento molto popolare:



Crittografia Asimmetrica

I cifrari tradizionali sono tutti caratterizzati da una **chiave segreta**; mittente e destinatario devono preventivamente concordare una qualche chiave.

Crittografia Asimmetrica

I cifrari tradizionali sono tutti caratterizzati da una **chiave segreta**; mittente e destinatario devono preventivamente concordare una qualche chiave.

Questa necessità di comunicarsi la chiave segreta è un grosso punto debole: o ci si vede di persona e in luogo riservato, o si deve usare un canale di comunicazione assolutamente sicuro.

Crittografia Asimmetrica

I cifrari tradizionali sono tutti caratterizzati da una **chiave segreta**; mittente e destinatario devono preventivamente concordare una qualche chiave.

Questa necessità di comunicarsi la chiave segreta è un grosso punto debole: o ci si vede di persona e in luogo riservato, o si deve usare un canale di comunicazione assolutamente sicuro.

Questi cifrari sono detti ***simmetrici:*** infatti cifratura e decifratura fanno uso della stessa chiave.

Crittografia Asimmetrica

Nel 1976 Whitfield Diffie and Martin Hellman proposero i cosiddetti *cifrari a chiave pubblica.*

Crittografia Asimmetrica

Nel 1976 Whitfield Diffie and Martin Hellman proposero i cosiddetti *cifrari a chiave pubblica.*

La rivoluzione: **la chiave per cifrare non è la stessa di quella per decifrare**;

Crittografia Asimmetrica

Nel 1976 Whitfield Diffie and Martin Hellman proposero i cosiddetti *cifrari a chiave pubblica.*

La rivoluzione: **la chiave per cifrare non è la stessa di quella per decifrare**;

la prima può allora essere resa pubblica mentre solo la seconda resta segreta. Per questo motivo sono detti anche cifrari ***asimmetrici.***

Crittografia Asimmetrica

Nel 1976 Whitfield Diffie and Martin Hellman proposero i cosiddetti *cifrari a chiave pubblica.*

La rivoluzione: **la chiave per cifrare non è la stessa di quella per decifrare**;

la prima può allora essere resa pubblica mentre solo la seconda resta segreta. Per questo motivo sono detti anche cifrari ***asimmetrici.***

La sicurezza di questi sistemi si fonda quasi sempre su funzioni relativamente facili da calcolare ma molto difficili da invertire (cosiddette *one-way functions*):

- ❏ calcolo del logaritmo discreto (DH);
- ❏ fattorizzazione di un intero (RSA);
- ❏ utilizzo delle curve ellittiche (ECC).

Crittografia Asimmetrica

2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)

On One-way Functions and Kolmogorov Complexity

Yanyi Liu
Cornell University
yl2866@cornell.edu

Rafael Pass
Cornell Tech
rafael@cs.cornell.edu

***Abstract*—We prove that the equivalence of two fundamental problems in the theory of computing. For every polynomial $t(n) \geq (1+\varepsilon)n$, $\varepsilon > 0$, the following are equivalent:**

- **One-way functions exists (which in turn is equivalent to the existence of secure private-key encryption schemes, digital signatures, pseudorandom generators, pseudorandom functions, commitment schemes, and more);**
- **t-time bounded Kolmogorov Complexity, K^t, is mildly hard-on-average (i.e., there exists a polynomial $p(n) > 0$ such that no PPT algorithm can compute K^t, for more than a $1 - \frac{1}{p(n)}$ fraction of n-bit strings).**

In doing so, we present the first natural, and well-studied, computational problem characterizing the feasibility of the central private-key primitives and protocols in Cryptography.

I. Introduction

We prove the equivalence of two fundamental problems in the theory of computing: (a) the existence of one-way functions, and (b) mild average-case hardness of the time-bounded Kolmogorov Complexity problem.

Existence of One-way Functions: A *one-way function* [13] (OWF) is a function f that can be efficiently computed (in polynomial time), yet no probabilistic polynomial-time (PPT) algorithm can invert f with

While many candidate constructions of OWFs are known—most notably based on factoring [42], the discrete logarithm problem [13], or the hardness of lattice problems [1]—the question of whether there exists some *natural* average-case hard problem that characterizes the hardness of OWFs (and thus the feasibility of the above central cryptographic primitives) has been a long-standing open problem:[1]

> *Does there exists some* natural *average-case hard computational problem (i.e., both the computational problem and the distribution over instances is "natural"), which characterizes the existence of one-way functions?*

This problem is particularly pressing given recent advances in quantum computing [7] and the fact that many classic OWF candidates (e.g., based on factoring and discrete log) can be broken by a quantum computer [45].

Average-case Hardness of K^{poly}-Complexity: What makes the string 12121212121212121 less random than 60484850668340357492? The notion of *Kolmogorov complexity* (K-complexity), introduced by Solomonoff [48], Kolmogorov [34] and Chaitin [12], provides an elegant method for measuring the amount of "randomness" in individual strings: The K-complexity of a string is the length of the shortest program (to be run on some

https://arxiv.org/abs/2009.11514

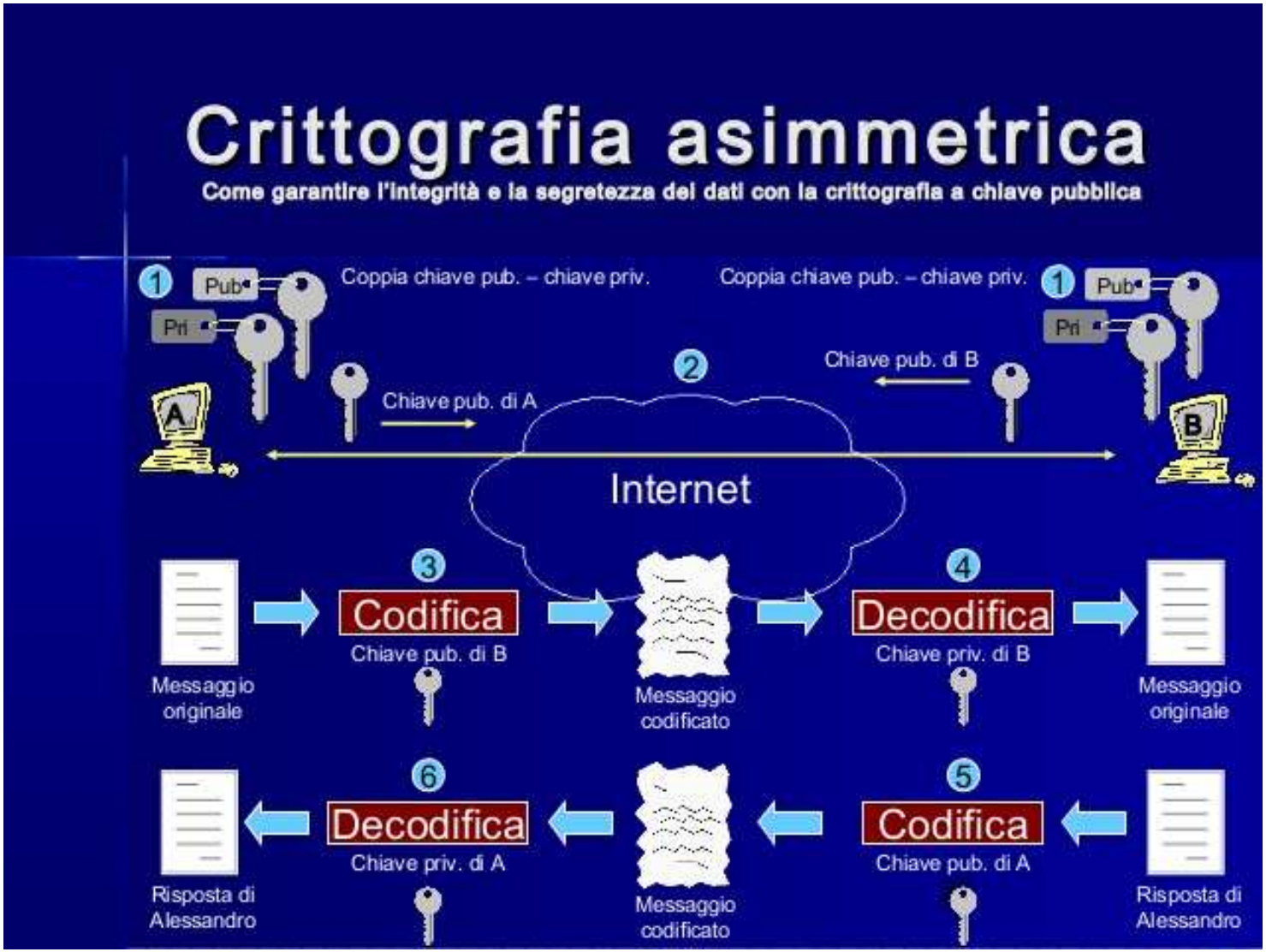
Kolmogorov Complexity

One measure of randomness is based on how easy it is to describe a string of numbers. The simpler the program that can output the string, the lower the Kolmogorov complexity of the string.

STRING	PROGRAM	COMPLEXITY
135791113151719 2123252729313 33537394143	Print: The first 22 odd numbers	Less
99999999931415 9265358979323 846264338327	Print: Nine 9s then the first 30 digits of pi	
3238226618594 07670964010280 409881234079	Print: 323822 6618594076709 6401028040988 1234079	More

https://www.quantamagazine.org/researchers-identify-master-problem-underlying-all-cryptography-20220406/

Crittografia Asimmetrica



Crittografia Asimmetrica

Tre matematici Ron Rivest, Adi Shamir e Leonard Adleman sfruttarono per la cifratura asimmetrica scoperta da Diffie e Hellman la difficoltà di fattorizzare un numero; la chiave pubblica è un numero N ottenuto moltiplicando due numeri primi molto grandi (centinaia di cifre decimali) che restano segreti.

Il sistema si basa su due risultati matematici dovuti a Fermat e a Eulero.

Crittografia Asimmetrica

Tre matematici Ron Rivest, Adi Shamir e Leonard Adleman sfruttarono per la cifratura asimmetrica scoperta da Diffie e Hellman la difficoltà di fattorizzare un numero; la chiave pubblica è un numero N ottenuto moltiplicando due numeri primi molto grandi (centinaia di cifre decimali) che restano segreti.

Il sistema si basa su due risultati matematici dovuti a Fermat e a Eulero.

RSA rimase per qualche anno nel limbo delle belle idee, ma poi con la sempre maggiore diffusione di Internet ha conosciuto un successo enorme, ed è ancor oggi il cifrario a chiave pubblica più usato. Quasi tutte le operazioni sicure sul web (protocollo https) usano oggi certificati basati su RSA.

Crittografia Asimmetrica

Crittografia Asimmetrica

Tre matematici Ron Rivest, Adi Shamir e Leonard Adleman sfruttarono per la cifratura asimmetrica scoperta da Diffie e Hellman la difficoltà di fattorizzare un numero; la chiave pubblica è un numero N ottenuto moltiplicando due numeri primi molto grandi (centinaia di cifre decimali) che restano segreti.

Il sistema si basa su due risultati matematici dovuti a Fermat e a Eulero.

La lunghezza delle chiavi deve essere tale che non venga forzata da attacchi a *forza bruta.*

Tempo di Protezione	fino 2010	fino 2030	dal 2031
Dimensione minima chiave simmetrica	80 bits	112 bits	128 bits
Dimensione minima chiave RSA	1024 bits	2048 bits	3072 bits

Crittografia Asimmetrica

Tre matematici Ron Rivest, Adi Shamir e Leonard Adleman sfruttarono per la cifratura asimmetrica scoperta da Diffie e Hellman la difficoltà di fattorizzare un numero; la chiave pubblica è un numero N ottenuto moltiplicando due numeri primi molto grandi (centinaia di cifre decimali) che restano segreti.

Il sistema si basa su due risultati matematici dovuti a Fermat e a Eulero.

Nel 1994 Peter Shor ha sviluppato un **algoritmo quantico** in grado di calcolare la fattorizzazione in tempi ragionevoli. Quindi l'avvento dei *calcolatori quantistici* potrebbe richiedere l'uso di chiavi RSA sempre più grandi, dell'ordine dei tera-bytes. Il processo di crittazione/decrittazione richiederebbe almeno 5 giorni!

Crittografia Asimmetrica


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (GNU/Linux)

mQGiBEjiB6IRBACsyXIxneEDxx/azYDUBKQGqyiSN+W8IxxLwTl98DXAOMw1oWJO
Xt9BCXYKR6RqvbCO09H34/WaO/z8MSOJa1sEldnoXX18dAeVjJ/QNTZVArsoM1I9
qOuoOVOC/B7JUKmrr11+kdicdyn8WhIVjcOqv4+dXcwlQx/AE5P+tPYQOwCg17uy
T9RJE3yspSgSAv5PsY2T3rkD/3Q1SZEsDD1bYMxFxMw77qyTMXSCKQ/skNcoUv+X
AE8DuUZK+BkoG39h5AI2qVVDtGKuOVmDJSUcGlO9sVfDWpoaMU+2+KkbvTVlw82W
eQUJjdbboDTjTxF3v4XxdtR4wNR2++JCyIkiOkgQBzTYjjheiDxHMZzQ9CuZqvfn
KdDCBACpHCpbDVFkrrW+u0Q3BTI8EJOaKrDJBdNiMvTxsH2i/SGriszSl+ywrMYF
c3lqWN/XCQW1LT41R7f+6oIwe7rAZ2x9XmOEmgkI/4818GxdF2GUQNHISqWjabZn
Z1Khd2qn2qSrXsbb4eW2z/9LGS86NEzh6LclBYeIzGlVUdCxbLQxTWF1cm8gT3Js
YW5kaW5pICHvcm1hKSA8b3JsYW5kaW5pQGlhc2Ziby5pbmFmLml0PohgBBMRAgAg
BQJI4geiAhsDBgsJCAcDAgQVAggDBBYCAwECHgECF4AACgkQD4utKwyP2ndAcwCg
kolnQt0bAnj6ei14TobFSKwFtf4An1R8A7HCjz8m0uq+/QPZEU8E7tyquQINBEji
B6IQCACwyh+ek56sXZp5OZPnfQkchTe/9EWJiRu3nb57NM5kqzGtbTqJ4A6hA99y
xa3jK3s3U7qImAKHhP07dZJaeV57R+Wsmoql5Va8ZyiA13R2zUDs9a63sqoVBx+2
UF6Ts/UtDlitdlMWNezVzS94tOJcQSCs9YWGkSquvtL+7aFdlnsxregqMfkVc+hj
Ugyl1CmY9cak5I3zJZZATV6P01oE4oKjqWae3MHep5jzutqNk/02Jrx46LE5wh7X
Xy6pbDXQtmcsJ0DWz2fxwum1kQL/t6Pz0+MTkxaK9FvqA9QoiKPhMW2l+zNygM0o
sjSpQ7C2miV+PSHyzXNzY9LwXG0nAAMFCACONxq1I4TJJVzOgqGZMKg8hOfyF0ln
bEjtsiSsKfoQCvo7pw7KfQl7dYGNg3Pc4qA2L2LJVEl7CMEp4O8QQpTMCw7tUUQ4
TW16uz1Z35mKalm5MZHNIB4xZpYOUGLHK3Bn92unqmmS2c2mlR7vtmczwFo+V85P
Dkr+UIKcytEDTpUG4RwDR8JJzbIgLr8Ax60RY2gTCkxeOqBzPlpIWCQQh+uHabYf
S0/CgRxyNKciPdLNqj3iUd6MFUN8cF5Mpitue6TgmjVidbFqo59tq87Zrpz5FDHV
YwcMYD4G/0T0j2mDfGs4SyndPcnfx76B0hUOWSLJfcxoVkPkjLKbFOQKiEkEGBEC
AAkFAkjiB6ICGwwACgkQD4utKwyP2ndeaQCggO+Qs6xTP5oSxBHMKYFntIDkw60A
oJP4tEVR6NE8fY5IDpuMZbhSI5Pa
=Plmn
-----END PGP PUBLIC KEY BLOCK-----
```

Vediamo come funziona la cifratura RSA:

1. Alice sceglie due numeri primi distinti p e q. $\rightarrow$ $p = 5; q = 11$
2. Calcola $N = p \times q$ $\rightarrow$ $N = 5 \times 11 = 55$
3. Calcola $b = (p-1) \times (q-1)$ $\rightarrow$ $b = 4 \times 10 = 40$
4. Calcola il primo intero e che sia primo con b. $\rightarrow$ $e = 3$
5. Calcola d tale che $e \times d (\text{mod } b) = 1$. $\rightarrow$ $d = 27$

Chiave pubblica:	(N, e)	**Cifratura:**	$c = m^e (\text{mod } N)$
Chiave privata:	(p, q, d)	**Decifratura:**	$m = c^d (\text{mod } N)$

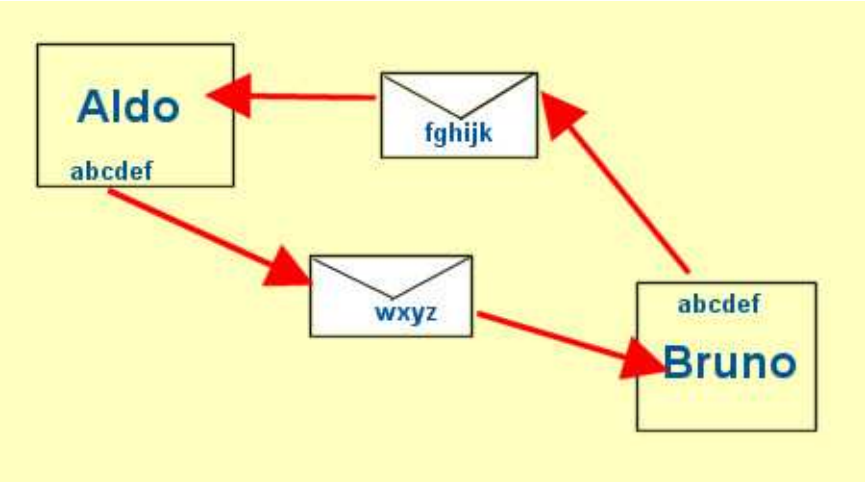
Bob cifra il numero 7 con la chiave pubblica di Alice e glielo invia:

$7 \rightarrow \quad 7^3 (\text{mod } 55) = 343 (\text{mod } 55) = 13$

Alice riceve da Bob il numero 13 e lo decifra con la sua chiave privata:

$13 \rightarrow \quad (13)^{27} (\text{mod } 55) = 7$

La firma digitale



Serve per autenticare un messaggio o un documento, cioè essere certi del mittente.

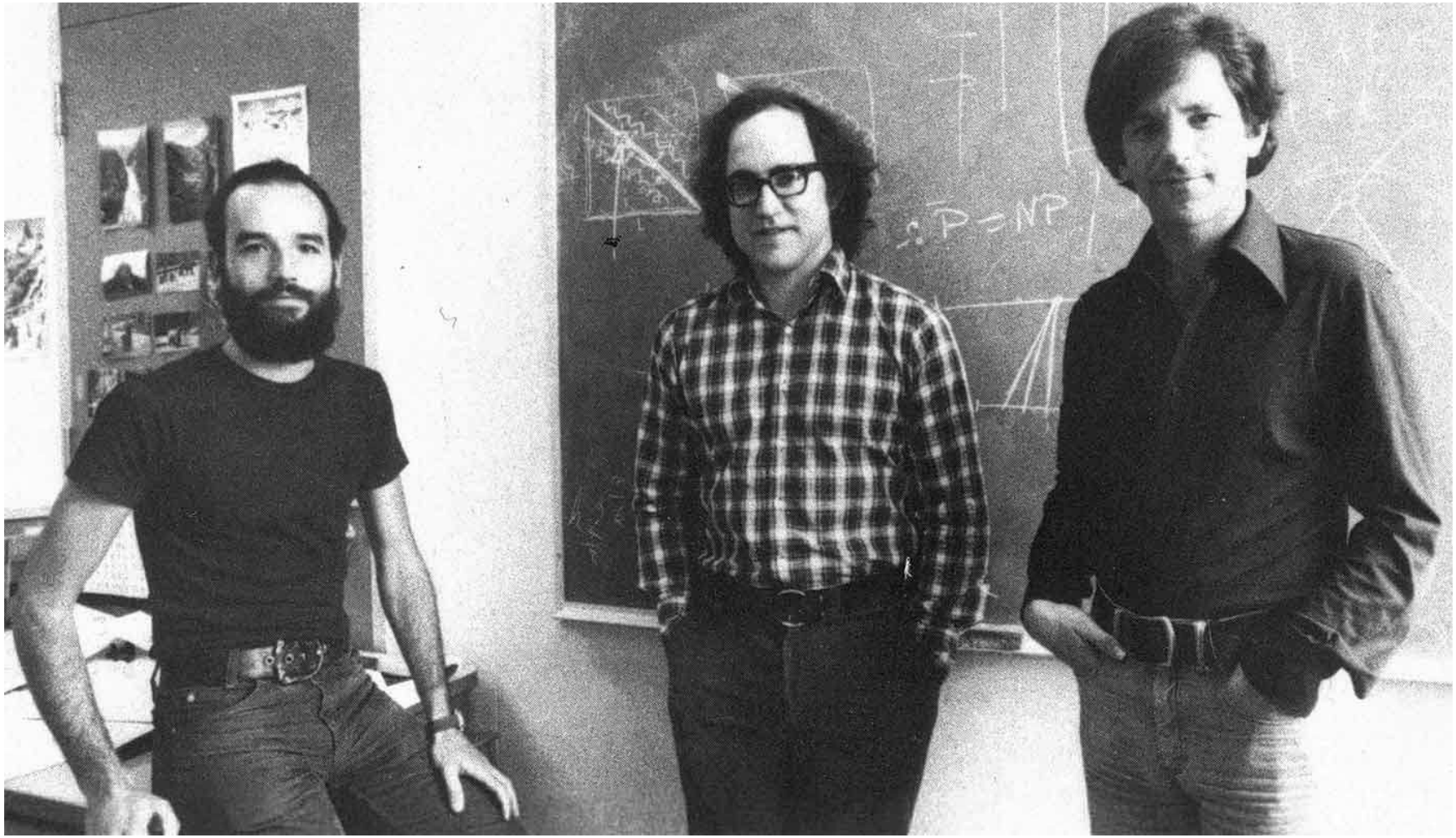
Aldo invia a Bruno una parola qualsiasi cifrata con la chiave pubblica di Bruno. Bruno la decifra usando la sua chiave segreta e la rispedisce ad Aldo cifrandola con la chiave pubblica di Aldo; Aldo la decifra usando la chiave pubblica di Bruno; se la parola decifrata è identica a quella inviata, Aldo è sicuro che il messaggio viene da Bruno.

Questo meccanismo ha il solo limite di non essere riutilizzabile, e quindi la firma digitale va rigenerata ad ogni nuovo messaggio.

Crittografia Asimmetrica

Ralph Merkle, Martin Hellman e Bailey Whitfield 'Whit' Diffie (1976)

Crittografia Asimmetrica

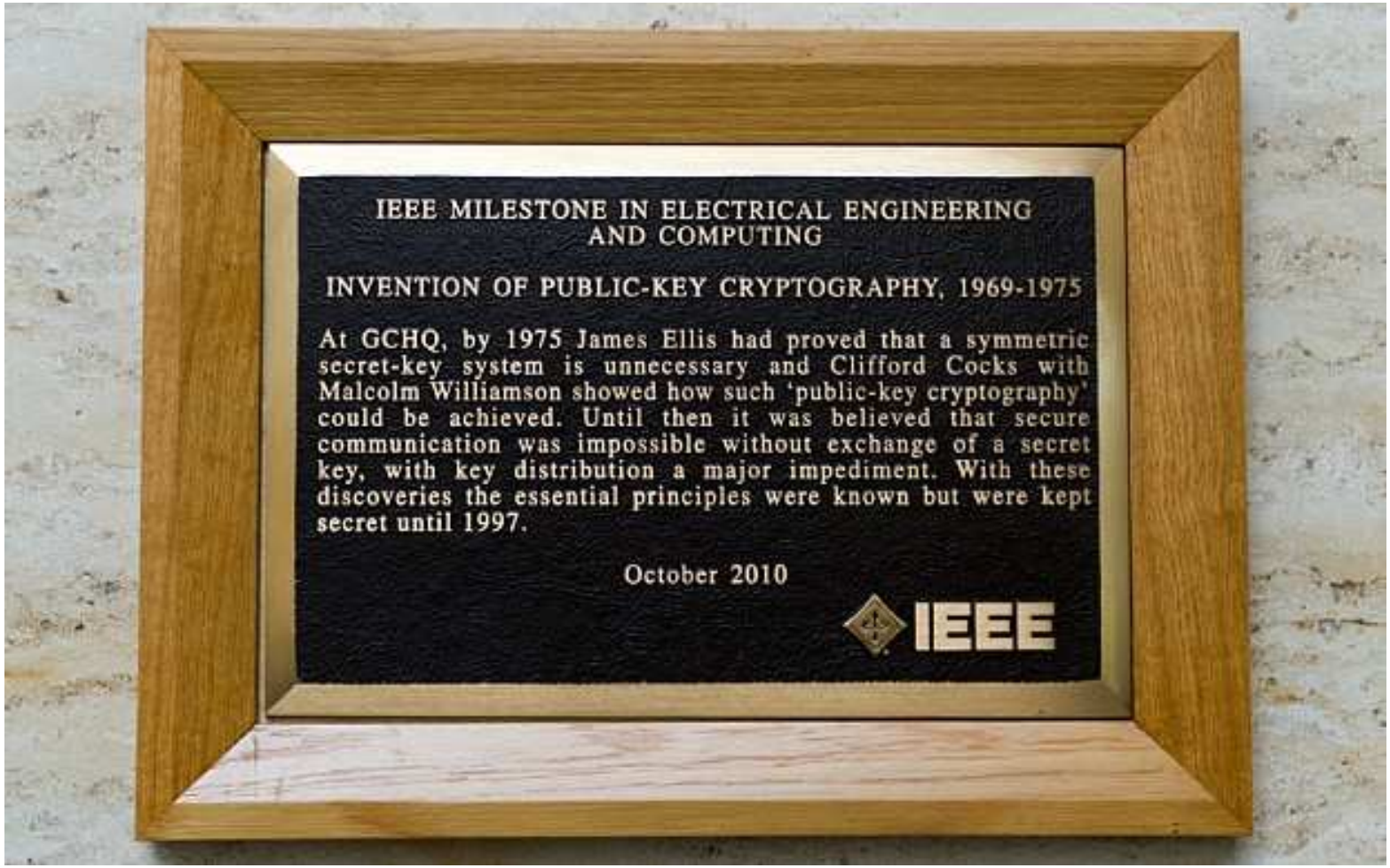


Ron Rivest, Adi Shamir e Leonard Adleman (1977)

Crittografia Asimmetrica

James Ellis, che formulò l'idea della crittografia asimmetrica 10 anni prima di Diffie e Hellman.

Crittografia Asimmetrica



La targa al Government Communications Headquarters (GCHQ) in cui viene dato credito dell'invenzione della crittografia asimmetrica a Ellis.

Crittografia Asimmetrica

Le scoperte nel campo della crittografia non sempre vengono divulgate!

Gli algoritmi di crittazione si basano sulla *difficoltà* della invertibilità di alcune funzioni, ma non esistono teoremi che *dimostrino* l'impossibilità di invertibilità.

Ad esempio, i calcolatori di prossima generazione (quantistici) potrebbero essere in grado di fattorizzare numeri molto grandi in tempi ragionevoli, in pratica rendendo inservibile la crittazione RSA.

Crittografia Asimmetrica

"Molte applicazioni di messaggistica criptano i messaggi solo tra te e loro, mentre la crittografia end-to-end di WhatsApp assicura che solo tu e la persona con cui stai comunicando possiate leggere ciò che viene inviato, e che non ci sia nessuno nel mezzo, nemmeno WhatsApp."

Il Cifrario Inattaccabile

Esiste un cifrario che sia stato *dimostrato* matematicamente essere inattaccabile?

Il Cifrario Inattaccabile

Esiste un cifrario che sia stato *dimostrato* matematicamente essere inattaccabile? La risposta è **SÌ**!!!

Il Cifrario Inattaccabile

Esiste un cifrario che sia stato *dimostrato* matematicamente essere inattaccabile? La risposta è **SÌ**!!!

Shannon ha dimostrato che un cifrario di Vigenère con una chiave lunga quanto il messaggio e formata da una stringa casuale genera a sua volta una stringa casuale.

Questo tipo di cifrario viene detto *cifrario di Vernam*, dal nome del suo ideatore, Gilbert Vernam, che lo brevettò nel 1919 (anche se era stato già discusso nel 1882 da Frank Miller).

Il Cifrario Inattaccabile

Il messaggio in chiaro e la chiave vengono “sommati” proprio come nel cifrario di Vigenère.

Supponiamo che Alice voglia mandare a Bob il messaggio “HELLO”. I due si metteranno d’accordo sulla chiave, che sarà “XMCKL”. Per semplicità associeremo un numero ad ogni lettera.

Alice → Bob:

```
      H        E        L        L        O     messaggio
-------------------------------------------------------------
      7 (H)    4 (E)   11 (L)   11 (L)   14 (O) messaggio
  + 23 (X)   12 (M)    2 (C)   10 (K)   11 (L) chiave
  = 30       16       13       21       25     messaggio + chiave
  =  4 (E)   16 (Q)   13 (N)   21 (V)   25 (Z) (messaggio + chiave) mod 26
-------------------------------------------------------------
      E        Q        N        V        Z     testo cifrato
```

Il Cifrario Inattaccabile

Il messaggio in chiaro e la chiave vengono “sommati” proprio come nel cifrario di Vigenère.

Supponiamo che Alice voglia mandare a Bob il messaggio “HELLO”. I due si metteranno d’accordo sulla chiave, che sarà “XMCKL”. Per semplicità associeremo un numero ad ogni lettera.

Bob → Alice:

```
     E       Q       N       V       Z     testo cifrato
-------------------------------------------------------
     4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) testo cifrato
  -  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) chiave
  = -19       4      11      11      14     testo cifrato - chiave
  =   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) testo cifrato - chiave (mod 26)
-------------------------------------------------------
     H       E       L       L       O     messaggio
```

Il Cifrario Inattaccabile

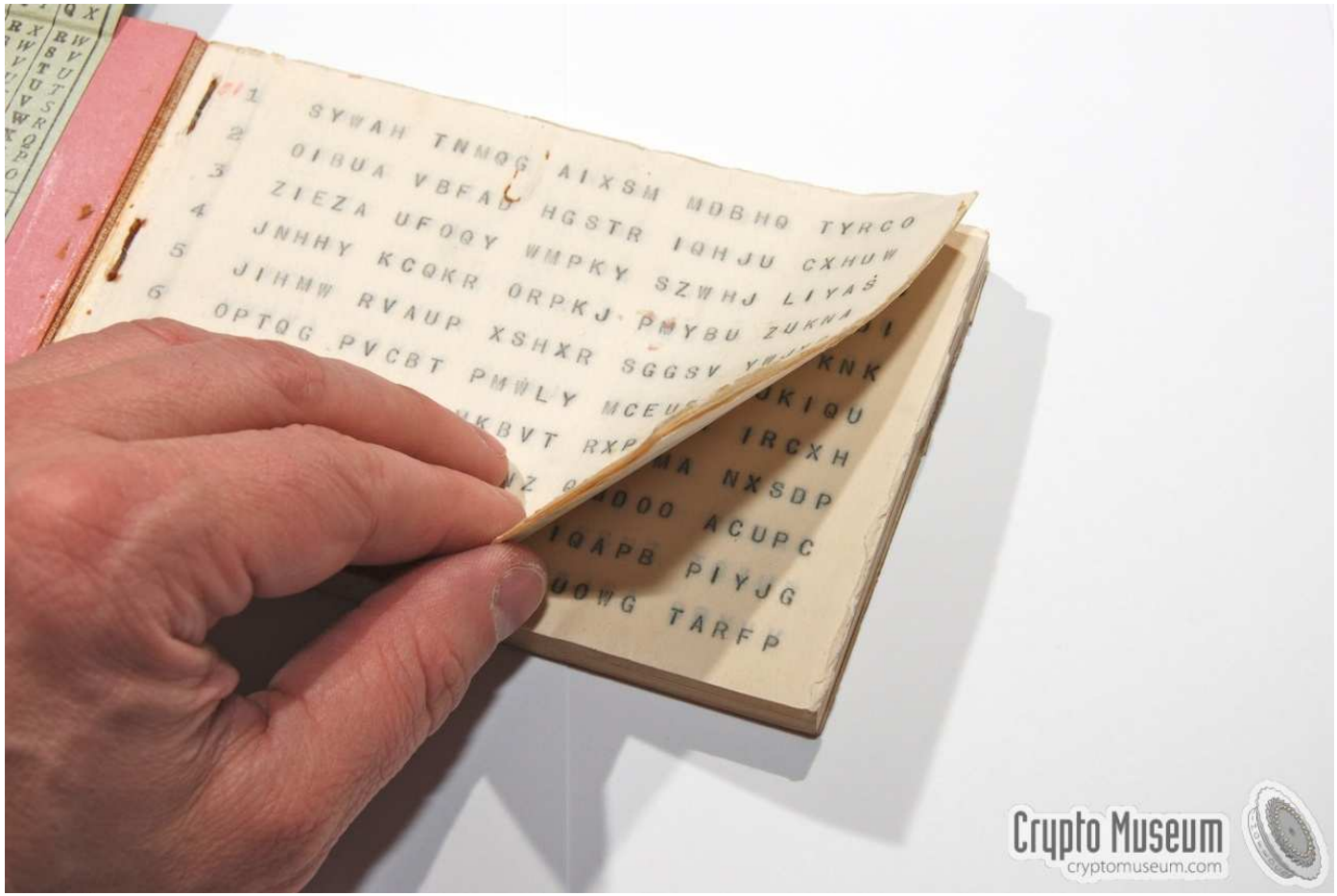
Supponiamo che Eva intercetti il messaggio cifrato di Alice e, senza conoscere la chiave, le provi tutte una ad una. Sicuramente troverà che la chiave “XMCKL” produce il messaggio “HELLO”, ma anche che la chiave “TQURI” produce il messaggio “LATER”:

```
     4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) testo cifrato
-------------------------------------------------------
  -  19 (T)  16 (Q)  20 (U)  17 (R)   8 (I) chiave possibile
  = -15       0      -7       4      17     testo cifrato - chiave
  =  11 (L)   0 (A)  19 (T)   4 (E)  17 (R) testo cifrato - chiave (mod 26)
-------------------------------------------------------
     L       A       T       E       R     messaggio
```

Non c’è alcuna informazione nel testo cifrato che permetta di selezionare quello esatto!

Se la chiave è *veramente casuale* e la si utilizza *una sola volta* la cifratura di Vernam ha la **segretezza perfetta.**

Il Cifrario Inattaccabile



Chiavi casuali monouso utilizzate dalle spie russe negli anni della guerra fredda. Per questo motivo il cifrario di Vernam è anche detto *one time pad (OTP)*, cioè “foglio monouso”.

Il Cifrario Inattaccabile

Problemi della cifratura OTP

- La chiave deve essere veramente casuale e non pseudo-casuale;
- Non deve MAI essere riutilizzata;
- Difficoltà nello scambio delle chiavi.

Parte II
Crittografia Quantistica

Un protocollo per generare e scambiare in assoluta sicurezza delle chiavi segrete tra due corrispondenti per usi crittografici, mediante particelle elementari e sfruttando le leggi della meccanica quantistica.

Come funziona il passaggio di informazioni?

Crittografia Quantistica

Un protocollo per generare e scambiare in assoluta sicurezza delle chiavi segrete tra due corrispondenti per usi crittografici, mediante particelle elementari e sfruttando le leggi della meccanica quantistica.

Attraverso due canali di comunicazione:

1. canale *quantico*, per lo scambio di particelle (fotoni);
2. canale *classico*, per le comunicazioni “standard”.

Crittografia Quantistica

Un protocollo per generare e scambiare in assoluta sicurezza delle chiavi segrete tra due corrispondenti per usi crittografici, mediante particelle elementari e sfruttando le leggi della meccanica quantistica.

Il protocollo ha la seguente struttura:

1. Alice e Bob si scambiano i fotoni preparati appositamente attraverso la fibra ottica (o lo spazio) che li connette;
2. dopo di che si scambiano alcune informazioni sul canale di comunicazione classico (protocollo a conoscenza zero);
3. alla fine di questo processo Alice e Bob hanno generato e si sono scambiati una chiave segreta casuale; se Eva è stata in grado di intercettare la chiave segreta Alice e Bob ne sono sicuramente a conoscenza e prenderanno le misure del caso.

Crittografia Quantistica

Un protocollo per generare e scambiare in assoluta sicurezza delle chiavi segrete tra due corrispondenti per usi crittografici, mediante particelle elementari e sfruttando le leggi della meccanica quantistica.

Una volta scambiatasi la chiave segreta, Alice e Bob possono utilizzare la crittografia OTP per lo scambio delle informazioni.

Crittografia Quantistica

Esistono due classi di protocollo per lo scambio quantico di chiavi, il cosiddetto *Quantum Key Distribution (QKD)*:

- basate sul principio di *sovrapposizione degli stati:* Bennett & Brassard (BB84);

Crittografia Quantistica

Esistono due classi di protocollo per lo scambio quantico di chiavi, il cosiddetto *Quantum Key Distribution (QKD)*:

- basate sul principio di *sovrapposizione degli stati:* Bennett & Brassard (BB84);
- basate sul fenomeno detto *quantum entanglement:* Eckert (E91)

La Cina lancia il primo satellite per le comunicazioni quantistiche

Pechino batte i rivali americani ed europei nella corsa alle trasmissioni ultrasicure. La tecnologia quantistica è infatti a prova di hacker e per realizzarla si stanno investendo miliardi di dollari

di ELENA DUSI

16 agosto 2016

la Repubblica.it

Crittografia Quantistica

Il satellite *Micius* (alias QUESS: Quantum Experiments at Space Scale), del peso di 600 kg, è stato posizionato su di un'orbita di 500 km il 16 Agosto 2016 alle ore 01:40 (tempo locale della base di Jiuquan, nel nord della Cina).
Al suo interno un cristallo in grado di generare fotoni *"entangled"*.

Crittografia Quantistica

RESEARCH

RESEARCH ARTICLE

QUANTUM OPTICS

Satellite-based entanglement distribution over 1200 kilometers

Juan Yin,[1,2] Yuan Cao,[1,2] Yu-Huai Li,[1,2] Sheng-Kai Liao,[1,2] Liang Zhang,[2,3] Ji-Gang Ren,[1,2] Wen-Qi Cai,[1,2] Wei-Yue Liu,[1,2] Bo Li,[1,2] Hui Dai,[1,2] Guang-Bing Li,[1,2] Qi-Ming Lu,[1,2] Yun-Hong Gong,[1,2] Yu Xu,[1,2] Shuang-Lin Li,[1,2] Feng-Zhi Li,[1,2] Ya-Yun Yin,[1,2] Zi-Qing Jiang,[3] Ming Li,[3] Jian-Jun Jia,[3] Ge Ren,[4] Dong He,[4] Yi-Lin Zhou,[5] Xiao-Xiang Zhang,[6] Na Wang,[7] Xiang Chang,[8] Zhen-Cai Zhu,[5] Nai-Le Liu,[1,2] Yu-Ao Chen,[1,2] Chao-Yang Lu,[1,2] Rong Shu,[2,3] Cheng-Zhi Peng,[1,2]* Jian-Yu Wang,[2,3]* Jian-Wei Pan[1,2]*

Long-distance entanglement distribution is essential for both foundational tests of quantum physics and scalable quantum networks. Owing to channel loss, however, the previously achieved distance was limited to ~100 kilometers. Here we demonstrate satellite-based distribution of entangled photon pairs to two locations separated by 1203 kilometers on Earth, through two satellite-to-ground downlinks with a summed length varying from 1600 to 2400 kilometers. We observed a survival of two-photon entanglement and a violation of Bell inequality by 2.37 ± 0.09 under strict Einstein locality conditions. The obtained effective link efficiency is orders of magnitude higher than that of the direct bidirectional transmission of the two photons through telecommunication fibers.

Quantum entanglement, first recognized by Einstein, Podolsky, and Rosen (*1*) and Schrödinger (*2*), is a physical phenomenon in which the quantum states of a many-particle system cannot be factorized into a product of single-particle wave functions, even when the particles are separated by large distances. Entangled states have been produced in laboratories (*3*–*5*) and exploited to test the contradiction between classical local hidden variable theory and quantum mechanics by using Bell's inequality (*6*). It is of fundamental interest to distribute entangled particles over increasingly large distances and study the behavior of entanglement under extreme conditions. Practically, large-scale dissemination of entanglement—eventually at a global scale—is useful as the essential physical resource for quantum information protocols such as quantum cryptography (*7*), quantum teleportation (*8*), and quantum networks (*9*).

Limitations on entanglement distribution

So far, entanglement distribution has only been achieved at a physical separation up to ~100 km (*10*) and is mainly limited by the photon loss in the channel (optical fibers or terrestrial free space), which normally scales exponentially with the channel length. For example, through bidirectional distribution of an entangled source of photon pairs with a 10-MHz count rate directly through two 600-km telecommunication fibers with a loss of 0.16 dB/km, eventually one would only obtain 10^{-12} two-photon coincidence events per second. When the transmitted photons are attenuated to a level comparable to the dark counts of the single-photon detectors, the entanglement cannot be established because of the low signal-to-noise ratio. To improve the signal-to-noise ratio, the entangled photons in the channel cannot simply be amplified because of the quantum noncloning theorem (*11*), but radically new methods to reduce the link attenuation must be developed.

One solution to improve the distribution is the protocol of quantum repeaters (*12*) that divide the whole transmission line into smaller segments and combine the functionalities of entanglement swapping (*13*), entanglement purification (*14*), and quantum storage (*15*). There has been considerable progress in the demonstrations of these building blocks (*16*–*18*) and proof-of-principle quantum repeater nodes (*19*, *20*). However, the practical usefulness of the quantum repeaters is still hindered by the challenges of simultaneously realizing and integrating all the key capabilities, including, most importantly, long storage time and high retrieval efficiency (*21*).

Satellite-based entanglement distribution

Another approach to global-scale quantum networks is making use of satellite- and space-based technologies. A satellite can conveniently cover two distant locations on Earth separated by thousands of kilometers. The key advantage of this approach is that the photon loss and turbulence predominantly occur in the lower ~10 km of the

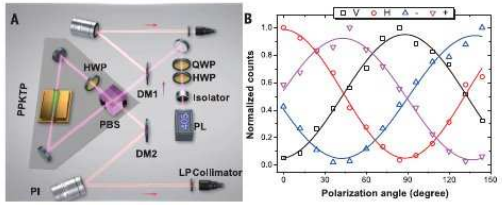


Fig. 1. Schematic of the spaceborne entangled-photon source and its in-orbit performance. (**A**) The thickness of the $KTiOPO_4$ (PPKTP) crystal is 15 mm. A pair of off-axis concave mirrors focus the pump laser (PL) in the center of the PPKTP crystal. At the output of the Sagnac interferometer, two dichromatic mirrors (DMs) and long-pass filters are used to separate the signal photons from the pump laser. Two additional electrically driven piezo steering mirrors (PIs), remotely controllable on the ground, are used for fine adjustment of the beam-pointing for an optimal collection efficiency into the single-mode fibers. QWP, quarter-wave plate; HWP, half-wave plate; PBS, polarizing beam splitter. (**B**) The two-photon correlation curves measured on-satellite by sampling 1% of each path of the entangled photons. The count rate measured from the overall 0.01% sampling is about 590 Hz, from which we can estimate the source brightness of 5.9 MHz.

[1]Department of Modern Physics and Hefei National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Hefei 230026, China. [2]Chinese Academy of Sciences (CAS) Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China. [3]Key Laboratory of Space Active Opto-Electronic Technology, Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai 200083, China. [4]Key Laboratory of Optical Engineering, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China. [5]Shanghai Engineering Center for Microsatellites, Shanghai 201203, China. [6]Key Laboratory of Space Object and Debris Observation, Purple Mountain Observatory, Chinese Academy of Sciences, Nanjing 210008, China. [7]Xinjiang Astronomical Observatory, Chinese Academy of Sciences, Urumqi 830011, China. [8]Yunnan Observatories, Chinese Academy of Sciences, Kunming 650011, China.
*Corresponding author. Email: pcz@ustc.edu.cn (C.-Z.P.); jywang@mail.sitp.ac.cn (J.-Y.W.); pan@ustc.edu.cn (J.-W.P.)

Il primo risultato ottenuto dal satellite *Micius* è stato l'aver trasmesso coppie di fotoni *entangled* tra due stazioni a Terra distanti oltre 1200 Km.

Article

Entanglement of two quantum memories via fibres over dozens of kilometres

https://doi.org/10.1038/s41586-020-1976-7

Received: 26 March 2019

Accepted: 12 November 2019

Published online: 12 February 2020

Yong Yu[1,2,3,6], Fei Ma[1,2,3,4,6], Xi-Yu Luo[1,2,3], Bo Jing[1,2,3], Peng-Fei Sun[1,2,3], Ren-Zhou Fang[1,2,3], Chao-Wei Yang[1,2,3], Hui Liu[1,2,3], Ming-Yang Zheng[4], Xiu-Ping Xie[4], Wei-Jun Zhang[5], Li-Xing You[5], Zhen Wang[5], Teng-Yun Chen[1,2,3], Qiang Zhang[1,2,3,4*], Xiao-Hui Bao[1,2,3*] & Jian-Wei Pan[1,2,3*]

A quantum internet that connects remote quantum processors[1,2] should enable a number of revolutionary applications such as distributed quantum computing. Its realization will rely on entanglement of remote quantum memories over long distances. Despite enormous progress[3–12], at present the maximal physical separation achieved between two nodes is 1.3 kilometres[10], and challenges for longer distances remain. Here we demonstrate entanglement of two atomic ensembles in one laboratory via photon transmission through city-scale optical fibres. The atomic ensembles function as quantum memories that store quantum states. We use cavity enhancement to efficiently create atom–photon entanglement[13–15] and we use quantum frequency conversion[16] to shift the atomic wavelength to telecommunications wavelengths. We realize entanglement over 22 kilometres of field-deployed fibres via two-photon interference[17,18] and entanglement over 50 kilometres of coiled fibres via single-photon interference[19]. Our experiment could be extended to nodes physically separated by similar distances, which would thus form a functional segment of the atomic quantum network, paving the way towards establishing atomic entanglement over many nodes and over much longer distances.

Article

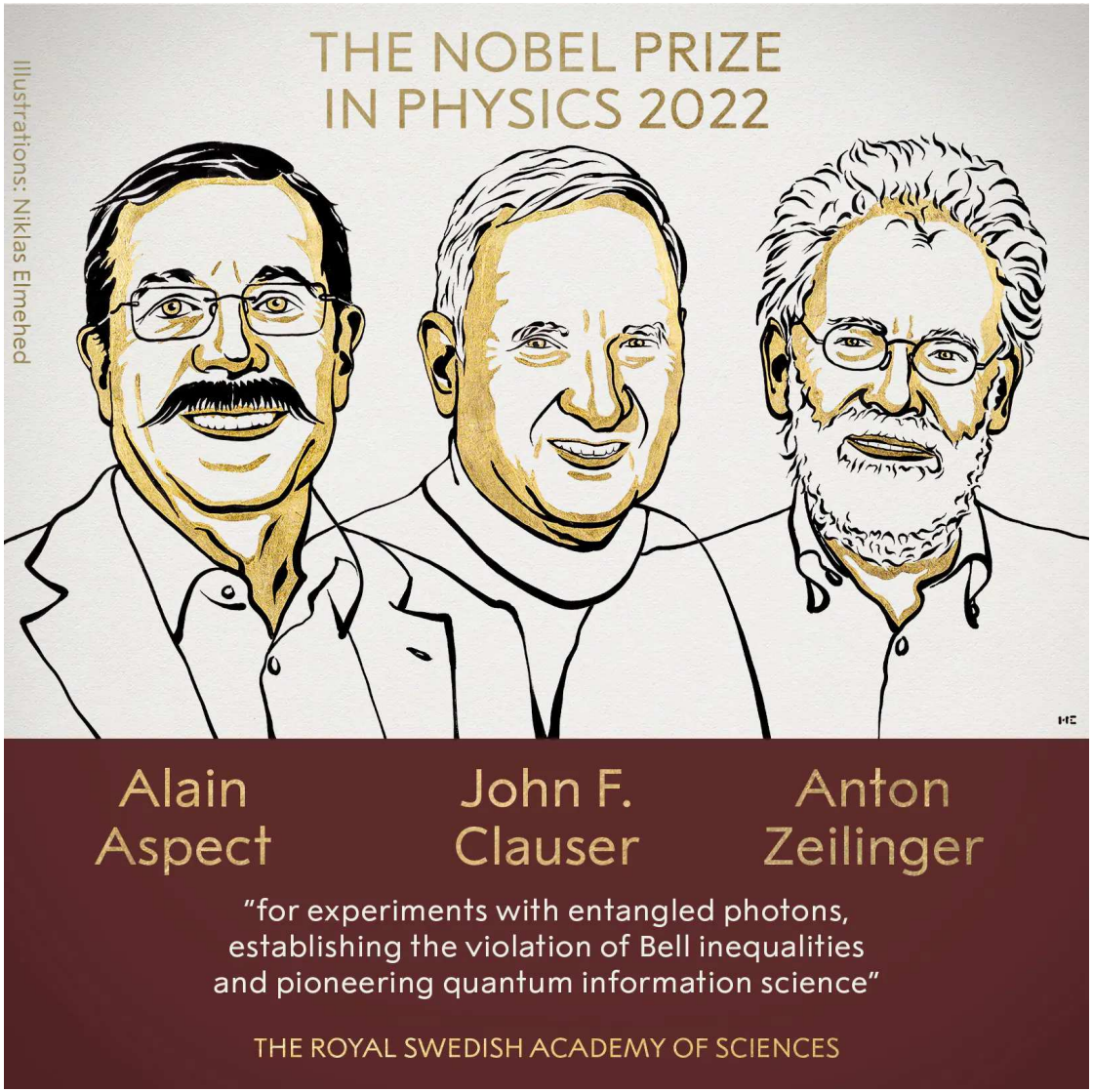
Experimental quantum key distribution certified by Bell's theorem

https://doi.org/10.1038/s41586-022-04941-5
Received: 29 September 2021
Accepted: 7 June 2022
Published online: 27 July 2022
Check for updates

D. P. Nadlinger[1]✉, P. Drmota[1], B. C. Nichol[1], G. Araneda[1], D. Main[1], R. Srinivas[1], D. M. Lucas[1], C. J. Ballance[1]✉, K. Ivanov[2], E. Y.-Z. Tan[3], P. Sekatski[4], R. L. Urbanke[2], R. Renner[3], N. Sangouard[5]✉ & J.-D. Bancal[5]✉

Cryptographic key exchange protocols traditionally rely on computational conjectures such as the hardness of prime factorization[1] to provide security against eavesdropping attacks. Remarkably, quantum key distribution protocols such as the Bennett–Brassard scheme[2] provide information-theoretic security against such attacks, a much stronger form of security unreachable by classical means. However, quantum protocols realized so far are subject to a new class of attacks exploiting a mismatch between the quantum states or measurements implemented and their theoretical modelling, as demonstrated in numerous experiments[3–6]. Here we present the experimental realization of a complete quantum key distribution protocol immune to these vulnerabilities, following Ekert's pioneering proposal[7] to use entanglement to bound an adversary's information from Bell's theorem[8]. By combining theoretical developments with an improved optical fibre link generating entanglement between two trapped-ion qubits, we obtain 95,628 key bits with device-independent security[9–12] from 1.5 million Bell pairs created during eight hours of run time. We take steps to ensure that information on the measurement results is inaccessible to an eavesdropper. These measurements are performed without space-like separation. Our result shows that provably secure cryptography under general assumptions is possible with real-world devices, and paves the way for further quantum information applications based on the device-independence principle.

Crittografia Quantistica



Protocollo a Conoscenza Zero

Metodo *interattivo* utilizzato da un soggetto per dimostrare ad un altro soggetto che una affermazione è vera, senza rivelare nient'altro oltre alla veridicità della stessa.

Protocollo a Conoscenza Zero

Metodo *interattivo* utilizzato da un soggetto per dimostrare ad un altro soggetto che una affermazione è vera, senza rivelare nient'altro oltre alla veridicità della stessa.

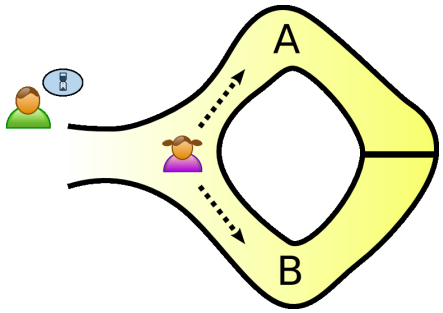
Alice conosce la parola segreta usata per aprire la porta magica in una caverna.

Bob dice che la pagherà per il segreto, ma non prima di essere sicuro che lei lo conosca davvero.

Alice si dice d'accordo a rivelargli il segreto, ma non prima di aver ricevuto i soldi.

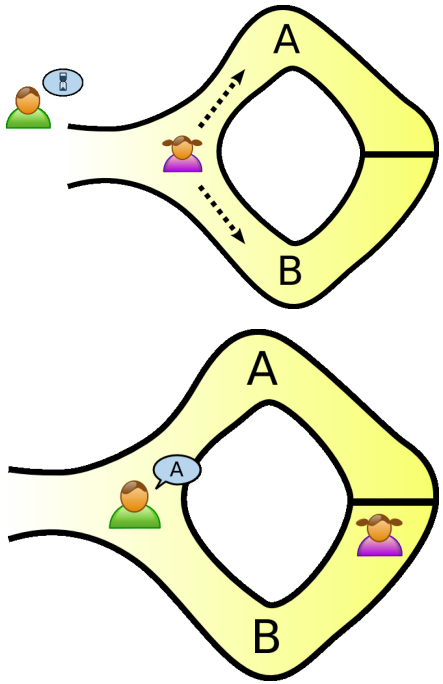
Pianificano quindi uno schema con il quale Alice può dare prova a Bob di conoscere la parola senza rivelargliela.

Protocollo a Conoscenza Zero



Bob aspetta fuori dalla caverna mentre Alice entra, scegliendo a caso uno dei due sentieri.

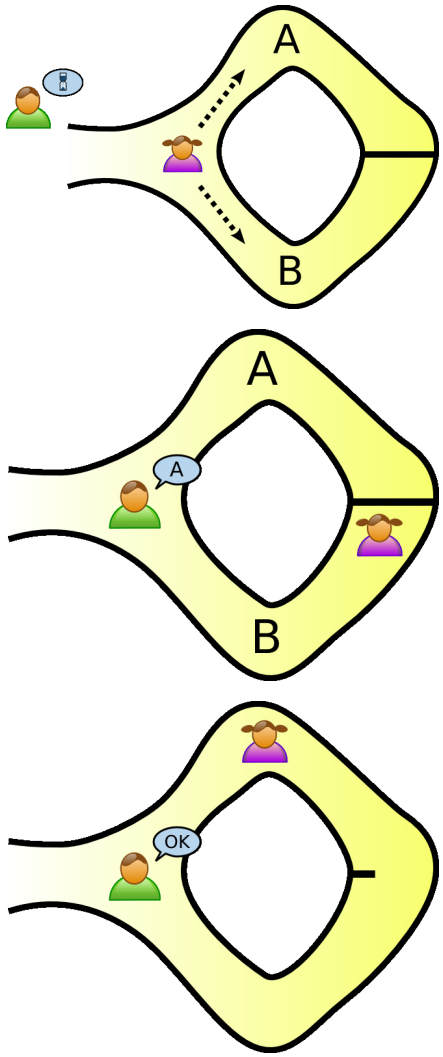
Protocollo a Conoscenza Zero



Bob aspetta fuori dalla caverna mentre Alice entra, scegliendo a caso uno dei due sentieri.

Bob entra nella caverna e grida il nome del sentiero che Peggy dovrà utilizzare per ritornare indietro, fra A e B, preso a caso.

Protocollo a Conoscenza Zero



Bob aspetta fuori dalla caverna mentre Alice entra, scegliendo a caso uno dei due sentieri.

Bob entra nella caverna e grida il nome del sentiero che Peggy dovrà utilizzare per ritornare indietro, fra A e B, preso a caso.

Se alice conosce come aprire la porta, ritornerà attraverso il sentiero desiderato. È da notare che Bob non conosce il sentiero per il quale Alice è entrata.

Protocollo a Conoscenza Zero

Se Alice non conosce parola segreta per aprire la porta, ha il 50% di probabilità di indovinare correttamente.

Ripetendo molte volte questo espediente Bob può concludere che *molto probabilmente* Alice conosce davvero la parola segreta.

Protocollo a Conoscenza Zero

Se Alice non conosce parola segreta per aprire la porta, ha il 50% di probabilità di indovinare correttamente.

Ripetendo molte volte questo espediente Bob può concludere che *molto probabilmente* Alice conosce davvero la parola segreta.

Le dimostrazioni a conoscenza zero non sono dimostrazioni in senso matematico poiché c'è sempre una piccola probabilità che un dimostratore imbroglione riesca a convincere un verificatore di una affermazione falsa.

Protocollo a Conoscenza Zero

Se Alice non conosce parola segreta per aprire la porta, ha il 50% di probabilità di indovinare correttamente.

Ripetendo molte volte questo espediente Bob può concludere che *molto probabilmente* Alice conosce davvero la parola segreta.

Le dimostrazioni a conoscenza zero non sono dimostrazioni in senso matematico poiché c'è sempre una piccola probabilità che un dimostratore imbroglione riesca a convincere un verificatore di una affermazione falsa.

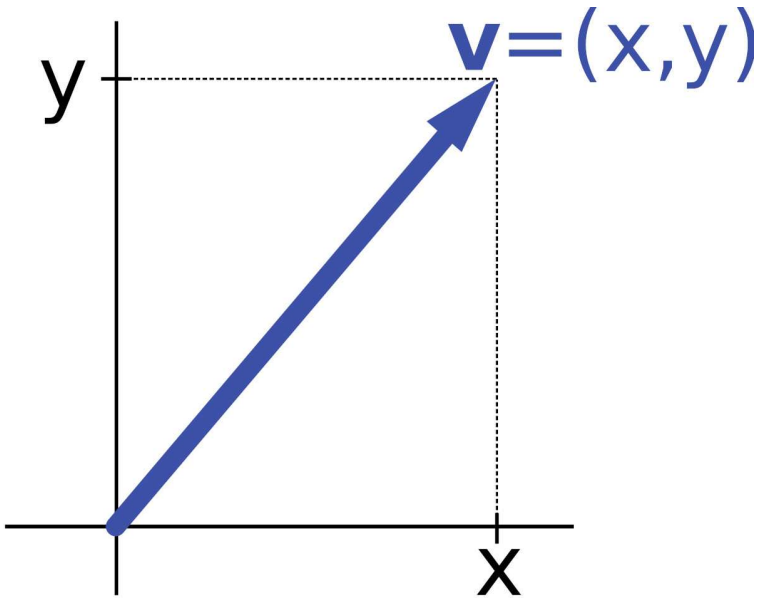
Questi tipi di algoritmi sono probabilistici e non deterministici. Tuttavia, ci sono tecniche per ridurre questa probabilità a valori piccoli a piacere.

Stato Quantico di un Sistema

In meccanica quantistica lo stato di un sistema viene rappresentato da un **vettore**, detto appunto *vettore di stato,* (o anche *funzione d'onda*) che appartiene ad uno spazio vettoriale: lo *spazio degli stati.*

Stato Quantico di un Sistema

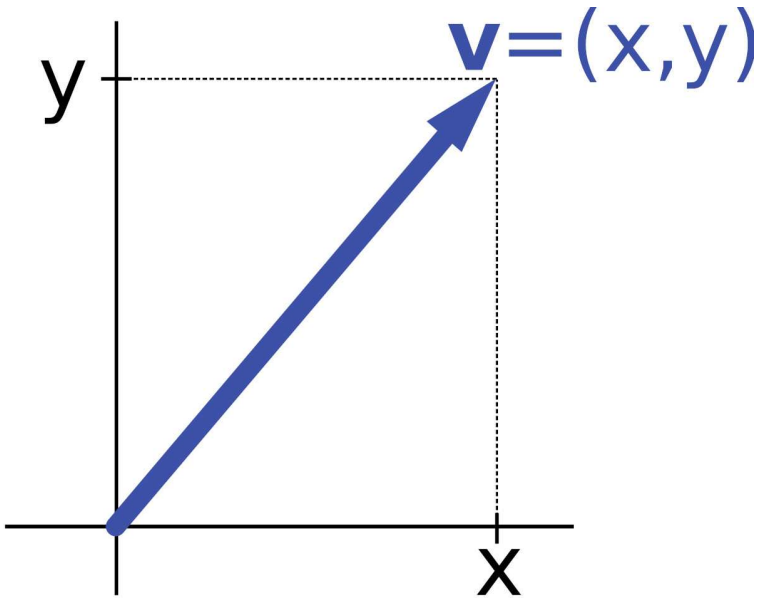
In meccanica quantistica lo stato di un sistema viene rappresentato da un **vettore**, detto appunto *vettore di stato,* (o anche *funzione d'onda*) che appartiene ad uno spazio vettoriale: lo *spazio degli stati.*



Gli stati possono essere sommati tra di loro: abbiamo il cosiddetto *principio di sovrapposizione.*

Stato Quantico di un Sistema

In meccanica quantistica lo stato di un sistema viene rappresentato da un **vettore**, detto appunto *vettore di stato,* (o anche *funzione d'onda*) che appartiene ad uno spazio vettoriale: lo *spazio degli stati.*

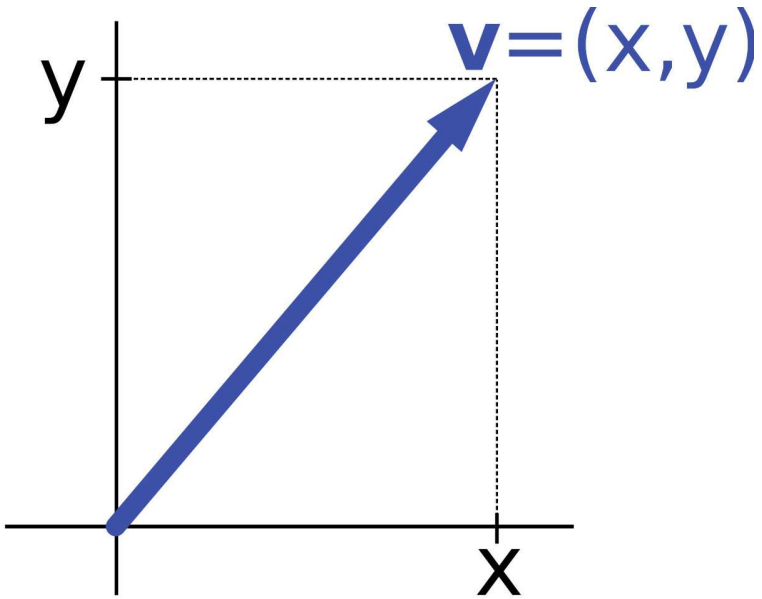


Gli stati possono essere sommati tra di loro: abbiamo il cosiddetto *principio di sovrapposizione.*

Si ottengono in questo modo infiniti possibili stati che descrivono lo stesso sistema.

Stato Quantico di un Sistema

In meccanica quantistica lo stato di un sistema viene rappresentato da un **vettore**, detto appunto *vettore di stato,* (o anche *funzione d'onda*) che appartiene ad uno spazio vettoriale: lo *spazio degli stati.*



Gli stati possono essere sommati tra di loro: abbiamo il cosiddetto *principio di sovrapposizione.*

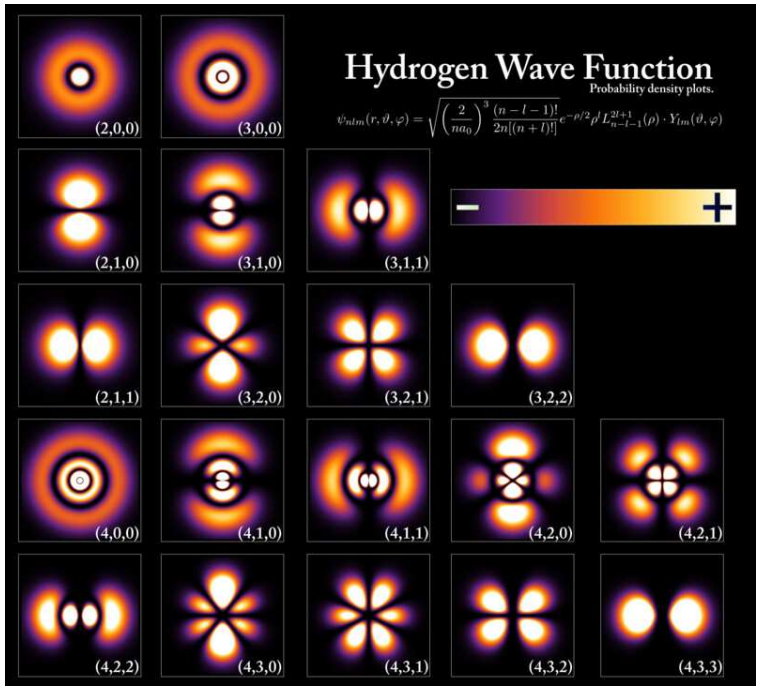
Si ottengono in questo modo infiniti possibili stati che descrivono lo stesso sistema.

Un sistema può quindi trovarsi **contemporaneamente** in due stati diversi.

Stato Quantico di un Sistema

Uno stato quantico è un'entità matematica che fornisce una *distribuzione di probabilità* per i risultati di ogni possibile misurazione su un sistema.

È una funzione complessa che ha come variabili reali le coordinate spaziali x, y, z ed il tempo t.



Stato Quantico di Due Sistemi

Supponiamo che il sistema A sia descritto da due stati $|\uparrow\rangle$ e $|\downarrow\rangle$. Lo stesso sia per il sistema B.

Stato Quantico di Due Sistemi

Supponiamo che il sistema A sia descritto da due stati $|\uparrow\rangle$ e $|\downarrow\rangle$. Lo stesso sia per il sistema B.

Il sistema $A + B$ potrà essere descritto dai quattro stati:

$$|\uparrow\uparrow\rangle\,,|\uparrow\downarrow\rangle\,,|\downarrow\uparrow\rangle\,,|\downarrow\downarrow\rangle$$

più tutte le loro possibili somme.

Stato Quantico di Due Sistemi

Supponiamo che il sistema A sia descritto da due stati $|\uparrow\rangle$ e $|\downarrow\rangle$. Lo stesso sia per il sistema B.

Il sistema $A + B$ potrà essere descritto dai quattro stati:

$$|\uparrow\uparrow\rangle\,, |\uparrow\downarrow\rangle\,, |\downarrow\uparrow\rangle\,, |\downarrow\downarrow\rangle$$

più tutte le loro possibili somme.

Ad esempio, A e B potranno essere entrambi $\uparrow$ e contemporaneamente entrambi $\downarrow$, cioè nello stato descritto dal vettore di stato

$$|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle\ .$$

Stato Quantico di Due Sistemi

Questo significa che lo stato è formato da una coppia: non è possibile dire in che stato sia A senza considerare lo stato di B.

Stato Quantico di Due Sistemi

Questo significa che lo stato è formato da una coppia: non è possibile dire in che stato sia A senza considerare lo stato di B.

Lo stato dei due sistemi è quantisticamente correlato, e le due particelle si dicono **entangled.**

Stato Quantico di Due Sistemi

Questo significa che lo stato è formato da una coppia: non è possibile dire in che stato sia A senza considerare lo stato di B.

Lo stato dei due sistemi è quantisticamente correlato, e le due particelle si dicono **entangled.**

Cosa succede quando effettuiamo una **misura** dello stato di un sistema?

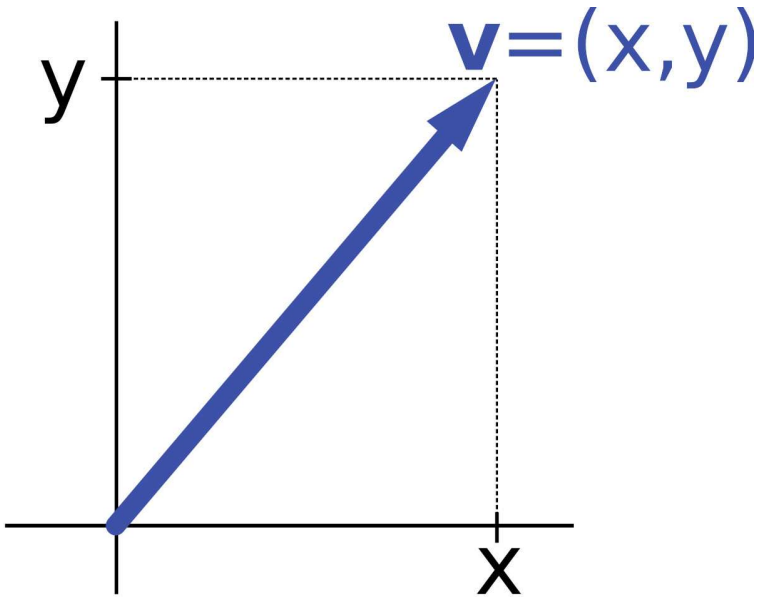
Misura di un Sistema Quantico

La misura di un sistema quantico, cioè l'interazione del sistema quantico con l'ambiente esterno, ne modifica lo stato.

Misura di un Sistema Quantico

La misura di un sistema quantico, cioè l'interazione del sistema quantico con l'ambiente esterno, ne modifica lo stato.

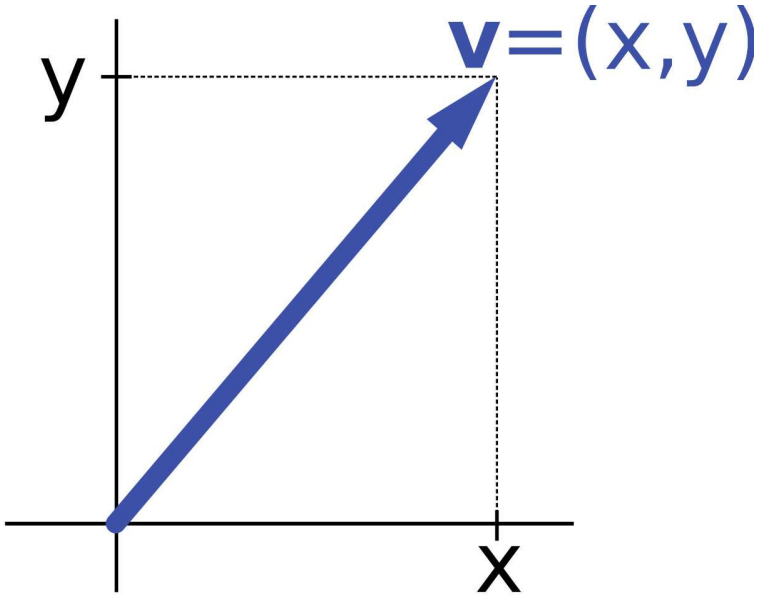
Abbiamo visto che un sistema è descritto come una sovrapposizione di stati.



Misura di un Sistema Quantico

La misura di un sistema quantico, cioè l'interazione del sistema quantico con l'ambiente esterno, ne modifica lo stato.

Abbiamo visto che un sistema è descritto come una sovrapposizione di stati.



La misura determina il **"collasso"** del vettore di stato.

$$A = |\uparrow\rangle + |\downarrow\rangle \xrightarrow{\text{misura}} \begin{cases} |\uparrow\rangle \\ \text{oppure} \\ |\downarrow\rangle \end{cases}$$

Misura di un Sistema Quantico

Quando misuriamo una particella “entangled”, il collasso del suo vettore di stato implica il collasso immediato anche del vettore di stato dell’altro membro della coppia.

Misura di un Sistema Quantico

Quando misuriamo una particella “entangled”, il collasso del suo vettore di stato implica il collasso immediato anche del vettore di stato dell’altro membro della coppia.

Nessun riferimento viene fatto a dove si trovino le due particelle, quindi il fenomeno dell’entanglement viola il **principio di località**: un oggetto è influenzato direttamente solo dalle sue immediate vicinanze.

Misura di un Sistema Quantico

Quando misuriamo una particella "entangled", il collasso del suo vettore di stato implica il collasso immediato anche del vettore di stato dell'altro membro della coppia.

Nessun riferimento viene fatto a dove si trovino le due particelle, quindi il fenomeno dell'entanglement viola il **principio di località**: un oggetto è influenzato direttamente solo dalle sue immediate vicinanze.

Per questo motivo Einstein liquidò l'entanglement come *spuckafte ferwirklung,* che può essere tradotto con "inquietante azione a distanza": paradosso di Einstein, Podolsky e Rosen (EPR).

- **Paradosso di Einstein, Podolsky e Rosen (EPR)**
  L'entanglement porta ad un paradosso perchè viene implicitamente assunto valido il **realismo locale**.

Paradosso di Einstein, Podolsky e Rosen (EPR)

L'entanglement porta ad un paradosso perchè viene implicitamente assunto valido il **realismo locale**.

In particolare, si assume la nozione intuitiva che i parametri delle particelle abbiano valori definiti indipendentemente dall'atto di osservazione.

Paradosso di Einstein, Podolsky e Rosen (EPR)

L'entanglement porta ad un paradosso perchè viene implicitamente assunto valido il **realismo locale**.

In particolare, si assume la nozione intuitiva che i parametri delle particelle abbiano valori definiti indipendentemente dall'atto di osservazione.

John Stuart Bell ha dimostrato che la condizione di realismo locale impone alcune restrizioni delle correlazioni statistiche previste dalla meccanica quantistica tra misure su particelle considerate entangled.

Paradosso di Einstein, Podolsky e Rosen (EPR)

L'entanglement porta ad un paradosso perchè viene implicitamente assunto valido il **realismo locale**.

In particolare, si assume la nozione intuitiva che i parametri delle particelle abbiano valori definiti indipendentemente dall'atto di osservazione.

John Stuart Bell ha dimostrato che la condizione di realismo locale impone alcune restrizioni delle correlazioni statistiche previste dalla meccanica quantistica tra misure su particelle considerate entangled.

Queste restrizioni statistiche possono essere verificate sperimentalmente tramite misure della polarizzazione di fotoni.

Paradosso di Einstein, Podolsky e Rosen (EPR)

L'entanglement porta ad un paradosso perchè viene implicitamente assunto valido il **realismo locale**.

In particolare, si assume la nozione intuitiva che i parametri delle particelle abbiano valori definiti indipendentemente dall'atto di osservazione.

John Stuart Bell ha dimostrato che la condizione di realismo locale impone alcune restrizioni delle correlazioni statistiche previste dalla meccanica quantistica tra misure su particelle considerate entangled.

Queste restrizioni statistiche possono essere verificate sperimentalmente tramite misure della polarizzazione di fotoni.

Risultato: le diseguaglianze di Bell sono violate, quindi il mondo reale è non locale.

Teorema di non clonazione quantistica

Una conseguenza importante del collasso del vettore di stato è il *Teorema di non clonazione quantistica (no cloning theorem):*

> Non è possibile duplicare esattamente (clonare) uno stato quantico sconosciuto a priori.

Aforismario

Se credete
di aver capito la
meccanica quantistica,
non avete capito la
meccanica quantistica.
Richard Feynman

Aforismario

If I were forced to sum up in one sentence what the Copenhagen interpretation says to me, it would be 'Shut up and calculate!'

- David Mermin -

Protocollo Bennett & Brassard (BB84)

Alice vuole mandare a Bob un messaggio che consiste in una serie di 0 e 1. Rappresenterà le cifre binarie con fotoni con un certo stato di polarizzazione. Si possono utilizzare due schemi:

- *rettilineo* o schema +
  - 1 fotone ↕
  - 0 fotone ↔
- *diagonale* o schema ×
  - 1 fotone ⤢
  - 0 fotone ⤡

Nell'inviare il messaggio, Alice passa da uno schema all'altro in maniera arbitraria.

Protocollo Bennett & Brassard (BB84)

Ecco un esempio di messaggio binario trasmesso:

Messaggio	1	1	0	1	1	0	1	0	0	1
Schema	+	×	+	×	×	×	+	+	×	×
Trasmissione	↕	⤢	↔	⤢	⤢	⤡	↕	↔	⤡	⤢

Protocollo Bennett & Brassard (BB84)

Bob riceve la sequenza di fotoni inviata da Alice. Dato che non conosce lo schema di polarizzazione utilizzato da Alice, va a caso. Ecco i possibili casi:

Schema di Alice	Bit di Alice	Alice invia	Rivel. di Bob	Rivel. giusto	Bob rileva	Bit per Bob	Bit giusto
Rettilineo	1	↕	+	sì	↕	1	sì
			×	no	⤢	1	sì
					⤡	0	no
	0	↔	+	sì	↔	0	sì
			×	no	⤢	1	no
					⤡	0	sì
Diagonale	1	⤢	+	no	↕	1	sì
					↔	0	no
			×	sì	⤢	1	sì
	0	⤡	+	no	↕	1	no
					↔	0	sì
			×	sì	⤡	0	sì

Protocollo Bennett & Brassard (BB84)

① Alice ha inviato a Bob una serie di 0 e 1;

Protocollo Bennett & Brassard (BB84)

① Alice ha inviato a Bob una serie di 0 e 1;

② Bob ne ha interpretati correttamente alcuni e fraintesi altri;

Protocollo Bennett & Brassard (BB84)

① Alice ha inviato a Bob una serie di 0 e 1;

② Bob ne ha interpretati correttamente alcuni e fraintesi altri;

③ Alice chiama Bob su una linea non protetta e comunica a Bob *lo schema di polarizzazione* usato per ogni fotone;

Protocollo Bennett & Brassard (BB84)

① Alice ha inviato a Bob una serie di 0 e 1;

② Bob ne ha interpretati correttamente alcuni e fraintesi altri;

③ Alice chiama Bob su una linea non protetta e comunica a Bob *lo schema di polarizzazione* usato per ogni fotone;

④ Bob comunica ad Alice in quale occasione ha indovinato lo schema di polarizzazione;

Protocollo Bennett & Brassard (BB84)

① Alice ha inviato a Bob una serie di 0 e 1;

② Bob ne ha interpretati correttamente alcuni e fraintesi altri;

③ Alice chiama Bob su una linea non protetta e comunica a Bob *lo schema di polarizzazione* usato per ogni fotone;

④ Bob comunica ad Alice in quale occasione ha indovinato lo schema di polarizzazione;

⑤ Alice e Bob decidono di ignorare i fotoni per i quali Bob ha usato lo schema sbagliato;

Protocollo Bennett & Brassard (BB84)

① Alice ha inviato a Bob una serie di 0 e 1;

② Bob ne ha interpretati correttamente alcuni e fraintesi altri;

③ Alice chiama Bob su una linea non protetta e comunica a Bob *lo schema di polarizzazione* usato per ogni fotone;

④ Bob comunica ad Alice in quale occasione ha indovinato lo schema di polarizzazione;

⑤ Alice e Bob decidono di ignorare i fotoni per i quali Bob ha usato lo schema sbagliato;

⑥ Alice e Bob hanno concordato una sequenza comune di cifre binarie **casuali**. Questa sarà la chiave per cifrare un messaggio.

Protocollo Bennett & Brassard (BB84)

Cosa succede se Eva intercetta i fotoni inviati da Alice a Bob? Potrebbe ad esempio farne una copia ed inviare l'originale a Bob (il cosiddetto *"man in the middle"*).
In questo modo si troverebbe nella stessa situazione di Bob e potrebbe effettuare le stesse procedure, intercettando lo schema di polarizzazione di Alice, trasmesso su di un canale non sicuro.

Protocollo Bennett & Brassard (BB84)

Cosa succede se Eva intercetta i fotoni inviati da Alice a Bob? Potrebbe ad esempio farne una copia ed inviare l'originale a Bob (il cosiddetto *"man in the middle"*).
In questo modo si troverebbe nella stessa situazione di Bob e potrebbe effettuare le stesse procedure, intercettando lo schema di polarizzazione di Alice, trasmesso su di un canale non sicuro.

① Eva non può fare una copia del fotone inviato da Alice;

② Eva non commetterà gli stessi errori di Bob.

Protocollo Bennett & Brassard (BB84)

Cosa succede se Eva intercetta i fotoni inviati da Alice a Bob? Potrebbe ad esempio farne una copia ed inviare l'originale a Bob (il cosiddetto *"man in the middle"*).
In questo modo si troverebbe nella stessa situazione di Bob e potrebbe effettuare le stesse procedure, intercettando lo schema di polarizzazione di Alice, trasmesso su di un canale non sicuro.

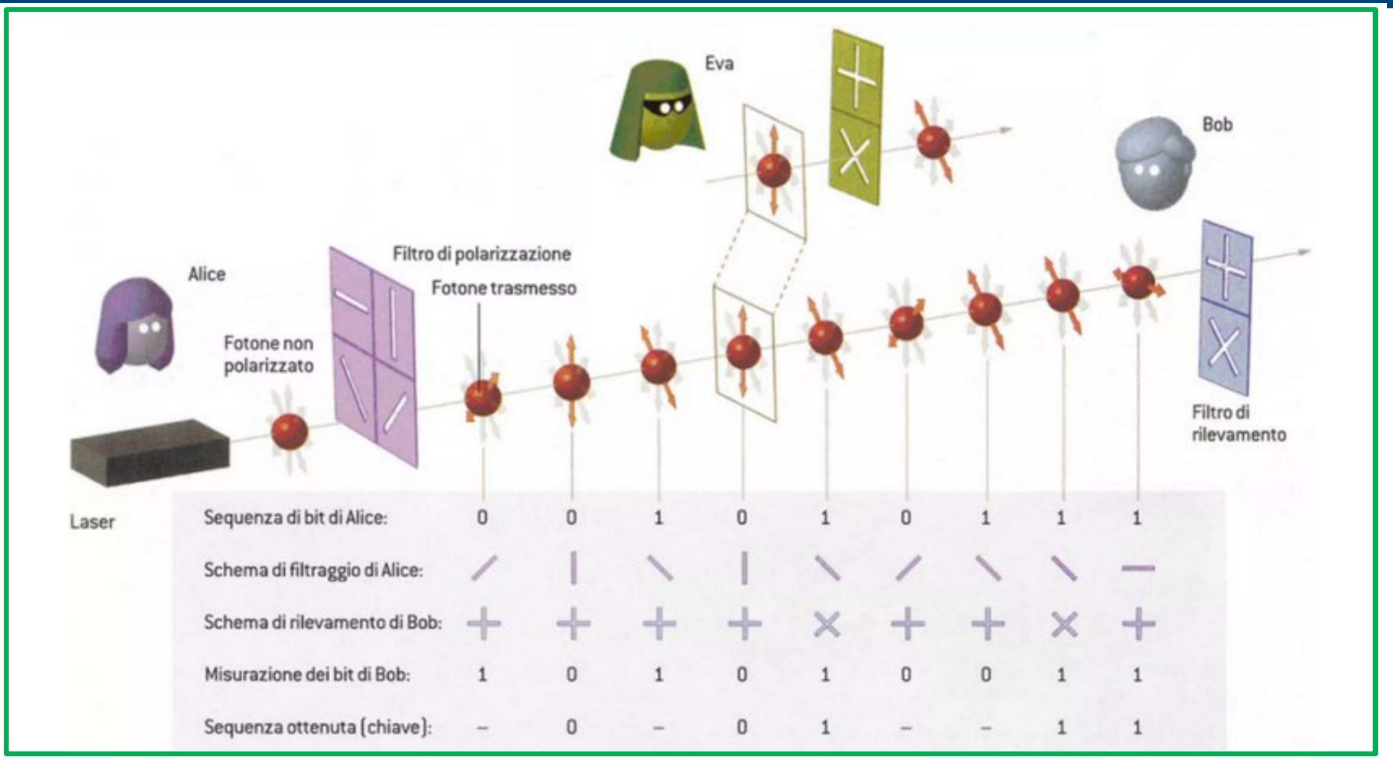
① Eva non può fare una copia del fotone inviato da Alice;

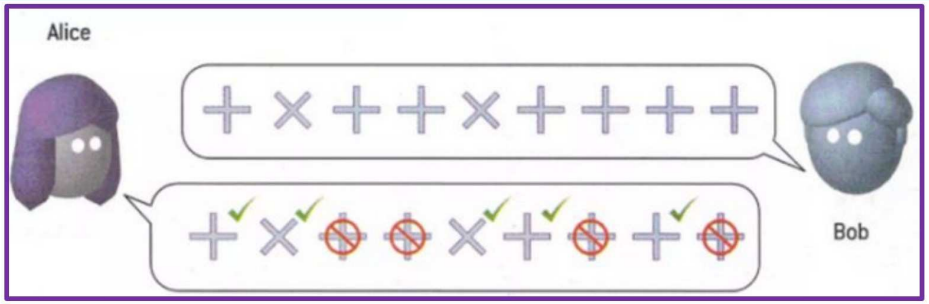
② Eva non commetterà gli stessi errori di Bob.

Qualsiasi azione faccia, Eva disturba e modifica i fotoni inviati da Alice!

Protocollo Bennett & Brassard (BB84)

Quantum Channel





Classic Channel

http://fredhenle.net/bb84/demo.php

Protocollo Eckert (E91)

① Alice e Bob ricevono fotoni “entangled”;

Protocollo Eckert (E91)

① Alice e Bob ricevono fotoni “entangled”;

② Alice e Bob scelgono uno schema di polarizzazione;

Protocollo Eckert (E91)

① Alice e Bob ricevono fotoni “entangled”;

② Alice e Bob scelgono uno schema di polarizzazione;

③ Alice e Bob si scambiano su una linea non protetta *lo schema di polarizzazione* usato per ogni fotone;

Protocollo Eckert (E91)

① Alice e Bob ricevono fotoni “entangled”;

② Alice e Bob scelgono uno schema di polarizzazione;

③ Alice e Bob si scambiano su una linea non protetta *lo schema di polarizzazione* usato per ogni fotone;

④ i fotoni analizzati con lo stesso schema di polarizzazione avranno polarizzazioni opposte;

Protocollo Eckert (E91)

① Alice e Bob ricevono fotoni “entangled”;

② Alice e Bob scelgono uno schema di polarizzazione;

③ Alice e Bob si scambiano su una linea non protetta *lo schema di polarizzazione* usato per ogni fotone;

④ i fotoni analizzati con lo stesso schema di polarizzazione avranno polarizzazioni opposte;

⑤ Alice e Bob hanno concordato una sequenza comune di cifre binarie **casuali**. Questa sarà la chiave per cifrare un messaggio.

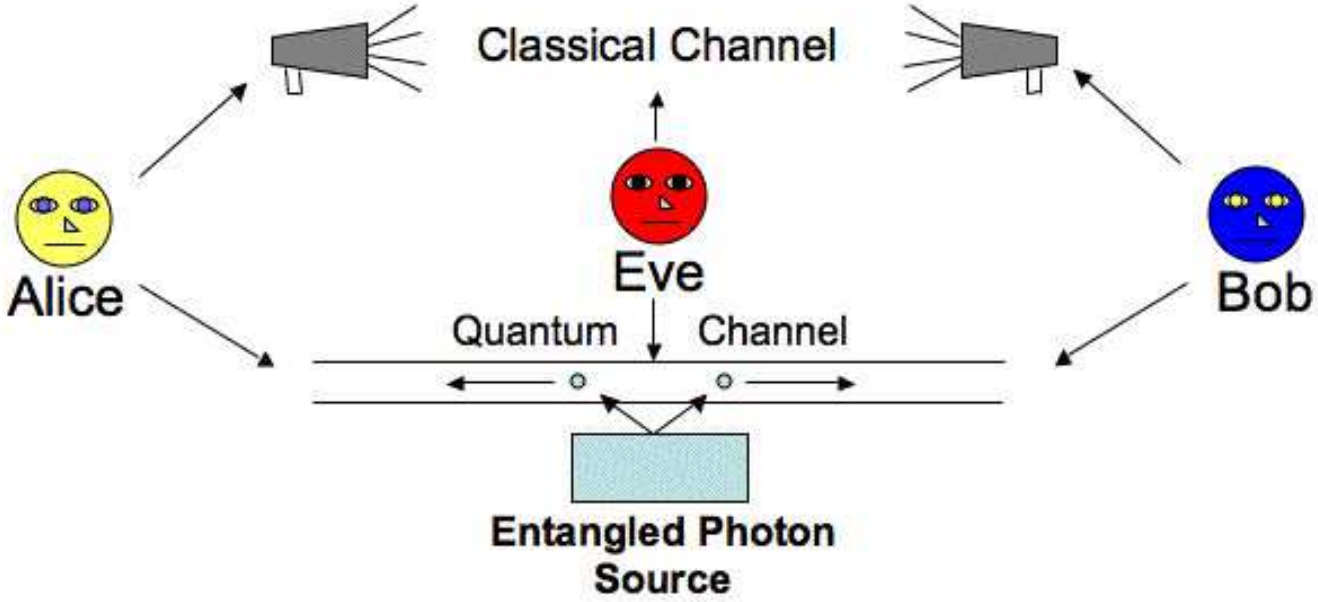
Protocollo Eckert (E91)

Cosa succede se Eva intercetta i fotoni inviati da Alice a Bob?

Protocollo Eckert (E91)

Cosa succede se Eva intercetta i fotoni inviati da Alice a Bob?

Alice e Bob possono analizzare i fotoni che hanno scartato utilizzando un terzo schema di polarizzazione. Scambiandosi questa informazione, ed utilizzando la *Disuguaglianza di Bell* possono capire se i fotoni sono stati intercettati da Eva, ed agire di conseguenza.



Bibliografia

- Simon Singh. 2001. *Codici & Segreti — La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet.* BUR Biblioteca Univ. Rizzoli
- *The Black Chamber*
  `http://www.simonsingh.net/The_Black_Chamber/chamberguide.html`
- *La Crittografia da Atbash a RSA*
  `http://www.crittologia.eu/`
- *Cifratura di Vigenère interattiva*
  `https://studio.code.org/s/vigenere/stage/1/puzzle/1`
- *Simulazione protocollo BB84 interattiva*
  `http://fredhenle.net/bb84/demo.php`
- Andrea Pasquinucci. 2004. *Aspetti di Crittografia Moderna — Da DES alla Crittografia Quantistica.* Quaderni CLUSIT


GRAZIE!