IL PENSIERO COMPUTAZIONALE

Percorso Formativo per i Docenti della Scuola Secondaria di Secondo Grado – Università di Pisa

Anna Bernasconi

Crittografia

Crittografia

Crittografia = "scrittura nascosta"

Studio di tecniche matematiche sofisticate per

mascherare i messaggi [CRITTOGRAFIA]

o tentare di svelarli [CRITTOANALISI]

Crittografia

Due mondi in contrapposizione

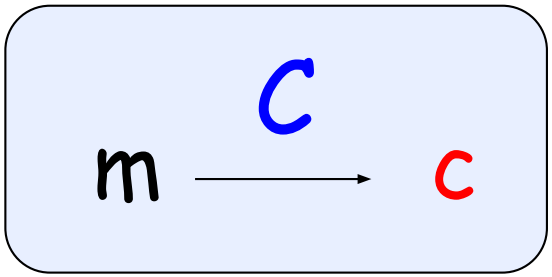
persone che vogliono scambiarsi privatamente delle informazioni

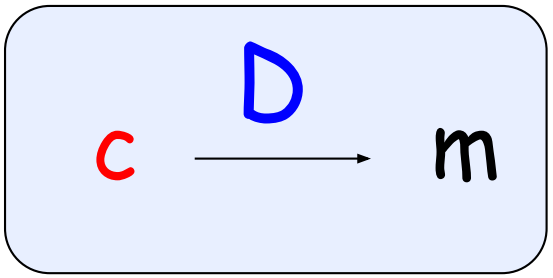
"impiccioni" che desiderano ascoltare o intromettersi nelle conversazioni altrui per

- curiosità,
- investigazione
- scopi malvagi

Schema di comunicazione

???





Cifratura

MSG: insieme dei messaggi (testi in chiaro)

CRITTO: insieme dei crittogrammi (testi cifrati)

Cifratura del messaggio

operazione con cui si trasforma un messaggio in chiaro m in un crittogramma c applicando una funzione

$$C: \ MSG \rightarrow CRITTO$$

e decifrazione

Decifrazione del crittogramma

operazione che permette di ricavare il messaggio in chiaro m a partire dal crittogramma c applicando una funzione

$$D: \text{CRITTO} \rightarrow \text{MSG}$$

Cifratura e decifrazione

- Le funzioni C e D sono una l'inversa dell'altra

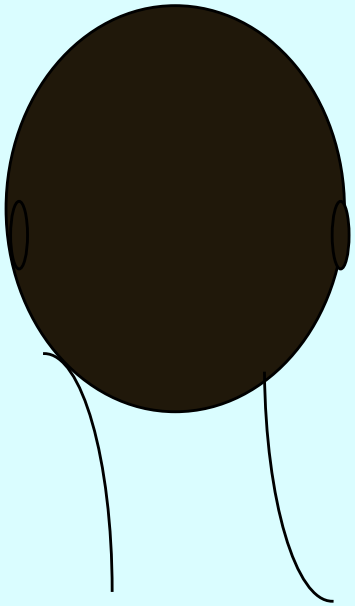
$$D(c) = D(C(m)) = m$$

- La funzione C è iniettiva

  a messaggi diversi devono corrispondere crittogrammi diversi

Antichi esempi

Erodoto: *Storie* (V secolo a. C.)



Antichi esempi

Spartani, V secolo a.C.

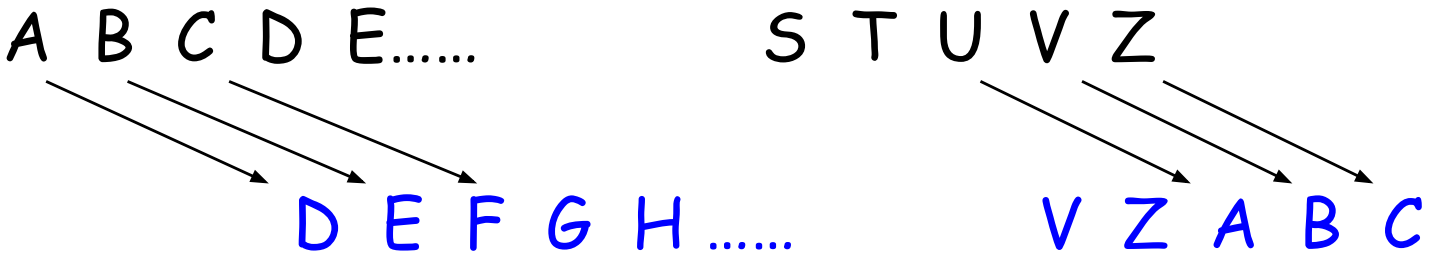
Scitale: asta cilindrica, costruita in due esemplari identici posseduti dai due corrispondenti

Cifrario di Cesare

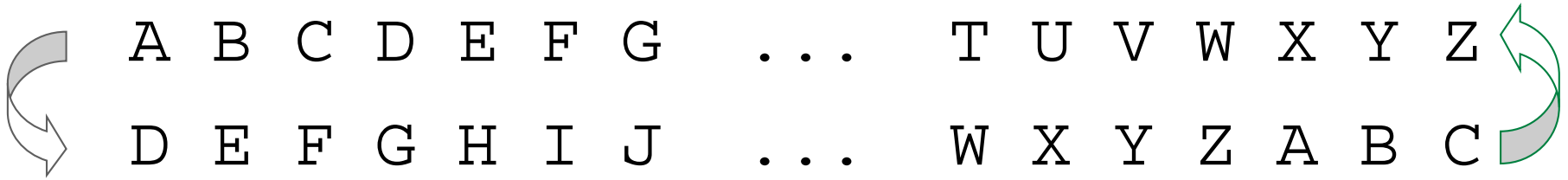
È il più antico cifrario di concezione moderna (Svetonio, *Le vite di dodici Cesari*)

Idea di base:

Il crittogramma c è ottenuto dal messaggio in chiaro m sostituendo ogni lettera di m con quella tre posizioni più avanti nell'alfabeto



Cifrario di Cesare



Cifratura

Decifrazione

ATTENTO A EVE

DWWHQWR D HYH

Cifrario di Cesare

La segretezza dipendeva dalla conoscenza del metodo

Scoprire il metodo di cifratura significa compromettere irrimediabilmente l'impiego del cifrario

Il cifrario era destinato all'uso ristretto di un gruppo di conoscenti

Livello di segretezza

Classificazione dei metodi crittografici (cifrari) in base al livello di segretezza

Cifrari per uso ristretto

Le funzioni di cifratura C e di decifrazione D sono tenute segrete in ogni loro aspetto

Impiegati per comunicazioni diplomatiche o militari

Non adatti per una crittografia "di massa"

Cifrari per uso generale

fondati sull'uso di una chiave segreta

Cifrari per uso generale

Ogni codice segreto non può essere mantenuto tale troppo a lungo

In un cifrario utilizzato da molti utenti, la parte segreta del metodo deve essere limitata a un'informazione aggiuntiva, la chiave, nota solo alla coppia di utenti che stanno comunicando (il codice di Cesare non aveva chiave)

Le regole devono essere pubbliche
e solo la chiave deve essere segreta

il nemico conosce il sistema!

Cifrari per uso generale

Le funzioni C e D sono pubblicamente note

Si usa una chiave segreta k

- diversa per ogni coppia di utenti
- inserita come parametro nelle funzioni di cifratura e decifrazione

$$c = C(m,k) \quad m = D(c,k)$$

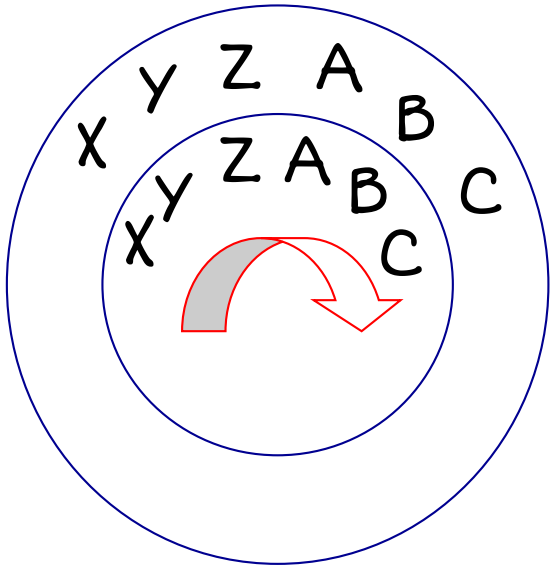
Se non si conosce k, la conoscenza di C e D e del crittogramma NON deve permettere di estrarre informazioni sul messaggio in chiaro.

Cifrario di Cesare generalizzato

Invece di rotare l'alfabeto di 3 posizioni, possiamo rotarlo di una quantità arbitraria k, $1 \leq k \leq 25$
(26 lascia inalterato il messaggio)

k è la chiave del cifrario

Alice e Bob hanno 25 chiavi diverse tra cui scegliere



Le chiavi segrete

Se la segretezza dipende unicamente dalla chiave

- il numero delle chiavi deve essere così grande da essere praticamente immune da ogni tentativo di provarle tutte
- la chiave segreta deve essere scelta in modo causale

Si può prendere una permutazione arbitraria dell'alfabeto come chiave:

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

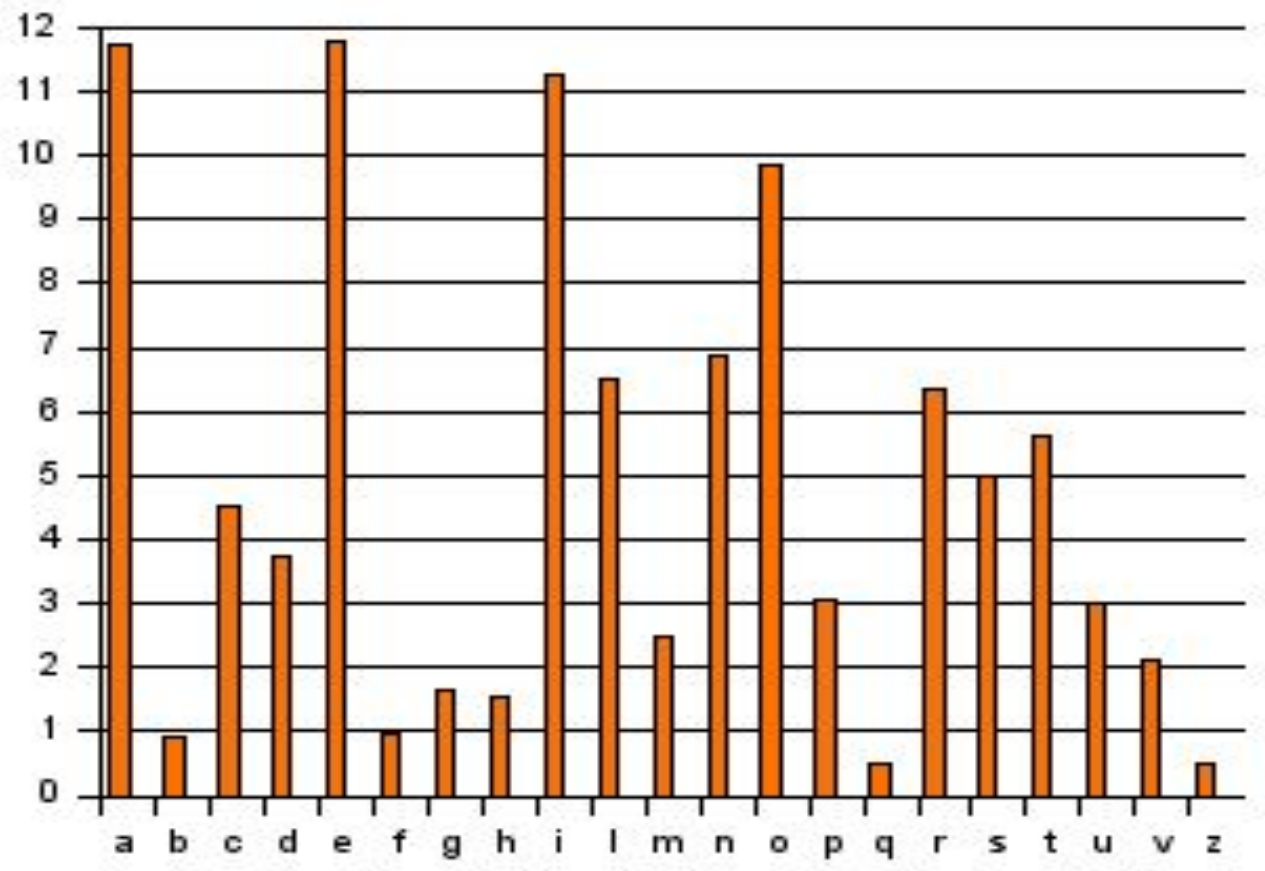
testo: BOBSTAIATTENTOAEVE

messaggio cifrato: DEDFWSRSWWBYWESBGB

Vi sono 26! chiavi possibili, un numero enorme ($\sim 1.5\ 10^{26}$). Non è possibile attaccare il cifrario provandole una a una, tuttavia .....

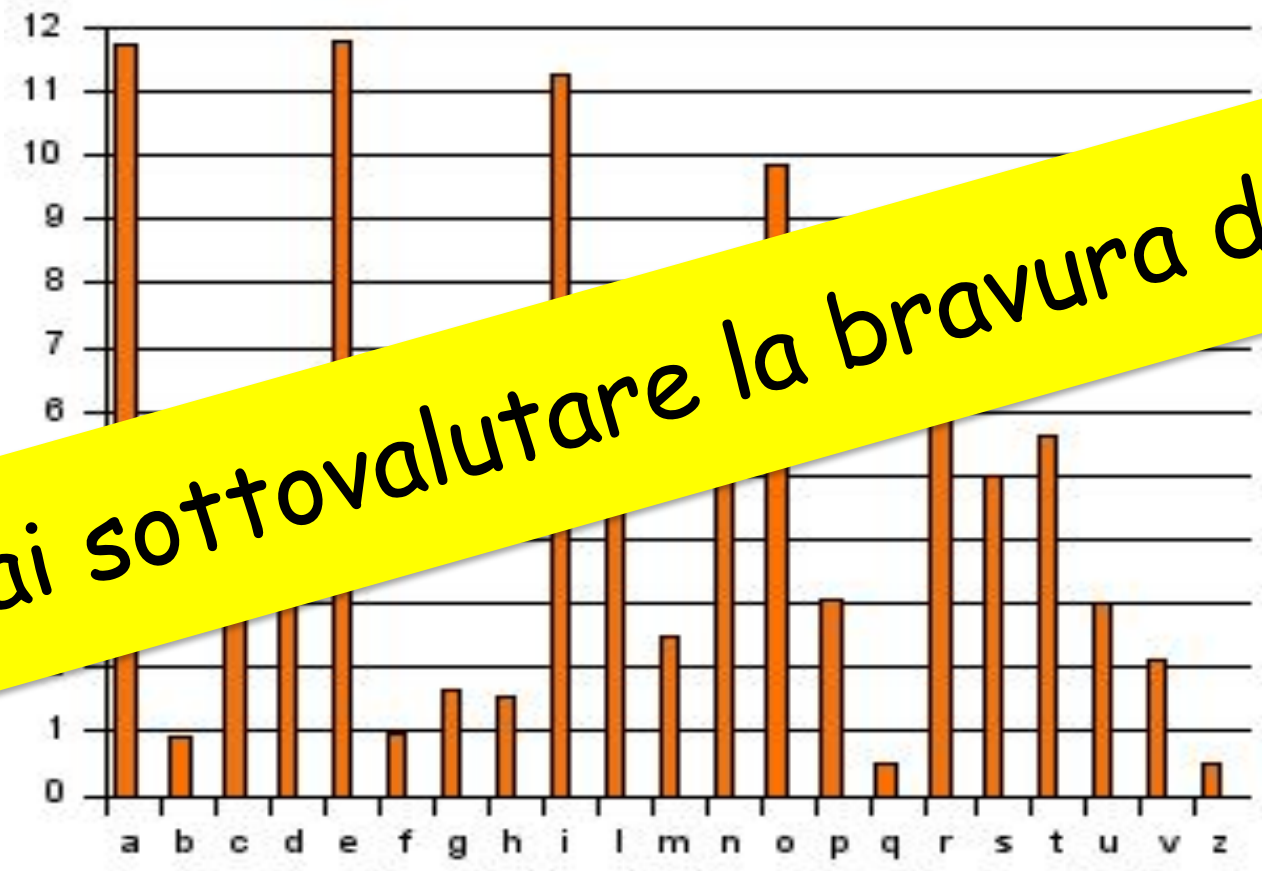
.... il sistema è attaccabile facilmente con un'analisi statistica sulla frequenza dei caratteri

Frequenze dei caratteri in italiano



.... il sistema è attaccabile facilmente con un'analisi statistica sulla frequenza dei caratteri

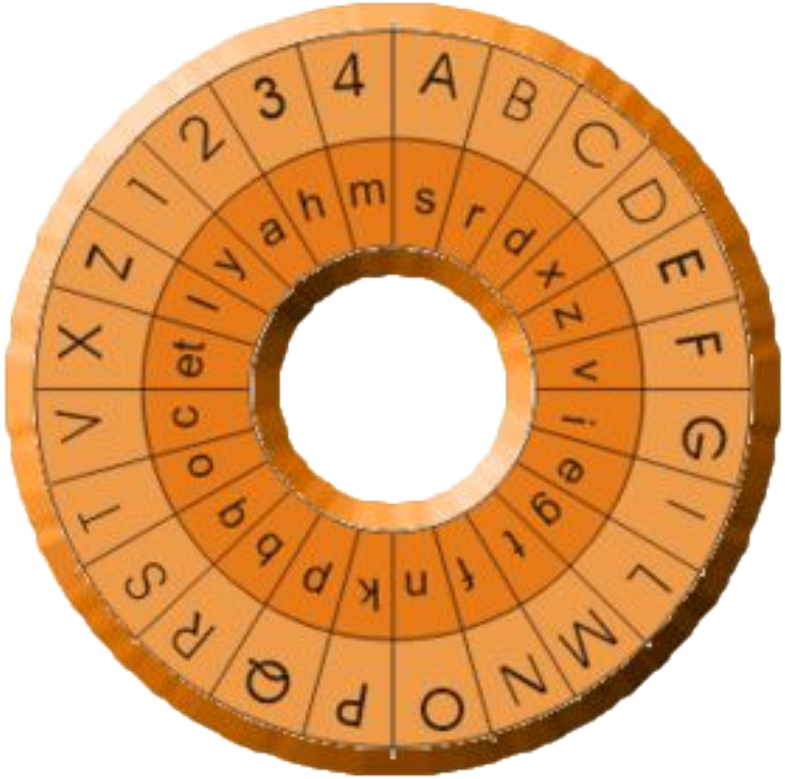
Frequenze dei caratteri in italiano



Mai sottovalutare la bravura di Eve!

Nascita dei cifrari polialfabetici

il disco cifrante di Leon Battista Alberti (XV secolo)



Alfabeto esterno
lettere (alcune) e numeri, per formulare il messaggio

Alfabeto interno
più ricco, disposto in modo arbitrario (e diverso per ogni coppia di utenti), per costruire il crittogramma

Cifrario di Alberti

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	1	2	3	4	5
S	D	T	K	B	J	O	H	R	Z	C	U	N	Y	E	P	X	V	F	W	A	G	Q	I	L	M

Chiave: A-S

Messaggio: NON FIDARTI DI EVE

m = NONFIDA2RTIDIEVE

c = UNUJRKSQ

qui la chiave diventa A-Q

Cifrario di Alberti

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	1	2	3	4	5
Q	I	L	M	S	D	T	K	B	J	O	H	R	Z	C	U	N	Y	E	P	X	V	F	W	A	G

Chiave: A-Q

Messaggio: NON FIDARTI DI EVE

m = NONFIDA2RTIDIEVE

c = UNUJRKSQUYBMBSPS

qui la chiave diventa A-Q

Cifrario di Alberti

- ➔ si cambia chiave ogni volta che si incontra un carattere speciale
- ➔ inserendo spesso i caratteri speciali (scartati nel messaggio ricostruito) il cifrario è difficile da attaccare
- ➔ il continuo cambio di chiave rende inutili gli attacchi basati sulla frequenza dei caratteri

La Macchina Enigma (Germania, 1918)

Estensione elettromeccanica del cifrario di Alberti

Sull'idea di Alberti lavorò de Vigenère (1586)

Usa una chiave corta e ripetuta ciclicamente.

Ogni lettera della chiave indica una traslazione della corrispondente lettera del testo.

chiave:			C		H		I		A		V		E		
traslazione:	2		7		8		0		24		4				

N	O	N	F	I	D	A	R	T	I	D	I	E	V	E	
2	7	8	0	24	4	2	7	8	0	24	4	2	7	8	
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
P	V	V	F	G	H	C	Y	B	I	B	M	G	C	M	

One-Time Pad (1917)

Se estendiamo il metodo di Vigenère impiegando una chiave lunga come il testo, casuale e non riutilizzabile, il cifrario diviene inattaccabile!

Non può essere decifrato senza conoscere la chiave

È il caso di One-Time Pad (1917) che impiega un codice binario per messaggi e chiavi

Fu usato nella Hot Line per le comunicazioni tra la Casa Bianca e il Cremlino a partire dal 1967

Cifrario inattaccabile (perfetto)

Claude Shannon, 1945
(pubblicazione rimandata al 1949 per motivi di segretezza militare)

Messaggio in chiaro e crittogramma risultano del tutto scorrelati tra loro

nessuna informazione sul testo in chiaro può filtrare dal crittogramma

la conoscenza di Eve non cambia dopo aver osservato un crittogramma sul canale

One-Time Pad

m = 01010101010101010101

k = 00111100100011100011...

c = 01101001110110110110

One-Time Pad

m = 01010101010101010101

k = 00111100100011100011...

c = 01101001110110110110

k = 00111100100011100011...

One-Time Pad

m = 010101010101010101010101

k = 001111001000111100011...

c = 011010011110110110110110

k = 001111001000111100011...

m = 010101010101010101010101

One-Time Pad

Assolutamente sicuro, ma...

- richiede una nuova chiave segreta per ogni messaggio
- perfettamente casuale
- e lunga come il messaggio da scambiare!

come si genera e come si scambia la chiave???

Estremamente attraente per chi richieda una sicurezza assoluta e sia disposto a pagarne i costi

Cifrari di oggi

Advanced Encryption Standard (AES)

- standard per le comunicazioni riservate ma "non classificate"
- pubblicamente noto e realizzabile in hardware su computer di ogni tipo
- Chiavi brevi (qualche decina di caratteri, 128 o 256 bit)
- Ogni carattere del crittogramma dipende da tutti i caratteri del testo in chiaro e della chiave

Sicurezza

La sicurezza è basata su due principi (Claude Shannon)

DIFFUSIONE

il testo in chiaro si deve distribuire su tutto il crittogramma

➔ *ogni carattere del crittogramma deve dipendere da tutti i caratteri del blocco di messaggio*

CONFUSIONE

messaggio e chiave sono combinati tra loro in modo complesso per non permettere al crittoanalista di separare le due sequenze tramite l'analisi del crittogramma

➔ *la chiave deve essere ben distribuita sul testo cifrato*

➔ *ogni bit del crittogramma deve dipendere da tutti i bit della chiave*

Advanced Encryption Standard (AES)

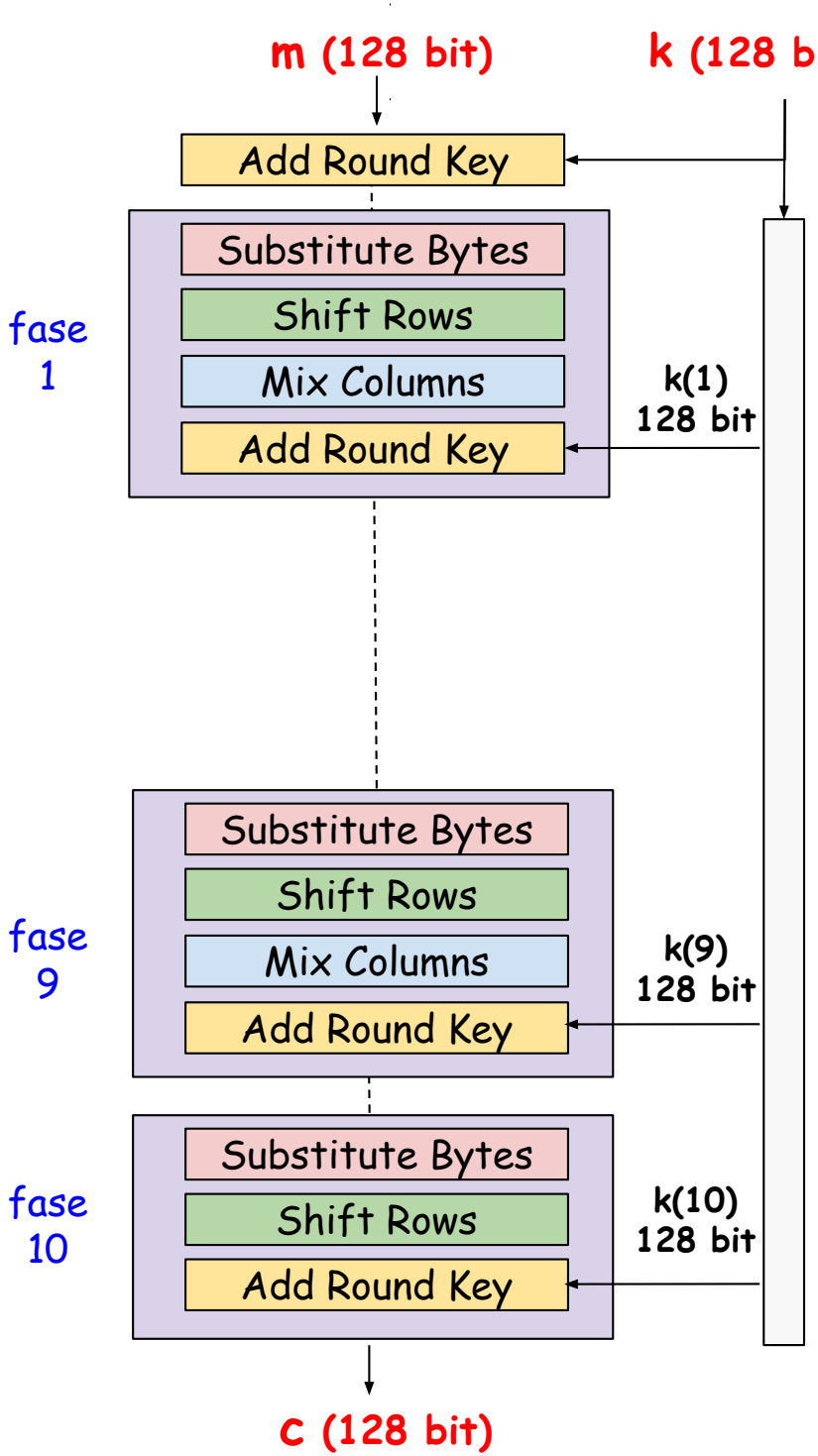
CIFRARIO SIMMETRICO A BLOCCHI

la stessa chiave è usata per cifrare e decifrare

il messaggio è diviso in blocchi lunghi come la chiave

la chiave è utilizzata per trasformare un blocco del messaggio in un blocco del crittogramma

AES (128)



Gestore delle chiavi
Espansioni e trasformazioni non lineari (S-box)

e le chiavi per usare i cifrari ?

Novità rispetto al passato:

le chiavi segrete non sono stabilite direttamente dai partner (Alice e Bob), ma dai mezzi elettronici che utilizzano per comunicare: PC, tablet, smartphone, terminali bancari

su Internet si costruisce una nuova chiave per ogni sessione

e le chiavi ?

Ma come si può scambiare una chiave segreta con facilità e sicurezza?

La chiave serve per comunicare in sicurezza, ma Alice e Bob la devono stabilire e scambiare comunicando "in sicurezza" senza poter ancora usare il cifrario...

Distribuzione delle chiavi

Nel 1976 viene proposta alla comunità scientifica un algoritmo per generare e scambiare una chiave segreta su un canale insicuro

Merkle Hellman Diffie

senza la necessità che le due parti si siano scambiate informazioni o incontrate in precedenza

questo algoritmo, detto protocollo DH, è ancora largamente usato nei protocolli crittografici su Internet

Distribuzione delle chiavi

Nel 1976 viene proposta alla comunità scientifica un algoritmo per generare e scambiare una chiave segreta su un canale insicuro

Merkle Hellman Diffie

Turing Award 2015

Protocollo DH per lo scambio pubblico delle chiavi

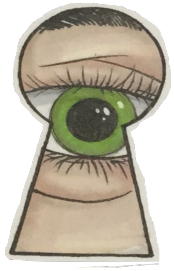
Alice e Bob generano una chiave k (un numero intero) in modo *incrementale*

- ★ scambiandosi in chiaro alcuni pezzi di k
- ★ questi pezzi sono sufficienti a ricostruire la chiave k solo se combinati con informazioni segrete in possesso di Alice e Bob, e diverse per entrambi

Non si condividono informazioni 'segrete', ma si COSTRUISCE insieme una chiave segreta

La chiave non viene mai trasmessa!

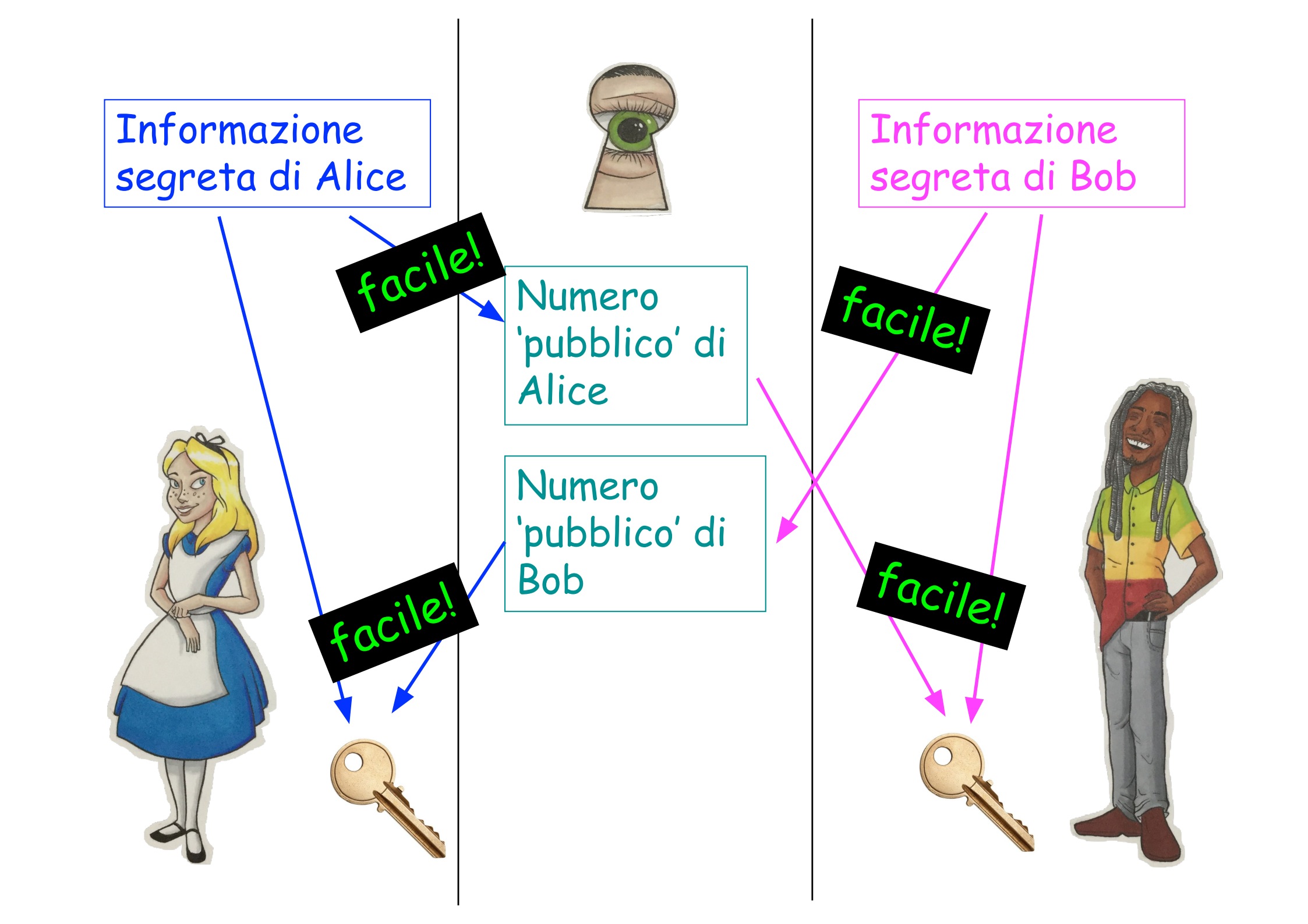
Informazione segreta di Alice



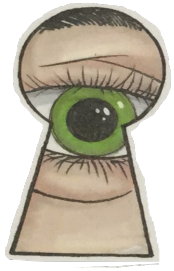
Informazione segreta di Bob

Numero 'pubblico' di Alice

Numero 'pubblico' di Bob


Informazione segreta di Alice
facile!
Numero 'pubblico' di Alice
Numero 'pubblico' di Bob
facile!
facile!
facile!
Informazione segreta di Bob

Informazione segreta di Alice



Informazione segreta di Bob

difficile!

Numero 'pubblico' di Alice

Numero 'pubblico' di Bob

difficile!

Funzione one-way

calcolare il numero pubblico dall'informazione segreta deve essere facile (Alice e Bob)

ricavare l'informazione segreta dal numero pubblico deve essere difficile (Eve)

Il protocollo DH utilizza una funzione one-way: una funzione facile da calcolare e difficile da invertire

facile da calcolare …

Dato x, si conosce un algoritmo efficiente (polinomiale) per calcolare $y = f(x)$

e difficile da invertire …

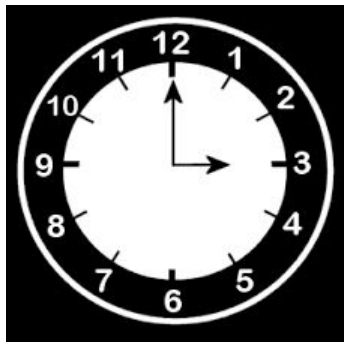
Dato y, si conoscono solo algoritmi inefficienti (esponenziali) per trovare un x t.c $y = f(x)$, ossia per calcolare $x = f^{-1}(y)$

Aritmetica modulare

È un campo della matematica ricco di funzioni one-way.
Sia m un intero positivo.
Si considerano solo i numeri interi compresi tra 0 e m-1 come se fossero 'disposti ad anello': ogni volta che che si passa dal punto di partenza, si riparte da 0, come accade sul quadrante di un orologio [Aritmetica dell'orologio]

Alice e Bob vanno a una festa alle 11 di sera e ci restano 4 ore, a che ora tornano?

Alle 3 di notte, ma 11 + 4 = 15
Abbiamo ridotto modulo 12!
15 mod 12 = 3



Aritmetica modulare

Sommare o sottrarre m, o un suo multiplo, è come sommare o sottrarre 0

non interessa il numero dei giri, ma solo che avanza alla fine (il resto della divisione)

il valore modulare k = N mod m coincide con il resto della divisione tra N e m

ESEMPI

m = 13

29 mod 13 = 3 infatti 29 = 3 + 2 * 13

39 mod 13 = 0 infatti 39 = 0 + 3 * 13

27 mod 13 = 1 infatti 27 = 1 + 2 * 13

Aritmetica modulare

Usata in molti algoritmi crittografici per

- ridurre lo spazio dei numeri su cui si opera, e quindi aumentare la velocità di calcolo
- rendere *difficili* problemi computazionali che sono semplici (o anche banali) nell'algebra non modulare

Aritmetica modulare

Nell'aritmetica modulare le funzioni tendono a comportarsi in modo 'imprevedibile'

La funzione 2^x nell'aritmetica ordinaria e' una funzione crescente

x	1	2	3	4	5	6	7	8	9	10	11	12
2^x	2	4	8	16	32	64	128	256	512	1024	2048	4096

La funzione 2^x mod 13 diventa

x	1	2	3	4	5	6	7	8	9	10	11	12
2^x	2	4	8	3	6	12	11	9	5	10	7	1

Aritmetica modulare

$2^x = 512$, $x = ?$

per errore, supponiamo $x = 8$
$2^8 = 256$ → è stato scelto un numero troppo basso
proviamo $x = 9$ ok!

$2^x \bmod 13 = 5$, $x = ?$

per errore, supponiamo $x = 6$
$2^6 \bmod 13 = 12$ → x è troppo alto...

???

occorre provare tutti i valori di x
la risposta giusta è $x = 9$

Una funzione one-way

Scegliamo un numero primo p molto grande (con 2048 cifre binarie, ~ 600 cifre decimali), e lavoriamo modulo p

Consideriamo l'insieme $Z^*_p = \{1, 2, \ldots, p-1\}$

Proprietà
Se p è un numero primo, Z^*_p ha almeno un generatore $g < p$

Generatore:
intero che elevato a tutti gli esponenti 1, 2, ..., p-1 (lavorando mod p), produce come risultati tutti gli elementi di Z^*_p, ma in un ordine difficile da prevedere

ESEMPIO: $g = 2$ è un generatore di $Z^*_{13} = \{1,2,\ldots, 12\}$

x	1	2	3	4	5	6	7	8	9	10	11	12
2^x	2	4	8	3	6	12	11	9	5	10	7	1

Elevamento a potenza

Dati un numero primo p (e.g., di 600 cifre decimali), un generatore g per Z^*_p e un intero $k < p$, calcolare

$$y = g^k \bmod p$$

ALGORITMO 1

algoritmo esponenziale

$y = g\ g\ g \ldots g$ (k volte)

esegue k moltiplicazioni, $k \sim 10^{600}$!!!

➜ numero di moltiplicazioni è proporzionale al VALORE di k

ALGORITMO 2

algoritmo polinomiale

esponenziazione veloce

esegue un numero di moltiplicazioni proporzionale al NUMERO DI CIFRE binarie di k, e non al suo valore

(600 cifre decimali, circa 2000 cifra binarie)

Elevamento a potenza 'veloce'

Quadrature successive

$(23)_{10} = (10111)_2$

$3^{23} \bmod 29 = 3^{16+4+2+1} \bmod 29$

$= (3^{16} \times 3^4 \times 3^2 \times \mathbf{3}) \bmod 29$

$3^2 \bmod 29 = 3 \times 3 \bmod 29 = \mathbf{9}$

$3^4 \bmod 29 = 9 \times 9 \bmod 29 = \mathbf{23}$

$3^8 \bmod 29 = 23 \times 23 \bmod 29 = 7$

$3^{16} \bmod 29 = 7 \times 7 \bmod 29 = \mathbf{20}$

$3^{23} \bmod 29 = \mathbf{20} \times \mathbf{23} \times \mathbf{9} \times \mathbf{3} \bmod 29 = 8$

7 moltiplicazioni

Logaritmo discreto

Dati un numero primo p, un generatore g per Z^*_p e un intero y < p, trovare x tale che

$$y = g^x \bmod p$$

è molto difficile

➔ non è noto a priori in che ordine sono generati gli elementi

➔ quindi non è noto per quale valore di *x* si genera y

Algoritmo bruteforce

si provano tutti i valori possibili di x tra 1 e p-1, fino a trovare il valore che permette di ottenere y

Richiede un numero di 'tentativi' proporzionale al valore di p (~ 2^{2048}, ~ 10^{600}))

Algoritmo esponenziale nel numero di cifre di p

Protocollo DH

Alice e Bob scelgono una coppia p, g (nota a tutti)

sceglie a caso
$1 < a < p-1$
(segreto di Alice)

calcola
$A = g^a \bmod p$

invia A a Bob

sceglie a caso
$1 < b < p-1$
(segreto di Bob)

calcola
$B = g^b \bmod p$

invia B ad Alice

A →

← B

riceve B e calcola

$K = B^a \bmod p$
$= g^{b \times a} \bmod p$

riceve A e calcola

$K = A^b \bmod p$
$= g^{a \times b} \bmod p$

Protocollo DH

Alice e Bob hanno costruito la stessa chiave segreta K

$$K = g^{b \times a} \bmod p = g^{a \times b} \bmod p$$

Alice e Bob hanno una chiave comune che possono usare per comunicare usando un cifrario simmetrico (AES)

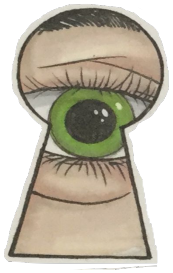
ESEMPIO

Alice e Bob scelgono una coppia $p = 13, g = 2$

sceglie a caso $a = 5$ (segreto di Alice)		sceglie a caso $b = 2$ (segreto di Bob)
calcola $A = 2^5 \bmod 13 = 6$		calcola $B = 2^2 \bmod 13 = 4$
invia 6 a Bob	6 →	
	← 4	invia 4 ad Alice
riceve $B=4$ e calcola $K = 4^5 \bmod 13 = 10$		riceve $A=6$ e calcola $K = 6^2 \bmod 13 = 10$

Alice e Bob hanno una chiave in comune: il numero 10.

Sicurezza del protocollo



Eve intercetta la trasmissione e viene a conoscenza di p, g, A, B

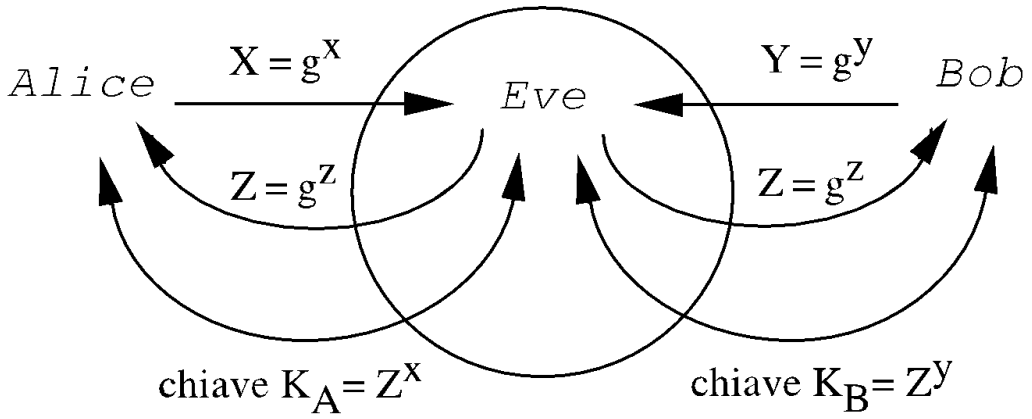
Per ricostruire la chiave deve

- risolvere $A = g^a \bmod p$ rispetto ad a, e calcolare $K = B^a \bmod p$
  oppure
- risolvere $B = g^b \bmod p$ rispetto a b, e calcolare $K = A^b \bmod p$

➔ deve calcolare il logaritmo discreto di A oppure il logaritmo discreto di B,
ma queste operazioni richiedono un numero di passi esponenziale nel numero di cifre di p

Attacco 'man in the middle'

Eve si finge Bob agli occhi e Alice agli occhi di Bob, sostituendo A e B con un proprio valore $Z = g^z \bmod p$



Alice e Bob interpretano Z come proveniente dall'altro partner e costruiscono le chiavi (diverse)

$K_A = Z^x \bmod p$ $K_B = Z^y \bmod p$

Eve conosce entrambe le chiavi

- comunica con Alice fingendosi Bob e usando l'AES con K_A
- comunica con Bob fingendosi Alice e usando l'AES con K_B

Certificati digitali

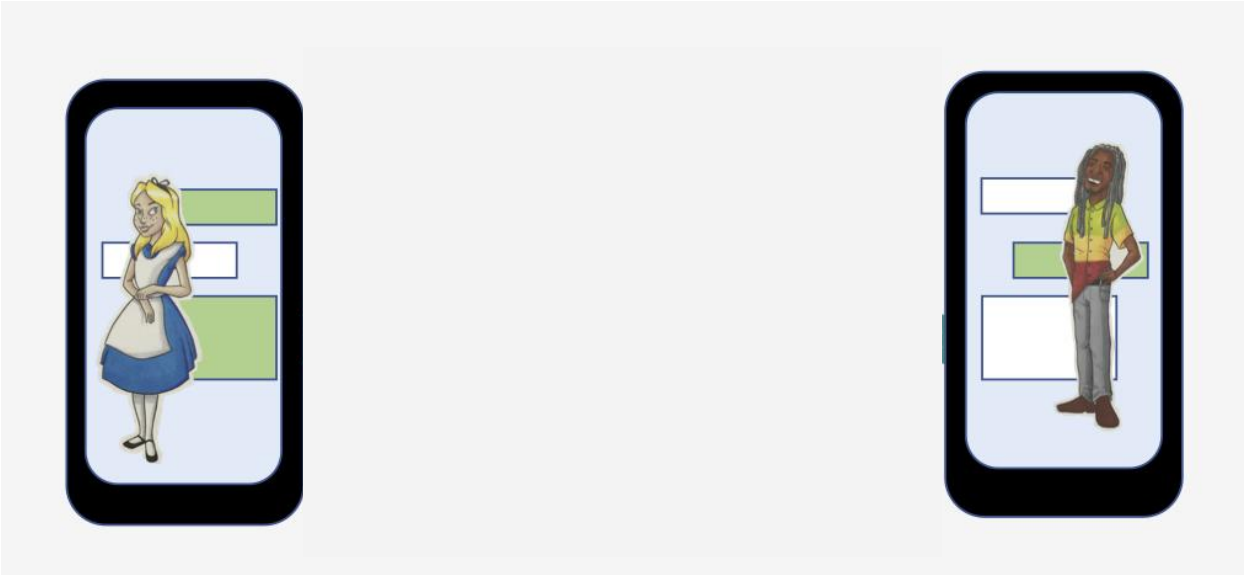
- Per scongiurare questi attacchi Alice e Bob utilizzano dei certificati digitali per scambiare tra loro le informazioni pubbliche 'A' e 'B'
- Sono rilasciati dalle Certification Authority enti preposti alla certificazione di validità delle chiavi pubbliche
- I certificati digitali autenticano l'associazione

  ⟨ utente, dati pubblici dell'utente ⟩

  e sono difficili da falsificare.

Conversazioni private in rete

Se Alice e Bob desiderano comunicare privatamente in rete, ad esempio via Whatsapp, usano la Crittografia End-to-End (E2EE)



Cifratura e decifrazione dei messaggi inviati e ricevuti avvengono interamente sui dispositivi di Alice e Bob

- il messaggio è già cifrato quando lascia il dispositivo di Alice, ed è decifrato solo quando raggiunge il dispositivo di Bob

Conversazioni private in rete

Se Alice e Bob desiderano comunicare privatamente in rete, ad esempio via Whatsapp, usano la Crittografia End-to-End (E2EE)

I messaggi transitano cifrati

- il server che si occupa di smistare i messaggi non ha un mezzo per decifrarli e li memorizza in forma cifrata
- WhatsApp non può vedere il contenuto dei messaggi
- Solo Alice e Bob possono conoscere il contenuto dei messaggi

Conversazioni private in rete

Se Alice e Bob desiderano comunicare privatamente in rete, ad esempio via Whatsapp, usano la Crittografia End-to-End (E2EE)

Le chiavi cambiano a ogni singolo messaggio inviato, e sono generate direttamente da Alice e Bob sui loro dispositivi

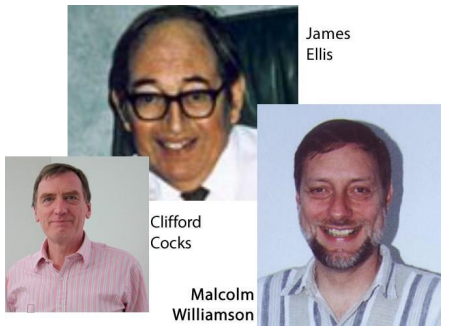
EE2E utilizza diverse primitive crittografiche, tra cui il protocollo DH e il cifrario AES(256)

Crittografia a chiave pubblica

Nel 1976 D. e H. propongono alla comunità scientifica anche la definizione di crittografia a chiave pubblica (ma senza averne un'implementazione pratica)

rivoluziona il modo di concepire le comunicazioni segrete

Nata ufficialmente nel 1976 ma preceduta dal lavoro, coperto da segreto, degli agenti britannici (Ellis, Cock e Williamson)



Cifrari simmetrici

Nei cifrari simmetrici, la chiave di cifratura è uguale a quella di decifrazione (o l'una può essere facilmente calcolata dall'altra)

ed è nota solo ai due partner che la scelgono di comune accordo e la mantengono segreta

Crittografia a chiave pubblica (1976)

Obiettivo: permettere a tutti di inviare messaggi cifrati ma abilitare solo il ricevente (BOB) a decifrarli

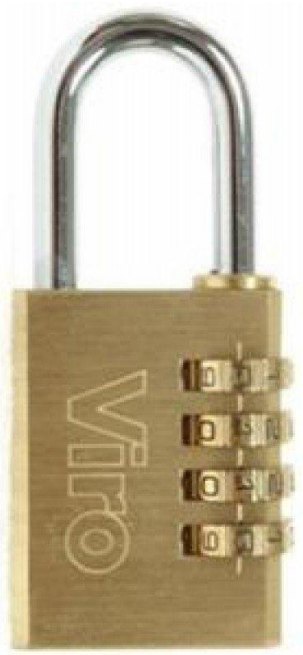
Le operazioni di cifratura e decifrazione sono pubbliche e utilizzano due chiavi diverse:

K_B[pub] per cifrare: è pubblica, nota a tutti;

K_B[prv] per decifrare: è privata, nota solo a BOB

Esiste una coppia <k[pub], k[prv]> per ogni utente del sistema

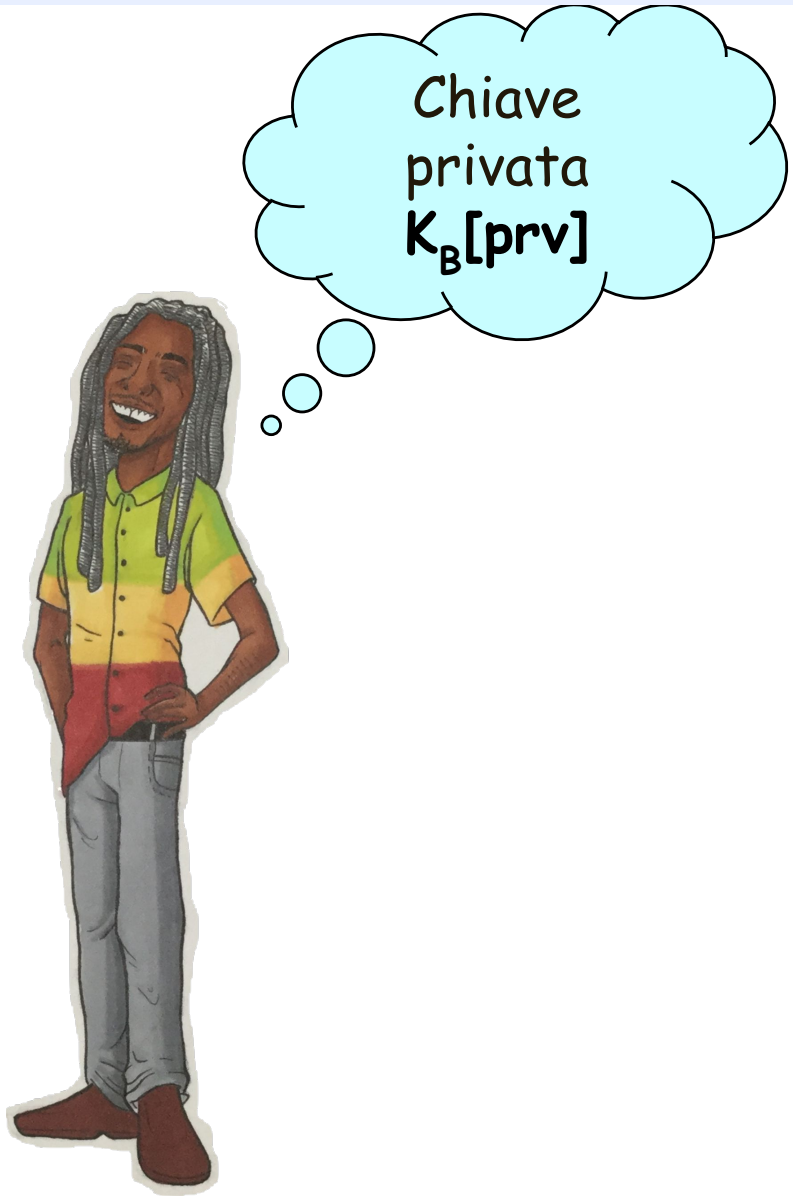
Crittografia simmetrica e crittografia a chiave pubblica



crittografia simmetrica

crittografia a chiave pubblica

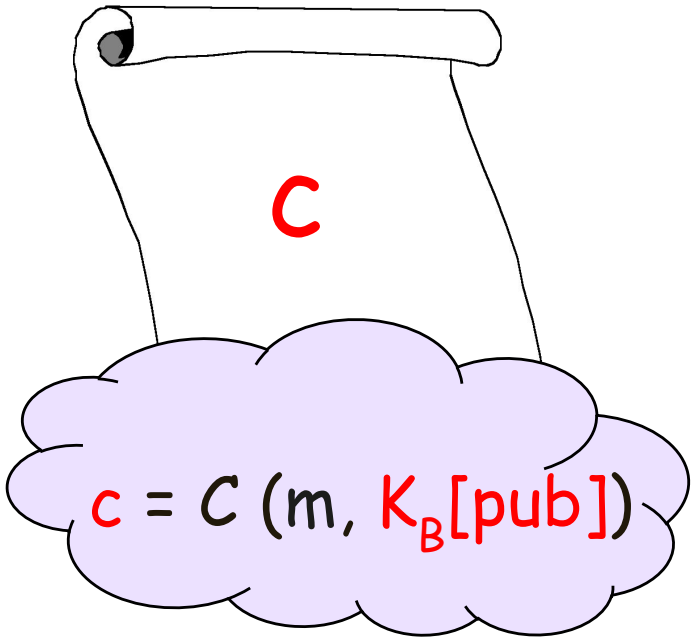
Bob sceglie due chiavi: una privata e una pubblica

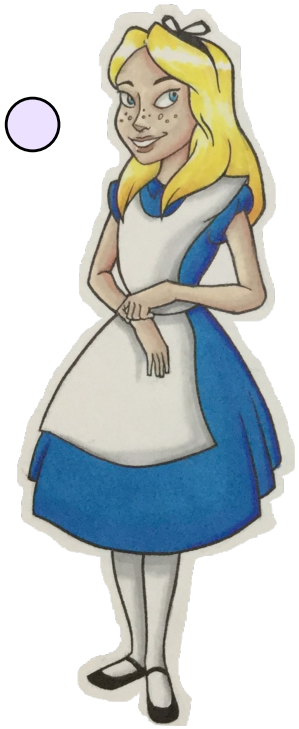


Pubblico Registro

Utente	Chiave pubblica
.....	.....
Bob	**$K_B[pub]$**

Alice vuole spedire un messaggio m a Bob in modo segreto





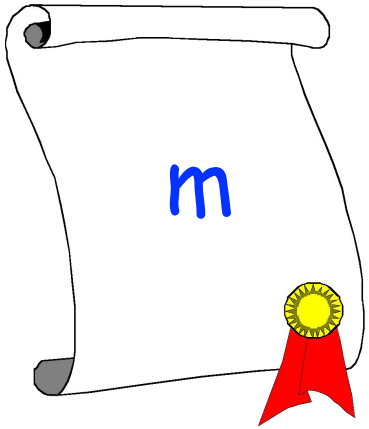
Pubblico Registro

Utente	Chiave pubblica
.....	.....
Bob	**K_B[pub]**

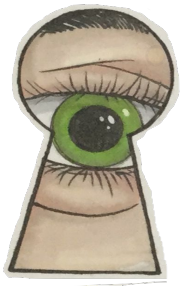
Bob traduce il crittogramma c di Alice

Nessun altro può farlo senza conoscere $K_B[prv]$

$m = D(c, K_B[prv])$



c ?



Cifrari a chiave pubblica

La cifratura di un messaggio *m* da inviare a BOB è eseguita da qualunque mittente come

$$c = C\,(m, K_B[pub])$$

chiave $K_B[pub]$ e funzione di cifratura sono note a tutti

La decifrazione è eseguita da BOB come

$$m = D\,(c, K_B[prv])$$

la funzione di decifrazione è nota a tutti, ma $K_B[prv]$ non è disponibile agli altri

Crittografia a chiave pubblica

La funzione di cifratura deve essere una funzione *one-way trap-door*

calcolare $c = C(m, K_B[pub])$ è computazionalmente facile

decifrare c è computazionalmente difficile

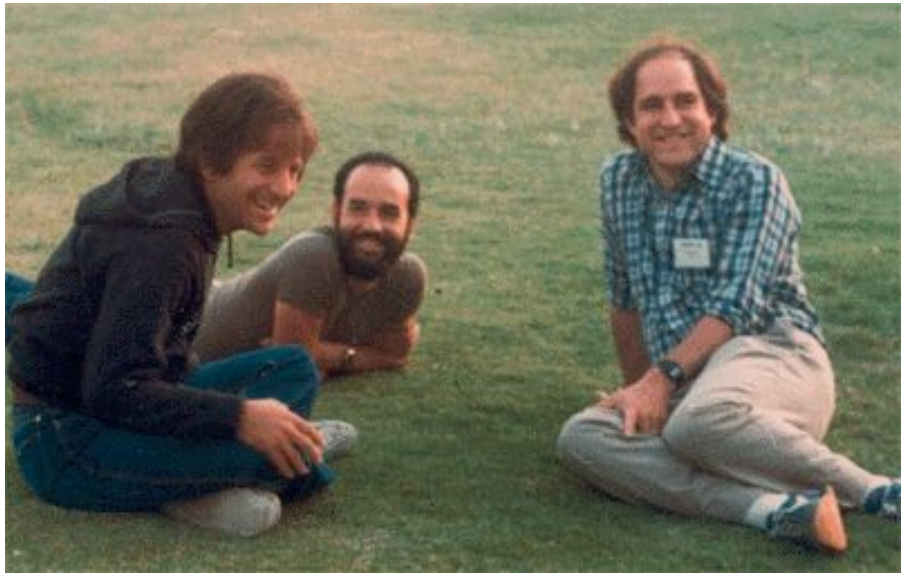
a meno che non si conosca un meccanismo segreto, rappresentato da $K_B[prv]$ (trap-door)

facile da calcolare …

e difficile da invertire …

a meno che non si conosca
la chiave privata!

RSA (1977)



Adleman Shamir Rivest

propongono un sistema a chiave pubblica basato su una funzione "facile" da calcolare e "difficile" da invertire

… era la stessa funzione individuata dagli agenti britannici (Ellis, Cock e Williamson)

(Turing Award 2002)

RSA (1977)

RSA si basa sulla moltiplicazione di due numeri primi p, q

Calcolare $n = p \times q$ è facile

Calcolare p, q da n è difficile
a meno che non si conosca uno dei due

Fattorizzare $n = 1841488427$

$p = ?$
$q = ?$

RSA (1977)

RSA si basa sulla moltiplicazione di due numeri primi p, q

Calcolare $n = p \times q$ è facile

Calcolare p, q da n è difficile
a meno che non si conosca uno dei due

Fattorizzare $n = 1841488427$

$p = 31723$
$q = 58049$

RSA (1977)

1. Si scelgono due numeri primi a caso p e q
2. Si calcola il prodotto $n = p * q$
3. Si calcola $\phi(n) = (p-1) * (q-1)$
4. Si sceglie a caso un numero e coprimo e minore di $\phi(n)$
5. Si calcola $d = e^{-1} \bmod \phi(n)$ ➜ $e\,d \equiv 1 \mod \phi(n)$
   ➜ $e\,d = 1 + k\,\phi(n)$

Chiave pubblica K[pub] = (n, e)

Chiave privata k[prv] = (d)

Cifratura e decifrazione

il messaggio m è codificato come una sequenza binaria, trattata come un numero intero $m < n$

se $m \geq n$ ➜ cifratura a blocchi, di $\log_2 n$ bit ciascuno

CIFRATURA	$c = C(m, k[pub]) = m^e \bmod n$
DECIFRAZIONE	$m = D(c, K[prv]) = c^d \bmod n$

ESEMPIO

p = 53 q = 61

n = p * q= 3233

ϕ(n) = (p-1) * (q-1) = 52 * 60 = 3120

e = 17

d = e^{-1} mod ϕ(n) = 17^{-1} mod 3120 = 2753

K[pub] = (3233, 17) k[prv] = 2753

m = 65

c = 65^{17} mod 3233 = 2790

m = 2790^{2753} mod 3233 = 65

La carta di credito su internet

Se Alice desidera comprare dalla ditta di Bob, i computer di Alice e Bob devono essere in grado di eseguire gli stessi algoritmi crittografici (per esempio DH e AES, oppure RSA e AES), cioè in questi computer devono essere installati programmi compatibili tra loro.

Un protocollo di scambio

1. Bob spedisce ad Alice un certificato digitale contenente la sua chiave pubblica $k_B[pub]$ di RSA
2. Alice costruisce una chiave segreta K da usare nell'AES, cifra K con la chiave pubblica $k_B[pub]$ di Bob e la invia a Bob
3. Bob ricostruisce K usando la sua chiave RSA privata $k_B[prv]$; ora Alice e Bob hanno la chiave comune K per l'AES
4. Alice e Bob si scambiano messaggi in AES, tra questi, i dati sensibili di Alice

Algoritmi Crittografici (Lab)

Implementeremo in Python:

- Il cifrario di Cesare
- Il One-Time-Pad
- L'esponenziazione veloce per Diffie-Helmann