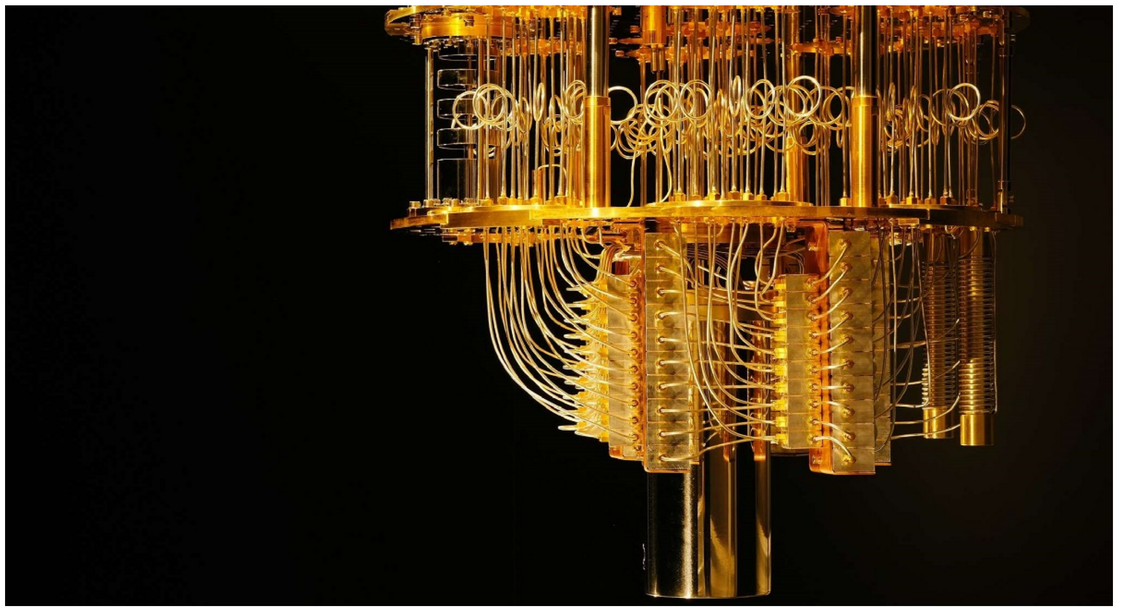
Tecnologie quantistiche

Didattica della fisica quantistica



PLS 2020-2021 - Università degli studi di Pavia - Fisica

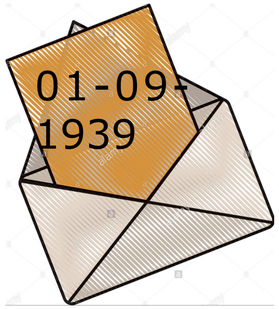
Chiara Macchiavello
Lidia Falomo
Massimiliano Malgieri
Claudio Sutrini

Crittografia classica: dall’antichità al Novecento

Alice

Bob

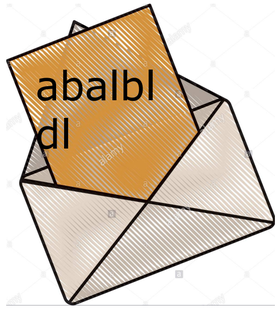
Testo in chiaro



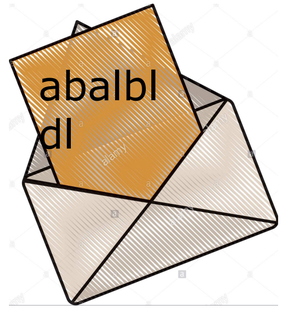
Algoritmo
Cifrario

Cifratura

Testo cifrato



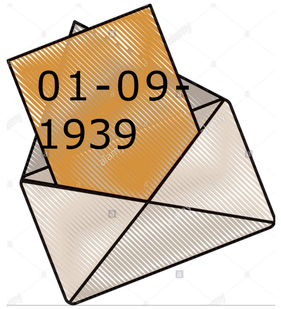
Testo cifrato



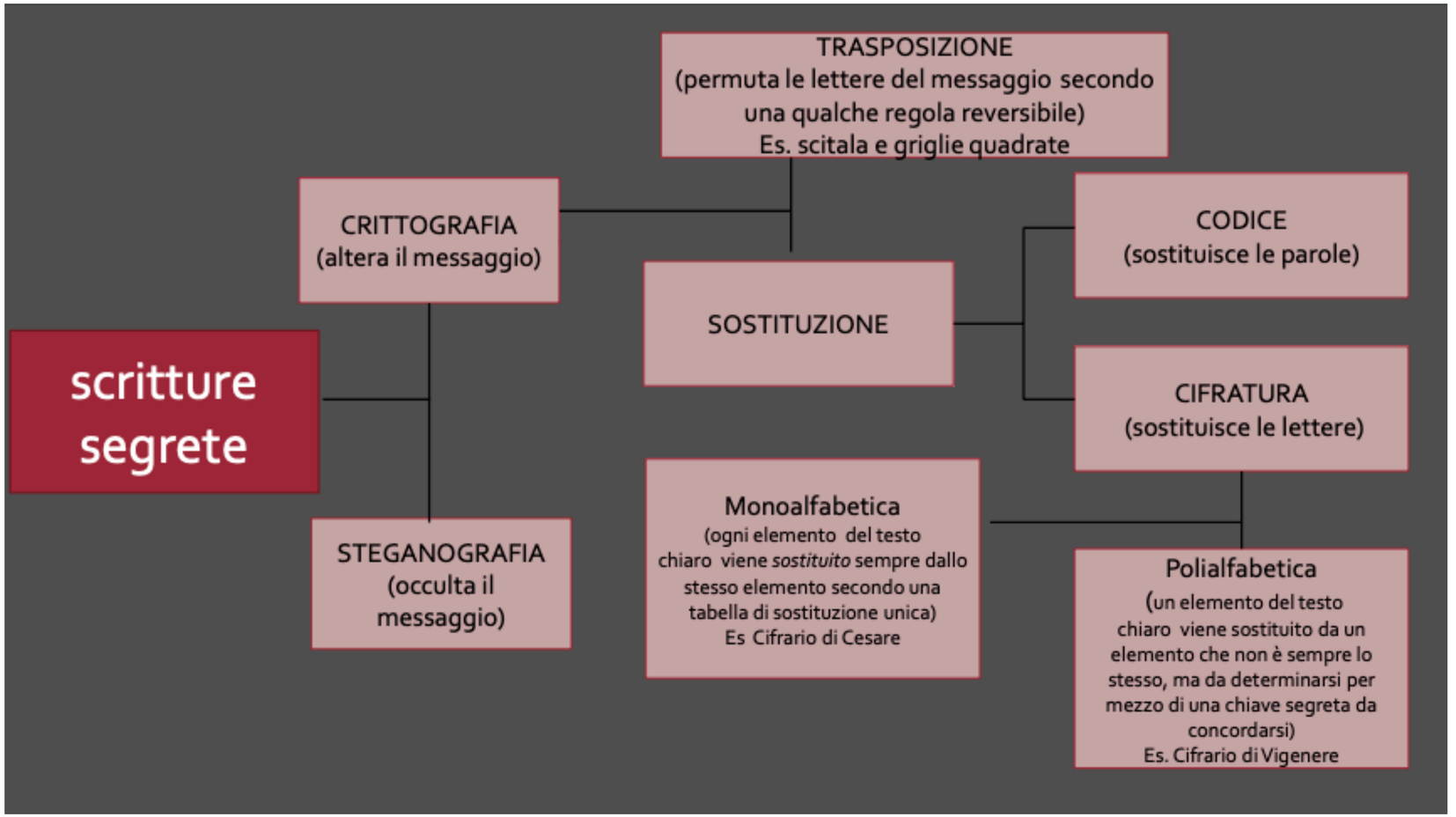
Algoritmo
Cifrario

Decifrazione

Testo decifrato

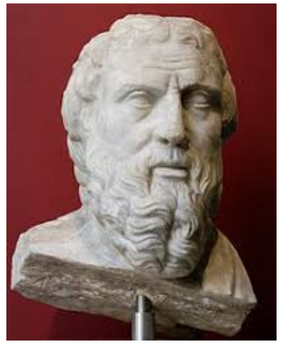


Crittografia classica: dall’antichità al Novecento



Steganografia

Storie,
Erodoto V sec. a.C.



1) *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 e disse 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.*

2) Testa rasata

Plinio il Vecchio
I sec. d.C.

3) Inchiostro invisibile dal lattice di titimabo (trasparente se asciutto, marrone al calore)

Crittografia classica: trasposizione

Vite parallele,
Plutarco (I-II sec. d.C.)

Scitala spartana

404 a.C. lo spartano Lisandro respinse il nemico persiano

Crittografia classica: sostituzione monoalfabetica

Vita dei Cesari,
Svetonio (II sec. a.C.)

Cifrario di Cesare

Alfabeto chiaro	a b c d e f g h i l m n o p q r s t u v z
Alfabeto cifrante	D E F G H I L M N O P Q R S T U V Z A B C
Testo chiaro	v e n i, v i d i, v i c i
Testo cifrante	B H Q N, B N G N, B N F N

$A = \{a, b, c, \ldots, z\}$ Alfabeto di *k* caratteri

j *chiave*

$$f : A \longrightarrow A$$
$$i \longmapsto i + j \ (mod\ k)$$

Mittente e destinatario devono possedere la chiave!

Con l'algoritmo di Grover le potremmo testare in pochi minuti!!!

Possiamo immaginare una versione meno semplice da decifrare: sostituzione del tutto generica.
21! possibili chiavi

Dalla sostituzione monoalfabetica a quella polialfabetica

Sostituzione monoalfabetica

Semplice

Affidabile

Resistette sino al Rinascimento

A metterla in crisi furono i lavori di linguistica operati dal mondo arabo

Frequenza delle lettere in italiano

·Lettera	·%	·Lettera	·%	·Lettera	·%
·a	·11,74	·h	·1,54	·q	·0,51
·b	·0,92	·i	·11,28	·r	·6,38
·c	·4,50	·l	·6,51	·s	·4,98
·d	·3,73	·m	·2,52	·t	·5,63
·e	·11,79	·n	·6,88	·u	·3,02
·f	·0,95	·o	·9,83	·v	·2,10
·g	·1,65	·p	·3,05	·z	·0,49

TRT QRDIAR NTMNFZ N GLPRIN

·Lettera	·Occor-renze	·Lettera	·Occor-renze	·Lettera	·Occor-renze
·A	·1	·H	·0	·Q	·1
·B	·0	·I	·2	·R	·4
·C	·0	·L	·1	·S	·0
·D	·1	·M	·1	·T	·3
·E	·0	·N	·4	·U	·0
·F	·1	·O	·0	·V	·0
·G	·1	·P	·1	·Z	·1

Esempio: **TRT QRDIAR NTMNFZ N GLPRIN**

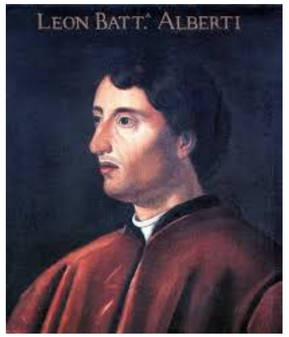
- Primo tentativo*:* inizio dalle lettere terminali di una parola e associando loro le vocali, in ordine di frequenza: **R = e, N = a , T = i, Z = o,**
- si ottiene **iei QeDIAe aiMNFZ a GLPeIa**
- Rivediamo alcune scelte (la prima parola non ha senso) **T = n**, (è la seconda consonante per frequenza: la prima è L che non sembra adatta), **R = o, Z = e,**
- Otteniamo **non QoDIAo anMaFe a GLPoIa**
- Ora introduciamo le consonanti più frequenti ancora mancanti (**l**, **r**,**t**,**s**,**c**) e reintroduciamo la **i**. Proviamo con **I = l**, **A = i**, **D = t**, **F = r, G = s** , **L=c:**

  non Qotlio anMare a scPola

  Posso modificare ancora **D = g** e continuare...

Crittografia classica: sostituzione polialfabetica

Leon Battista Alberti
XV secolo



Ebbe per primo l'idea di cifrare usando più di un alfabeto, ma non lo fece diventare una tecnica definita.

Blaise de Vigenère
XVI secolo

Chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Parola chiave:	M	O	N	T	E	M	O	N	T	E	M	O	N	T	E	M	O	N	T	E	M	O	N	T	E	M	O	N
Testo chiaro:	s	p	o	s	t	a	r	e	t	r	u	p	p	e	s	u	c	i	m	a	e	s	t					
Testo in cifra:	E	D	B	L	X	M	F	R	M	V	G	D	C	X	W	G	Q	V	F	E	Q	G	G					

Rimase inviolato fino a metà Ottocento
(Storia dei crittogrammi di Bale!!!)

Crittografia classica: il Santo Graal

Se sommiamo (mod 2) due testi cifrati otteniamo la somma dei due testi in chiaro perdendo la casualità della chiave!

Il limite del metodo Vigenère stava nella ciclicità della parola chiave

Gilbert Vernam

1917

Cifrario di Vernam

Cifratura inviolabile

1. il testo in chiaro è scritto come una sequenza binaria di 0 e 1;
2. la chiave segreta è una sequenza binaria completamente casuale della stessa lunghezza del testo in chiaro;
3. il testo cifrato si ottiene aggiungendo la chiave segreta somma modulo 2 al testo in chiaro

001010011	plain text,
100111010	secret key,
101101001	cypher text.

Pertanto, il problema principale della crittografia non è la trasmissione del testo cifrato ma la distribuzione della chiave segreta. Questa distribuzione richiede un qualche tipo di "corriere fidato"; cioè, il problema della segretezza della comunicazione viene semplicemente trasferito al problema della segretezza della chiave. Il problema è che Eve potrebbe, almeno in linea di principio, trovare un modo per leggere la chiave senza lasciare alcuna traccia della sua azione.

L'inviolabilità è data dalla causalità della chiave a meno di utilizzarla una sola volta (*one time pad*).

Sommando di nuovo la chiave si ottiene il testo in chiaro

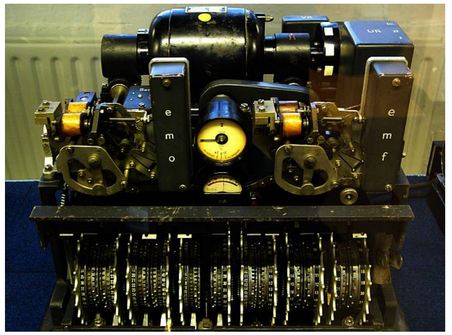
Crittografia classica: secondo Novecento

L'utilizzo monouso rendeva il cifrario di Vernam non utilizzabile in concreto

Tra le due grandi guerre l'aspetto elettro-meccanico-automatico aveva preso il sopravvento.

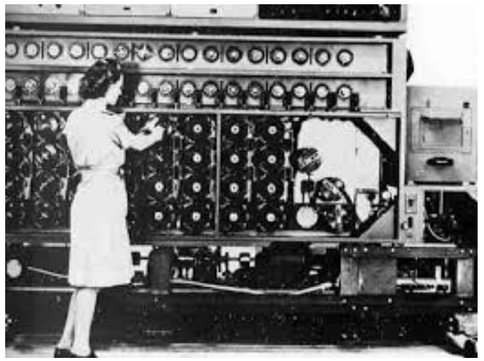
CIFRATURA AUTOMATICA

Enigma

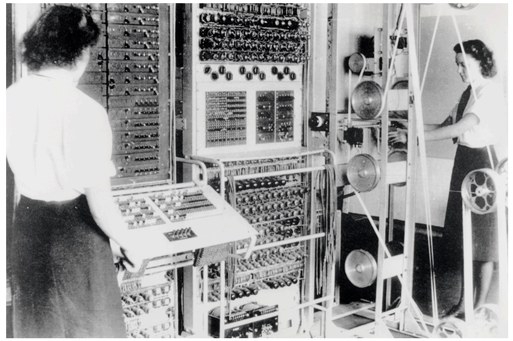


Lorenz SZ40

DECIFRATURA AUTOMATICA (in parte!)

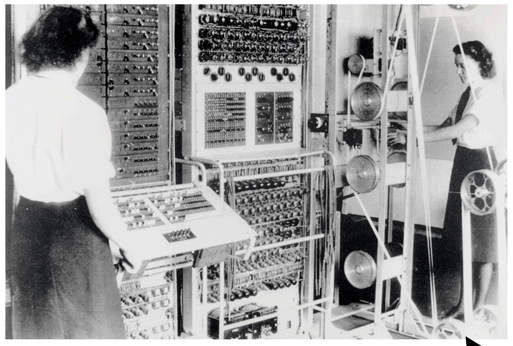


Macchina per decifrare Enigma



Colossus

Crittografia classica: secondo Novecento



Colossus

Max Newman, matematico

Tommy Flowers, ingegnere

dicembre, 1943 → **Fine guerra** *distrutta*, 1945

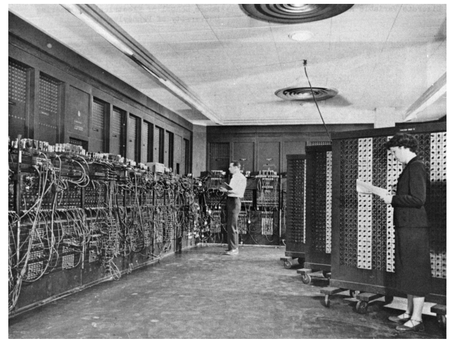
MACCHINA UNIVERSALE DI TURING

NASCITA DEL COMPUTER

Al termine della guerra il procedimento computerizzato si era imposto!

J. Presper Eckert e John W. Mauchly

Per tradizione è il primo computer

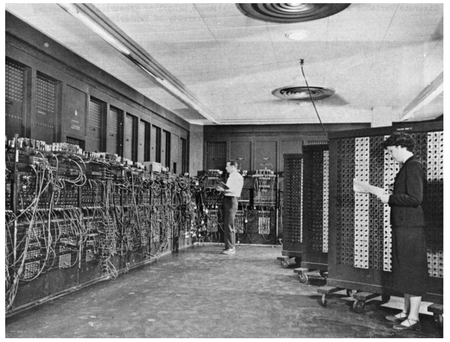


ENIAC
Electronic Numerical Integrator And Calculator

Crittografia classica: nascita del computer

Enigma

$\neq$



ENIAC

1.Una cifratrice meccanica o elettromeccanica ha una potenza limitata, perché con queste tecnologie le dimensioni, il costo e la tendenza a guastarsi aumentano vertiginosamente col crescere della complessità, mentre un computer può **simulare** una cifratrice estremamente complicata con alta affidabilità

2. La seconda differenza è una semplice questione di velocità. L'elettronica opera molto più rapidamente di uno scambiatore elettromeccanico.

3. La terza, e forse più importante, differenza è che un computer scambia e traspone numeri anziché caratteri alfabetici.

Crittografia classica: crittografia con calcolatori

3. La terza, e forse più importante, differenza è che un computer scambia e traspone numeri anziché caratteri alfabetici.

Matematici e scienziati prendono il posto dei linguisti.

Prima della cifratura un messaggio dev'essere convertito in cifre binarie

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

American Standard Code for Information Interchange (ASCII)

Ciao = 1000011 1001001 1000001 1001111

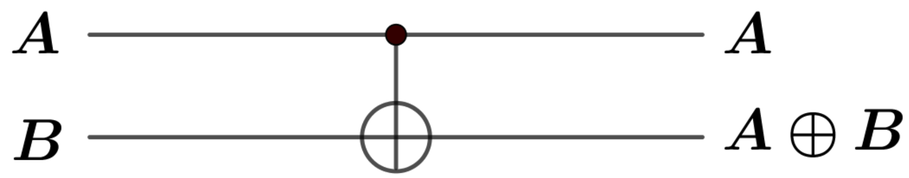
Crittografia classica: crittografia con calcolatori

Versione computerizzata di crittografia per sostituzione

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

Messaggio	Ciao
Messaggio ASCII	10000111001001100000011001111
Chiave = rosa	10100101001111101001110000001
Testo cifrato	00100010000110001001000011110

Metodo riservato ai governi e alle forze armate, ossia chi disponeva di computer.



Crittografia classica: sviluppo tecnologico

Sviluppo tecnologico rapido:

Transistor 1947 Bell Labs: Walter Brattain e John Bardeen
1948 William Shockley (transistor a giunzione)

NOBEL (1956)

Metodo riservato ai governi e alle forze armate, ossia chi disponeva di computer.

IBM 1953 primi elaboratori

Computer IBM 650

Uso dei calcolatori si diffuse soprattutto presso i privati rese necessario lo sviluppo della crittografia per messaggi al proprio interno, ma soprattutto verso l' esterno.

Circuito integrato 1959 Robert Noyce, Kurt Lehovec

Robert Noyce

Crittografia classica: sistema crittografico standard

15 maggio 1973

Invita ufficialmente ad avanzare proposte per l'adozione di un sistema crittografico standardizzato, che consentisse lo scambio di informazioni cifrate tra tutti gli operatori economici.

64 bits

LUCIFER IBM

"*Immaginiamo una massa soda di acqua e farina sulla quale si sia scritto un messaggio. Dapprima essa è divisa in blocchi di 64 cm. Poi nell'ambito di un blocco un mezzo blocco da 32 cm è separato, appiattito, arrotolato, aggiunto all'altro mezzo blocco e riplasmato in modo da formare un nuovo blocco da 64 cm. Il procedimento è ripetuto sedici volte, dopo di che si passa al blocco successivo, finché tutto l'impasto sia stato lavorato. Il testo in cifra può quindi essere inviato al destinatario, che lo volgerà in chiaro invertendo il processo.*"

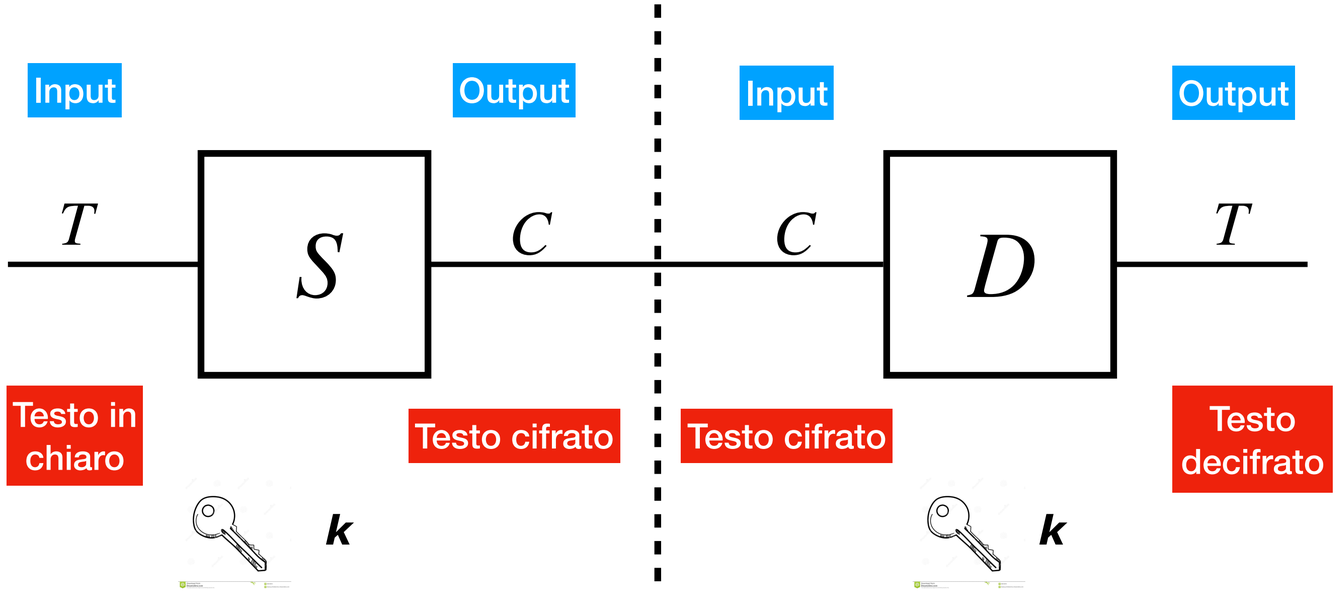
I particolari della funzione deformante possono mutare a ogni messaggio, in quanto dipendono dalla chiave concordata dal mittente e dal destinatario. In altre parole, lo stesso messaggio può essere cifrato in un'infinità di modi a seconda della chiave scelta. Nella crittografia computerizzata le chiavi sono essenzialmente numeri. Perciò la selezione della chiave si riduce alla scelta, di comune accordo, di un numero da parte del mittente e del destinatario.

1976, 23 novembre

DES (Data Encryption Standard)

Crittografia classica: distribuzione delle chiavi

Crittografia a chiave privata



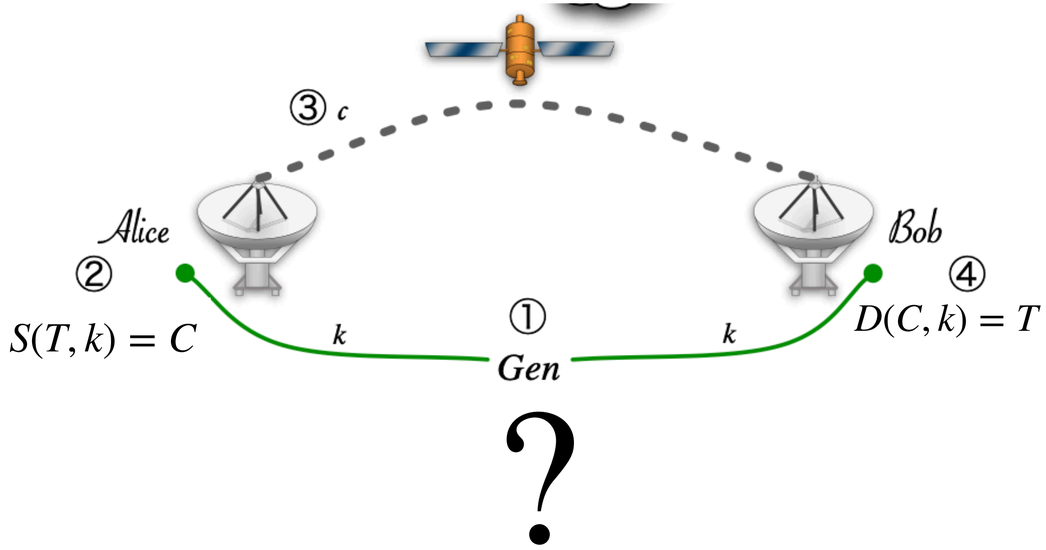
$S(T,k) = C$

Chypher Text

$D(C,k) = T$

Algoritmo di crittografia Simmetrico

Algoritmo di decrittazione



?

Il problema più grande rimaneva quello della ***distribuzione delle chiavi***

Crittografia classica: distribuzione delle chiavi

Il problema più grande rimaneva quello della ***distribuzione delle chiavi***

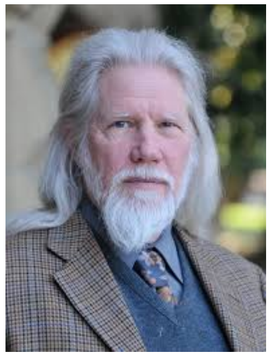
Esiste un unico modo sicuro: ***brevi manu***

Anni ’70 le banche assumevano personale specializzato per trasportare chiavi negli USA. Naturalmente i costi crebbero fino a rendere impraticabile il sistema.

La soluzione del problema di distribuzione delle chiavi è effettivamente il risultato più importante nella storia della crittografia dopo l’invenzione della cifratura monoalfabetica

Postulato crittografia: per mandare un messaggio cifrato e far in modo che possa essere decrittato, occorre generare una chiave privata che venga consegnata segretamente sia al mittente che al destinatario.

Crittografia classica: fine di un postulato!



Whitfield Diffie

Martin Hellman

Prefigurava un mondo interconnesso nel quale la privacy sarebbe stata fondamentale

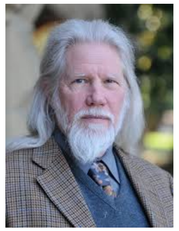
"Capì che le persone comuni avrebbero un giorno posseduto un computer, e che i computer avrebbero comunicato tra loro per mezzo delle linee telefoniche."

1974 tiene un seminario sul problema dell'attacco alle chiavi ai centri IBM

«Avevo promesso a mia moglie di tornare presto a casa per badare ai bambini, perciò lui mi accompagnò e cenammo insieme. Se ne andò verso mezzanotte. Le nostre personalità sono molto diverse - lui è molto più "alternativo" di me - ma alla fine questa diversità si è rivelata molto complementare. Per me fu come una boccata d'aria fresca. Lavorare nel più completo isolamento era stato veramente duro» (Hellmann).

Ralph Merkle

Crittografia classica: fine di un postulato!



Whitfield Diffie

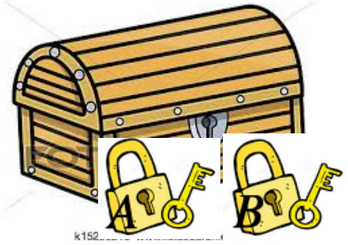
Martin Hellman

Ralph Merkle

Postulato crittografia: per mandare un messaggio cifrato e far in modo che possa essere decrittato, occorre generare una chiave privata che venga consegnata segretamente sia al mittente che al destinatario.

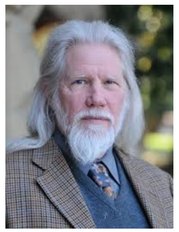
Alice

Bob



Risolto?

Crittografia classica: fine di un postulato!



Whitfield Diffie

Postulato crittografia: per mandare un messaggio cifrato e far in modo che possa essere decrittato, occorre generare una chiave privata che venga consegnata segretamente sia al mittente che al destinatario.

Martin Hellman

PROBLEMA: l'ordine con cui la cifratura e la decifrazione viene eseguita

Ralph Merkle

L'ordine dell'apertura dei lucchetti è ininfluente a differenza della decifrazione

Chiave di Alice

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

Chiave di Bob

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

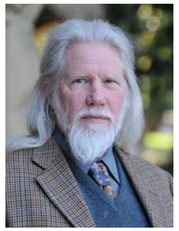
Messaggio	ci	vediamo	all	una	
Cifrato da Alice	SV	RGUVHYB	HOO	QJH	
Ricifrato da Bob	HD	YNSDOLP	OBB	REO	
Decifrato da Alice	AJ	MQCJLZP	LOO	VKL	
Decifrato da Bob	ei	cnaiywb	yhh	zxy	

Il problema era trovare una funzione matematica in grado di comportarsi come il lucchetto con le chiavi!

Funzioni esponenziali mod n

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
$3^x \pmod 7$	3	2	6	4	5	1

Crittografia classica: fine di un postulato!
1976

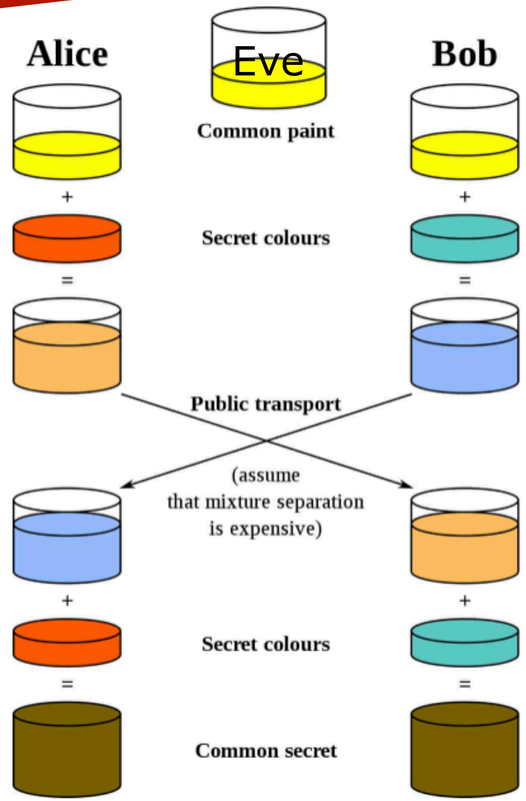


Whitfield Diffie

Martin Hellman

Ralph Merkle

Postulato crittografia: per mandare un messaggio cifrato e far in modo che possa essere decrittato, occorre generare una chiave privata che venga consegnata segretamente sia al mittente che al destinatario.



$$Y^x (mod\ P),\ P\ primo\ e\ Y < P$$

$$7^x (mod\ 11)$$

$A = 3$	$B = 6$
$\alpha = 7^3 (mod\ 11) = 2$	$\beta = 7^6 (mod\ 11) = 4$
$\beta = 4$	$\alpha = 2$
$\beta^3 (mod\ 11)$	$\alpha^6 (mod\ 11)$
$4^3 (mod\ 11) = 9$	$2^6 (mod\ 11) = 9$

Crittografia classica: crittografia a chiave pubblica

Mary Fisher

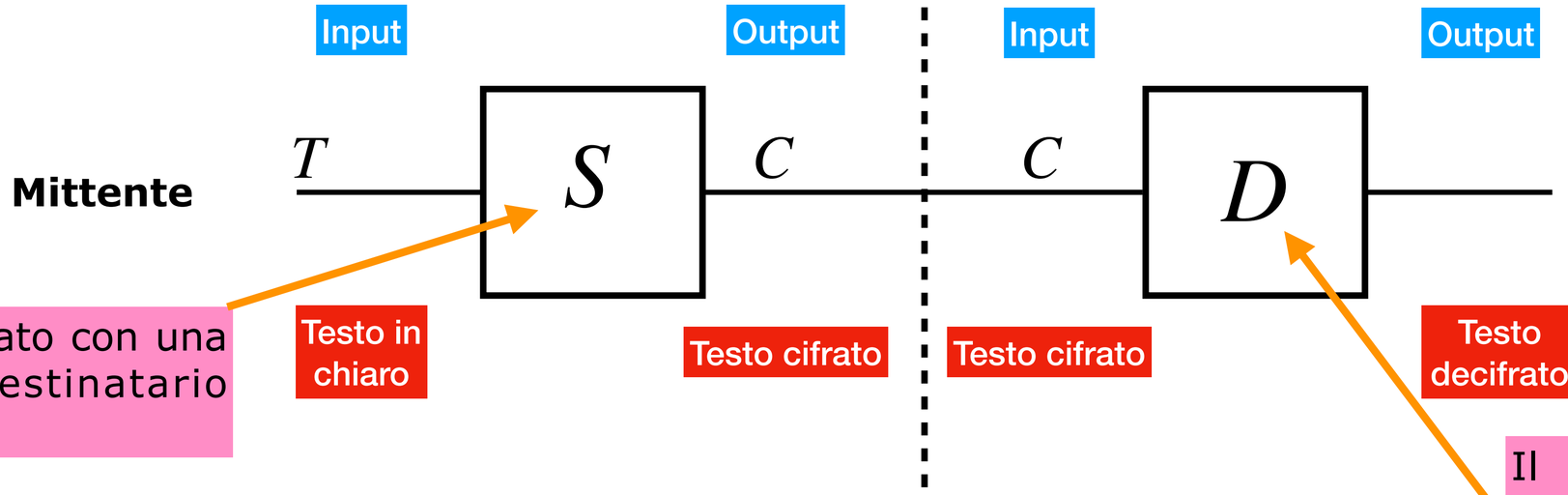
Whitfield Diffie

«Whit mi aspettava sulla soglia», ricorda l'archeologa. «Affermò di avere qualcosa da comunicarmi, e aveva una buffa espressione. Entrai, e lui disse: "Siediti, per piacere, voglio parlarti. Credo di aver fatto una grande scoperta - qualcosa a cui nessun altro aveva ancora pensato". In quel momento, ebbi come l'impressione che il mondo si fosse fermato. Mi sentivo dentro la trama di un film hollywoodiano.»

1975

Cifratura asimmetrica

Il destinatario genera una chiave per cifrare che rende pubblica e che usa un qualsiasi mittente. Ma solo il destinatario possiede la chiave privata per decifrare.

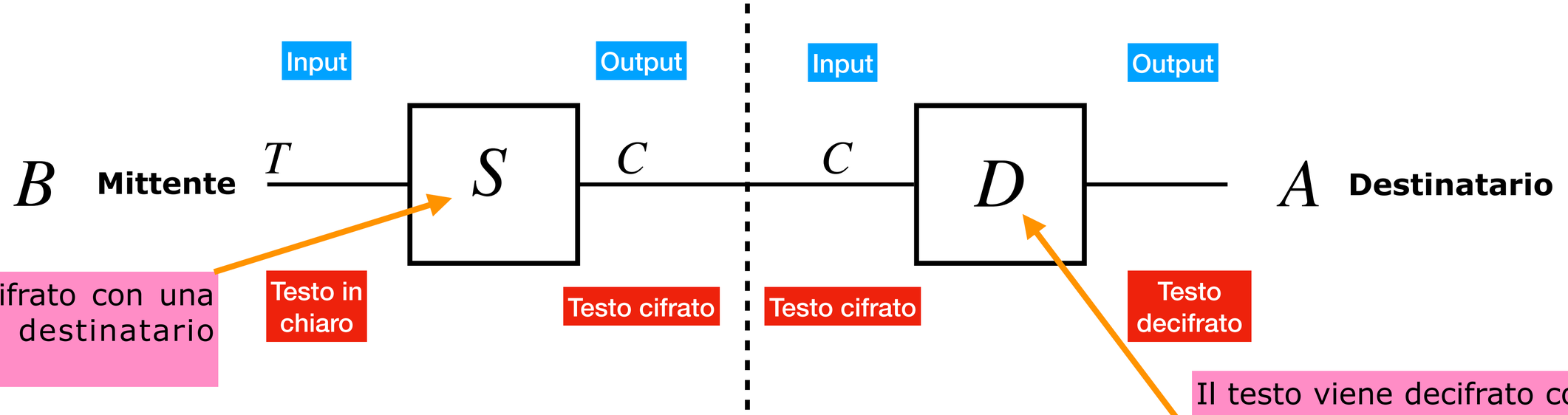


Il testo viene crittato con una chiave che il destinatario rende pubblica

Il testo viene decrittato con una chiave privata del destinatario

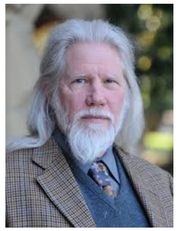
Crittografia classica: crittografia a chiave pubblica

Cifratura asimmetrica



Il testo viene cifrato con una chiave che il destinatario rende pubblica

Il testo viene decifrato con una chiave privata del destinatario



Whitfield Diffie

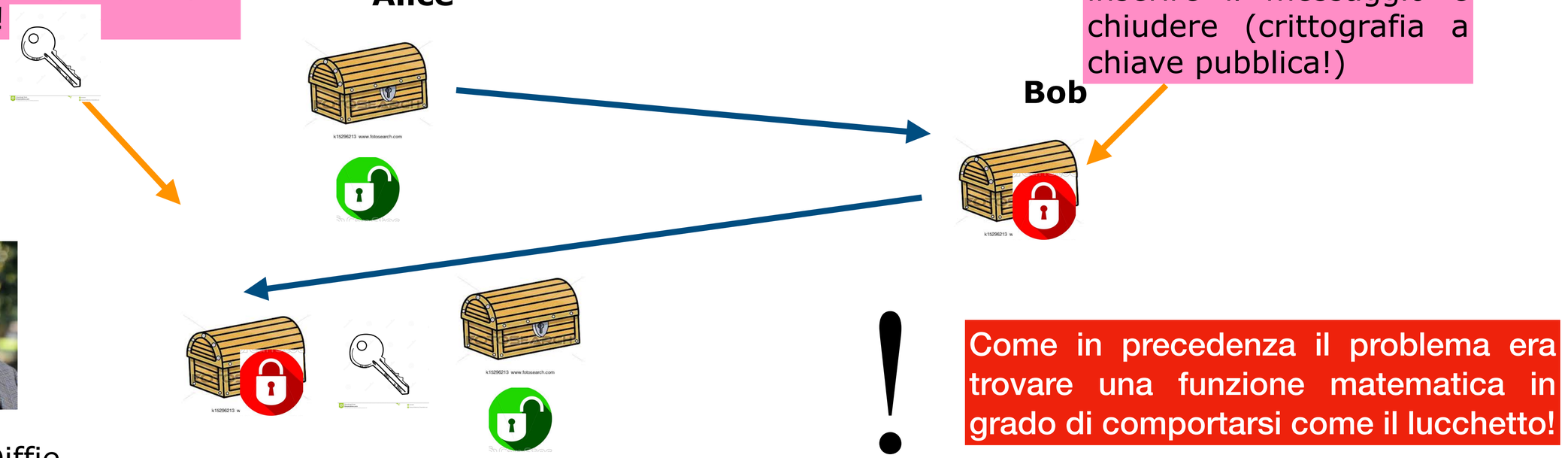
Il vantaggio rispetto al protocollo precedente risiede ad esempio nel fatto che non è richiesto che il destinatario e mittente debbano aspettare di avere informazioni reciproche per cifrare il messaggio. Bob può cifrare il messaggio con la chiave pubblica di Alice.

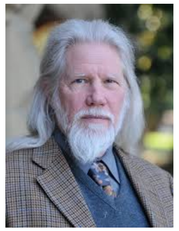
Crittografia classica: crittografia a chiave pubblica

Cifratura asimmetrica

Alice prepara le scatole dove chiunque può inserire il messaggio cifrato (chiave pubblica), ma tiene per sé l'unica chiave (privata) che riapre il lucchetto!

Una volta che A ha inviato una scatola con il lucchetto Bob può inserire il messaggio e chiudere (crittografia a chiave pubblica!)





Whitfield Diffie

Come in precedenza il problema era trovare una funzione matematica in grado di comportarsi come il lucchetto!

Crittografia classica: crittografia a chiave pubblica

Cifratura asimmetrica

Ron Rivest - Adi Shamir
Leonard Adleman

Nell'aprile 1977 Rivest, Shamir e Adleman avevano festeggiato la Pasqua a casa di uno studente, e bevuto parecchio vino. Verso mezzanotte, erano tornati alle rispettive abitazioni. Incapace di prender sonno, Rivest si era sdraiato sul letto e aveva aperto un libro di matematica. Cominciò a rimuginare la questione che lo assillava da settimane: è possibile realizzare una cifratura asimmetrica? è possibile concepire una funzione unidirezionale, invertibile per chi disponga di particolari informazioni? Di colpo, la nebbia cominciò a diradarsi ed egli intravide la soluzione.

1977

"Il mattino seguente consegnò lo scritto ad Adleman, che si preparò a farlo a brandelli come di consueto; ma questa volta non trovò sbagli. La sola critica che gli venne in mente riguardava l'elenco degli autori. «Pregai Ron di cancellare il mio nome dall'articolo», racconta. «Gli dissi che la scoperta era sua, non mia. Ron rifiutò e ne nacque una discussione. Stabilimmo che sarei tornato a casa, ci avrei dormito su e poi gli avrei comunicato la mia decisione. Il giorno dopo suggerii a Ron di lasciare il mio nome, ma di collocarlo in fondo alla lista. Rammento di aver pensato dentro di me che difficilmente sarei stato coautore di un articolo meno interessante.» Adleman non avrebbe potuto essere più fuori strada. Il sistema che quei fogli tennero a battesimo, soprannominato RSA (Rivest, Shamir, Adleman) anziché ARS, sarebbe diventato la cifratura più influente della moderna crittografia."

Crittografia classica: protocollo RSA

Cifratura asimmetrica

Ron Rivest - Adi Shamir
Leonard Adleman

Generazione chiavi

1. si scelgono due numeri primi p e q
2. si calcola $n = pq$
3. si calcola la funzione di Eulero $\varphi(n) = (p-1)(q-1)$
4. si sceglie un numero e tale che $1 < e < \varphi(n)$ coprimo con $\varphi(n)$
5. si calcola d come l'inverso moltiplicativo di e modulo $\varphi(n)$.
   i.e $ed \equiv 1 \mod \varphi(n)$

La coppia (e, n) è detta *chiave pubblica* mentre (d, n) è detta *chiave privata*

n è pubblico!

Crittografia classica: protocollo RSA

Cifratura asimmetrica

Ron Rivest - Adi Shamir
Leonard Adleman

Cifratura

Per cifrare il messaggio m occorre calcolare il cyphertext con la chiave pubblica

$$c \equiv m^e \bmod n. \qquad (e, n) \quad \text{chiave pubblica}$$

Decifratura

Per decifrare il messaggio c si ricalcola il testo in chiaro con la chiave privata

$$m \equiv c^d \bmod n. \qquad (d, n) \quad \text{chiave privata}$$

Crittografia classica: protocollo RSA

Cifratura asimmetrica

1. si scelgono due numeri primi p e q
2. si calcola $n = pq$
3. si calcola la funzione di Eulero $\varphi(n) = (p-1)(q-1)$
4. si sceglie un numero e tale che $1 < e < \varphi(n)$ coprimo con $\varphi(n)$
5. si calcola d come l'inverso moltiplicativo di e modulo $\varphi(n)$. i.e $ed \equiv 1 \mod \varphi(n)$

La coppia (e, n) è detta *chiave pubblica* mentre (d, n) è detta *chiave privata*

Ron Rivest - Adi Shamir
Leonard Adleman

Esempio:

- Generazione delle chiavi
  1. $p = 5$ e $q = 11$ dunque $n = 55$
  2. $\varphi(n) = (p-1)(q-1) = 40$
  3. $e = 7 \rightarrow e < 40,\ \mathrm{MCD}(e, 40) = 1$
  4. $d = 23 \rightarrow 7 * 23 = 161 \equiv 1 \mod 40$

  chiave pubblica $\rightarrow (7, 55)$ n è pubblico!
  chiave privata $\rightarrow (23, 55)$
- Cifratura - decifratura
- $m = 18$
  1. $m^e = 18^7 \equiv c \equiv 17 \mod 55$
  2. $c^d = 17^{23} \equiv m \equiv 18 \mod 55$

Per cifrare il messaggio m occorre calcolare il cyphertext con la chiave pubblica

$$c \equiv m^e \mod n.$$

Per decifrare il messaggio c si ricalcola il testo in chiaro con la chiave privata

$$m \equiv c^d \mod n.$$

Crittografia classica: RSA divulgativo

Quella che segue è una spiegazione divulgativa dei passaggi matematici alla base della RSA, per quanto riguarda tanto la genesi quanto l'interpretazione del crittogramma.

(1) Alice sceglie due numeri primi molto grandi, p e q. Per semplificare il nostro esempio non attribuiremo a p e q valori enormi, e supporremo che Alice abbia scelto $p = 17$, $q = 11$. Questi numeri dovranno essere tenuti segreti.

(2) Alice moltiplica p e q, e ottiene N. In questo caso $N = 187$. Poi, Alice deve scegliere un altro numero, che chiameremo e; supponiamo che scelga $e = 7$.

(e e $(p - 1) \times (q - 1)$ dovrebbero essere primi tra di loro, ma questo è un dettaglio tecnico.)

(3) A questo punto, Alice è libera di pubblicare e e N in un elenco accessibile a tutti. Poiché e e N sono necessari alla cifratura, devono essere disponibili a chiunque voglia inviarle un messaggio protetto tramite la RSA. e e N sono le «chiavi pubbliche» di Alice. (Oltre a far parte della chiave per cifrare di Alice, e potrebbe far parte di quella di chiunque altro. Tuttavia, ogni utente della RSA deve avere un proprio ed esclusivo valore di N, che dipende dai valori scelti per p e q).

(4) Per cifrare un messaggio, questo deve innanzitutto essere trasformato in un numero M. Per esempio, una parola viene trasformata in cifre binarie ASCII, e le cifre binarie corrispondono a un numero decimale. M è quindi cifrato in modo da generare C, il crittogramma, secondo la formula:

$$C = M^e \pmod N$$

(5) Supponiamo che Bob voglia mandare ad Alice un semplice bacio epistolare: nient'altro che la lettera X. In codice ASCII X è 1011000, cioè 88 in notazione decimale. Quindi, $M = 88$.

(6) Per crittare il messaggio, Bob comincia col procurarsi la chiave pubblica di Alice, e constata che $N = 187$ e $e = 7$. Così egli può utilizzare la formula necessaria a crittare il messaggio di Alice. Per $M = 88$, la formula dà:

$$C = 88^7 \pmod{187}$$

Crittografia classica: RSA divulgativo

(7) Non conviene cercare di stabilire direttamente il valore di quest'espressione con una calcolatrice, perché è improbabile che il display possa contenere il risultato. Tuttavia, c'è uno stratagemma che permette di gestire facilmente gli esponenti in aritmetica dei moduli.

Da $7 = 4 + 2 + 1$, segue che:

$88^7 \pmod{187} = [88^4 \pmod{187} \times 88^2 \pmod{187} \times 88^1 \pmod{187}] \pmod{187}$

$88^1 = 88 = 88 \pmod{187}$

$88^2 = 7{,}744 = 77 \pmod{187}$

$88^4 = 59{,}969{,}536 = 132 \pmod{187}$

$88^7 = 88^1 \times 88^2 \times 88^4 = 88 \times 77 \times 132 = 894{,}432 = 11 \pmod{187}$

Bob può quindi inviare ad Alice il testo cifrato, $C = 11$.

(8) Sappiamo che le funzioni esponenziali in aritmetica dei moduli sono unidirezionali; è quindi molto difficile ritrovare M, il messaggio originale, partendo da $C = 11$. Perciò, Eva non è in grado di decifrare il messaggio.

(9) Alice, al contrario, può decifrare il messaggio perché è in possesso di informazioni speciali: i valori di p and q. Ella calcola un numero speciale, d, la sua personale chiave per la decifrazione, nota anche come chiave privata. Il numero d è ottenuto per mezzo della formula seguente:

$e \times d = 1 \pmod{(p\text{-}1) \times (q\text{-}1)}$

$7 \times d = 1 \pmod{16 \times 10}$

$7 \times d = 1 \pmod{160}$

$d = 23$

(La deduzione del valore di d non è immediata, ma un procedimento noto come algoritmo di Euclide permette ad Alice di trovare d rapidamente e facilmente.)

(10) Per decifrare il messaggio, Alice usa semplicemente questa formula:

$M = C^d \pmod{187}$

$M = 11^{23} \pmod{187}$

$M = [11^1 \pmod{187} \times 11^2 \pmod{187} \times 11^4 \pmod{187} \times 11^{16} \pmod{187}] \pmod{187}$

$M = 11 \times 121 \times 55 \times 154 \pmod{187}$

$M = 88 =$ «*X*» in codice ASCII.

Crittografia classica: protocollo RSA

Cifratura asimmetrica

Ron Rivest - Adi Shamir
Leonard Adleman

Generazione chiavi

1. si scelgono due numeri primi p e q
2. si calcola $n = pq$

La difficoltà in un eventuale tentativo di decifrazione di Eve sta proprio nel fatto fatto che sia molto semplice moltiplicare numeri primi, ma molto meno, dato un numero, ricavarne la fattorizzazione!

! NUMERI PRIMI

Crittografia classica: protocollo RSA

Cifratura asimmetrica

! NUMERI PRIMI

Classicamente il miglior algoritmo di fattorizzazione di un numero N in primi richiede un tempo esponenziale: non risolubile!

Chi poteva garantire che non si sarebbe trovato un algoritmo più efficiente?

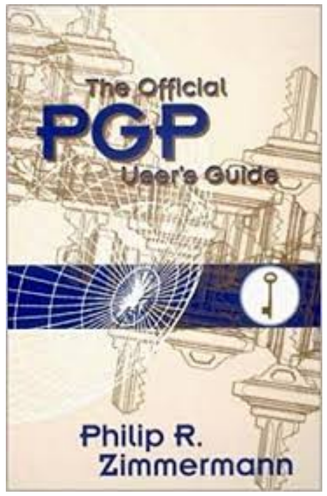
Shor 1994

Algoritmo quantistico di fattorizzazione troppo complesso per il nostro percorso!

Crittografia classica: un inciso da approfondire

Phil Zimmermann

PGP *Pretty Good Privacy*



Crittografia RSA democratica

1991

Crittografia quantistica

La crittografia quantistica si inserisce nel contesto dei sistemi a chiave segreta

1. Cifratura e decifratura pubbliche
2. Chiave casuale segreta

   $$C = M \oplus K$$

   dove C è la cifratura, M il messaggio e K la chiave, tutto espresso naturalmente in forma di bit.
3. Canale pubblico:
   - accessibile a chiunque
   - intercettazione passiva possibile
   - intercettazione attiva supposta non possibile[4]
4. Canale privato:
   - molto sicuro
   - intercettazione difficile
   - difficile da realizzare

In linea di principio chiunque può intercettare senza essere scoperto. Classicamente è possibile!

L'intercettazione è un atto di misurazione. Possiamo sfruttare le proprietà dei sistemi quantistici e il fatto che la misurazione perturba il sistema.

Crittografia quantistica: fotoni

Stephen Wiesner

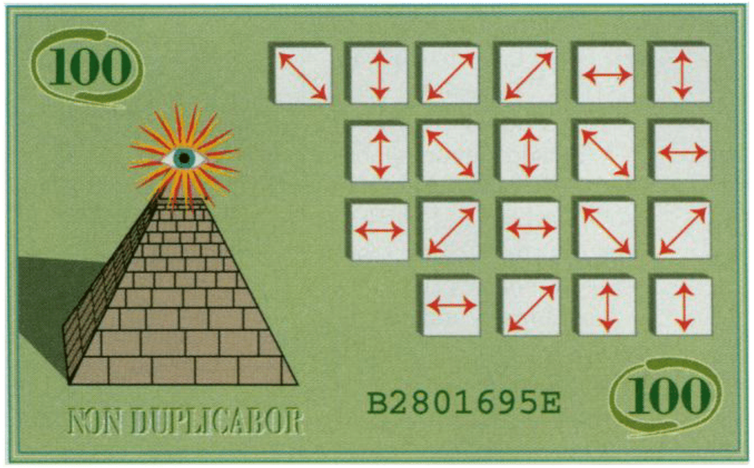
Quantum money

1969

L’idea è quella di inserire delle piccole celle all’interno delle banconote polarizzate nei quattro modi in figura con intrappolato un fotone polarizzato in ciascuna. L’eventuale falsario non potrebbe determinare l’orientamento della polarizzazione (grazie al teorema di non clonazione!)…

Crittografia quantistica: fotoni

Stephen Wiesner



Quantum money

1969

Charles Bennett

Pubblicazione

1983

Crittografia quantistica: fotoni

Charles Bennett

Jilles Brassard

Quantum Cryptography

Charles H. Bennett, Gilles Brassard and Artur K. Ekert

1984

Protocollo BB84

Sfortunatamente inviare una chiave privata in modo sicuro è difficile in quanto richiede l'uso di qualche altro schema di crittografia come l'RSA che è teoricamente violabile. In alternativa entrambe le parti possono incontrarsi faccia a faccia per scambiarsi la chiave, ma questo a volte non è fattibile. Fortunatamente la distribuzione quantistica delle chiavi (QKD) propone una soluzione per questo.

Necessità di un protocollo di distribuzione di chiavi quantistico

Vernman Cipher

The Vernman cipher (one time pad) is theoretically unbreakable if implemented correctly. It requires three things:

1. A private key that is shared between both parties
2. That the key be longer than or equal to the size of the message
3. A new key to be used for each message sent

```
      H       E       L       L       O  message
    7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= 30      16      13      21      25     message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) (message + key) mod 26
       E       Q       N       V       Z  → ciphertext
```

Figure 1: Vernman cipher encryption [1]

In this example the each number in the key is used to move a letter across the alphabet.
Note: the first 'L' in HELLO is changed to 'N' and the second 'L' to 'V' (this makes cryptanalysis difficult)

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

Figure 2: Vernman cipher decryption [1]

Unfortunately sending a private key securely is difficult as it requires the use of some other encryption scheme such as RSA which is theoretically crackable. Alternatively both parties can meet face-to-face to exchange the key, but this is sometimes unfeasible. Luckily quantum key distribution (QKD) proposes a solution for this.

Crittografia quantistica: fotoni

Charles Bennett

Jilles Brassard

Quantum Key Distribution

Quantum Key distribution is a method of securely sending private keys between two parties (Alice and Bob in the example below). This is useful for implementation of the Vernman cipher.

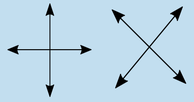


Figure 6: Polarisation filters (rectilinear and diagonal)

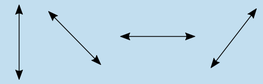
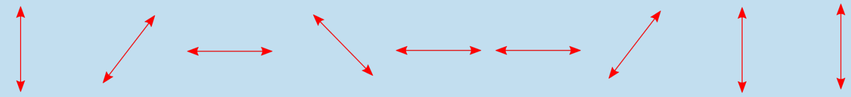
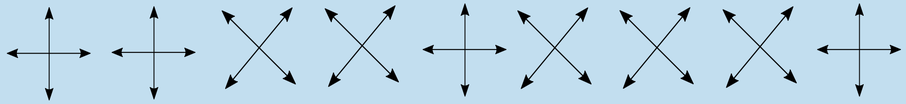


Figure 7: Polarised photons

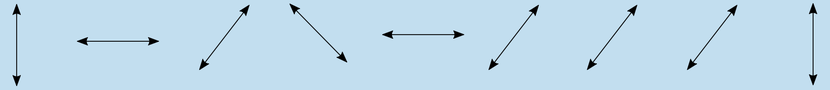
1. Alice prepares a set of polarised photons using a random sequence of rectilinear and diagonal polarising filters (The sequence is only known to Alice)



2. Bob receives the photons and uses another random sequence of polarising filters to measure the photons



3. Bob gets these measurements.



Crittografia quantistica: fotoni

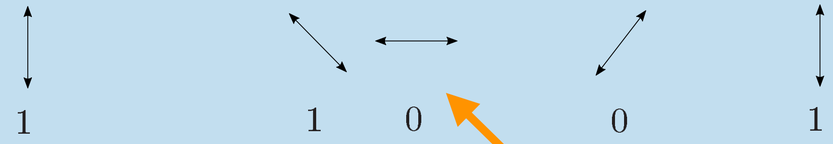
Charles Bennett

Jilles Brassard

4. Bob now communicates with Alice (can be through an open channel) the polarisation filters used and Alice tells him which were correct. All the incorrect measurements are thrown out and a subset of the measurements are also thrown out to check for any tempering in the quantum channel (this can also be done by checking the parity of multiple subsets).

✓ ✓ ✓ ✓ ✓

5. The correct remaining polarisations can now be used as binary which make up the private key.



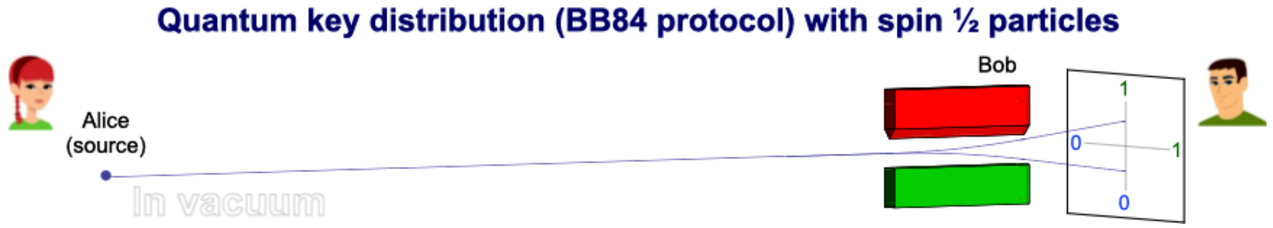
Note: Figures above are adapted from [2]

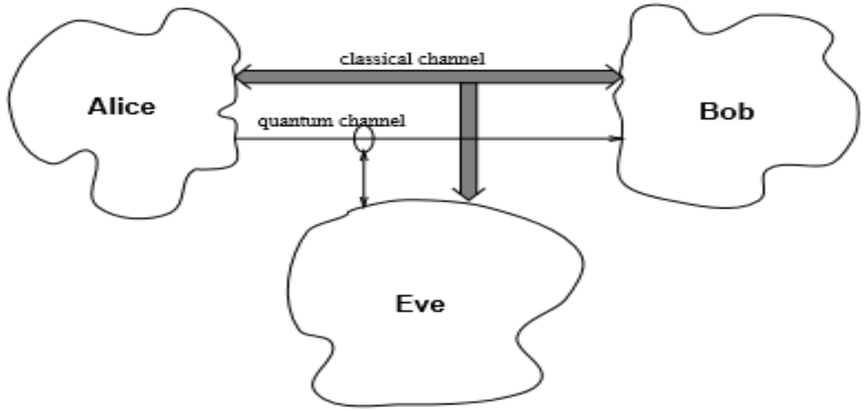
CHIAVE

Un altro punto debole nell'implementazione del cifrario di Vernman è la conservazione sicura delle chiavi. Questo può essere risolto grazie all'effetto EPR dove un atomo sfericamente simmetrico emette due fotoni in direzioni opposte (entrambi contenenti polarizzazioni opposte)
1. Alice prepara delle coppie di fotoni EPR, tenendo una di ogni coppia per sé e dando l'altra a Bob.
2. Alcuni dei fotoni sono misurati immediatamente per controllare se ci sono intercettazioni.
3. Una volta che Alice e Bob hanno bisogno di comunicare, possono misurare un sottoinsieme di fotoni (usando lo stesso tipo di polarisation Iter) e se la memorizzazione non è stata disturbata, Alice e Bob otterranno sempre misurazioni opposte di tutte le coppie.
4. I fotoni rimanenti vengono misurati per recuperare la chiave privata.

Crittografia quantistica: spin

Protocollo BB84 per generare una chiave con elettroni





Quattro stati e due alfabeti binari: $|0\rangle \; e \; |1\rangle$ alphabeto-z

$|0\rangle_x = |+\rangle \; e \; |1\rangle_x = |-\rangle$ alphabeto-x

Lancia una moneta

1. **Alice** genera una sequenza random di 0 e 1;
2. **Alice** codifica: 0 con $|0\rangle \; o \; |0\rangle_x$

   1 con $|1\rangle \; o \; |1\rangle_x$

1	0	0	0	1	1	0	1	0	1
x	z	x	z	x	x	x	z	z	x
$\|1\rangle_x$	$\|0\rangle$	$\|0\rangle_x$	$\|0\rangle$	$\|1\rangle_x$	$\|1\rangle_x$	$\|0\rangle_x$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle_x$

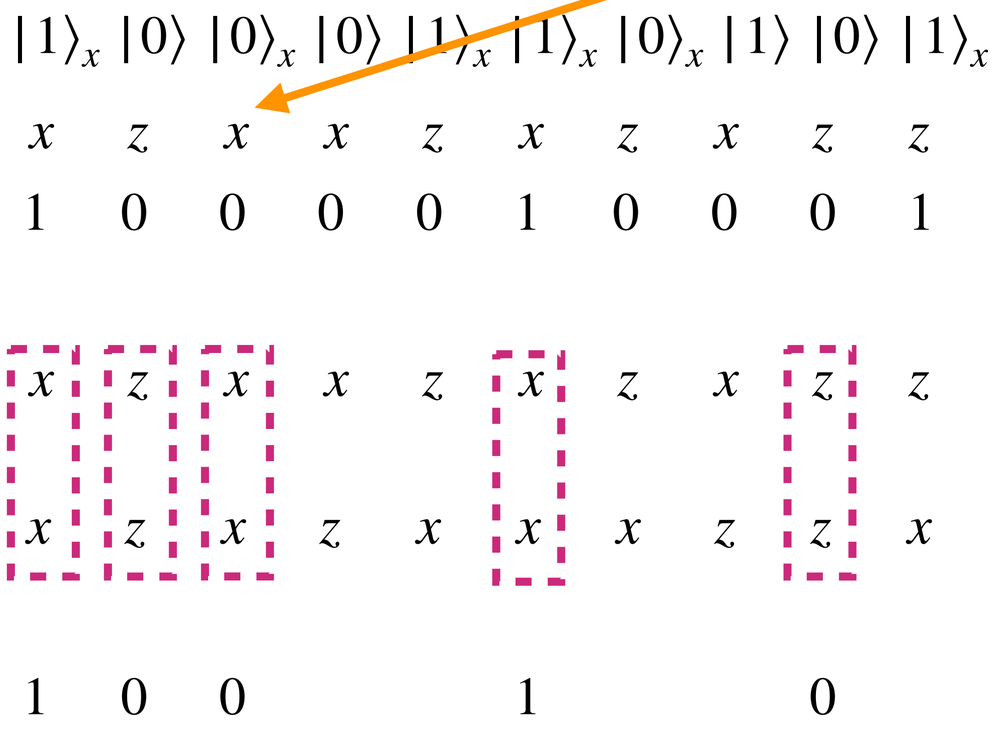
Da questo momento in poi A e B comunicano solo informazione classica su un canale pubblico

Crittografia quantistica: spin

Protocollo BB84 per generare una chiave con elettroni

Lancia una moneta

3. **Alice** invia a Bob mediante il canale pubblico la stringa di qubit risultante;
4. **Bob** effettua una misurazione random di ogni qubit nelle due basi del proprio alfabeto; tali esiti sono i bits di Bob;
5. **Bob** comunica ad Alice l'alfabeto utilizzato per ogni misurazione dei qubit, senza comunicare l'esito;
6. **Alice** comunica a Bob l'alfabeto utilizzato per ogni qubit trasmesso, senza comunicare l'esito;
7. **Alice** e **Bob** cancellano i bits corrispondenti al caso in cui abbiano scelto alfabeti diversi;



Crittografia quantistica: spin

Protocollo BB84 per generare una chiave con elettroni

8. **Alice** e **Bob** utilizzano la stringa, comune ad entrambi, come chiave crittografica

1 0 0 1 0

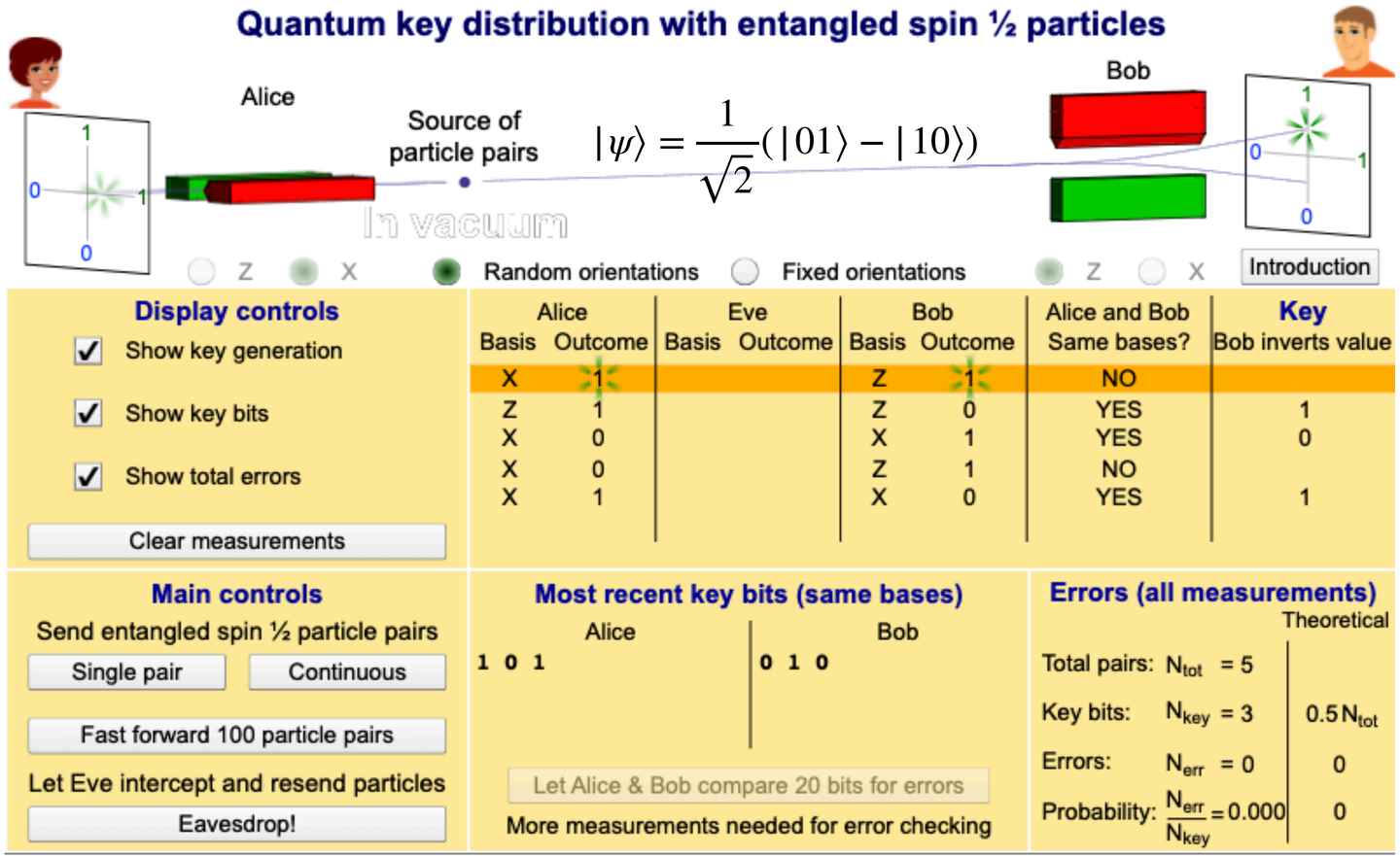
La stringa ottenuta è totalmente casuale perché casuale è la determinazione iniziale dell'alfabeto di Alice! Inoltre se Eve avesse cercato di intercettare i qubit sul canale quantistico, alcune misurazioni di Bob effettuate nella stessa base di Alice avrebbero dato esiti diversi, mostrando l'intervento di Eve.

Oss. 1: la validità del protocollo dipende dal fatto che i due alfabeti sono associati a due osservabili non compatibili X e Z. Eve non può misurare simultaneamente lo spin lungo x e lungo z per lo stesso qubit. Quindi, se lei misura Z per il qubit $|0\rangle_x$ ottiene 0 o 1 con la stessa probabilità. Perciò avrà irrimediabilmente reso casuale lo spin originariamente inviato da Alice. Alice e Bob si accorgerebbero del suo intervento. L'intercettazione non è più passiva!

Oss. 2: inoltre è di fondamentale importanza il teorema di non clonazione. Infatti quest'ultimo garantisce l'impossibilità da parte di Eve di distinguere con certezza tra stati non ortogonali. Se esistesse una macchina clonatrice di stati quantistici Eve potrebbe creare molte copie di ogni qubit e risalire con precisione tra gli autostati di X e Z.

Crittografia quantistica: spin

Protocollo BBM92: esercizio



VOLUME 68, NUMBER 5 PHYSICAL REVIEW LETTERS 3 FEBRUARY 1992

Quantum Cryptography without Bell's Theorem

Charles H. Bennett
IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York 10598

Gilles Brassard
Département IRO, Université de Montréal, CP 6128, succursale "A," Montréal, Québec, Canada H3C 3J7

N. David Mermin
Laboratory of Atomic and Solid State Physics, Cornell University, Ithaca, New York, 14853-2501
(Received 26 September 1991)

Bibliografia

Benenti, G., Casati, G., Rossini, D., & Strini, G. (2018). Principles of Quantum Computation and Information: A Comprehensive Textbook. World scientific.

Bennett, C. H., & Brassard, G. (1984, August). An update on quantum cryptography. In *Workshop on the theory and application of cryptographic techniques* (pp. 475-480). Springer, Berlin, Heidelberg.

Bennett, C. H., & Brassard, G. (1984, December). Quantum cryptography. In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (pp. 175-179).

Bennett, C. H., Brassard, G., & Mermin, N. D. (1992). Quantum cryptography without Bell's theorem. *Physical review letters*, *68*(5), 557.

Nielsen, M. A., & Chuang, I. (2002). Quantum computation and quantum information.

Protocollo RSA: http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-9900/rsa/testo.htm

Protocollo RSA: http://www.dmi.unipg.it/~bista/didattica/sicurezza-pg/seminari2011-12/Baldantoni-Manasse/presentazione-parte2.pdf

Protocollo RSA liceo matematico: https://www.mat.uniroma1.it/sites/default/files/PLINIOSENIORE-CrittografiaRSA.pdf

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, *41*(2), 303-332.

http://math.unipa.it/~fbenanti/Crittografia291111.pdf