Crittografia

A COSA SERVE LA CRITTOGRAFIA?

La crittografia serve ad aiutare due utenti, Alice e Bob, a comunicare in modo sicuro...

Mister X

...anche in presenza di Mister X, un avversario che ascolta la loro comunicazione.

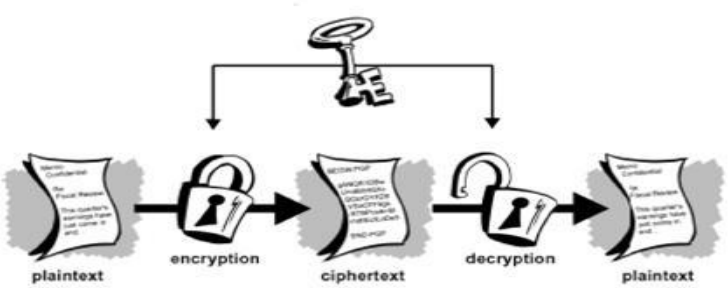
Oggi serve anche a molto altro:

Firme digitali, autenticazione, divisione di segreti, criptovalute...

Crittografia

La parola CRITTOGRAFIA deriva dalle parole greche kryptós, che significa “nascosto”, e gráphein, che significa “scrivere”.

Come funziona?



Nella crittografia **tradizionale o simmetrica** Alice cifra, cioè trasforma il messaggio originale M in un altro messaggio C dal quale è “quasi” impossibile ricavare M.

L’unica persona in grado di recuperare M da C è Bob, che condivide con Alice alcune informazioni segrete.

Queste informazioni sono dette anche chiave del codice.

Cifrario di Cesare

Identifichiamo $\mathbb{Z}_{26}$ con l'alfabeto:

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8
J	K	L	M	N	O	P	Q	R
9	10	11	12	13	14	15	16	17
S	T	U	V	W	X	Y	Z	
18	19	20	21	22	23	24	25	

Scelta una chiave k in $\mathbf{Z}_{26}$,si cifra lettera per lettera

CIFRATURA:

$x \to x+k \pmod{26}$

DECIFRATURA:

$y \to y-k \pmod{26}$

Ex. per k=3 si cifra

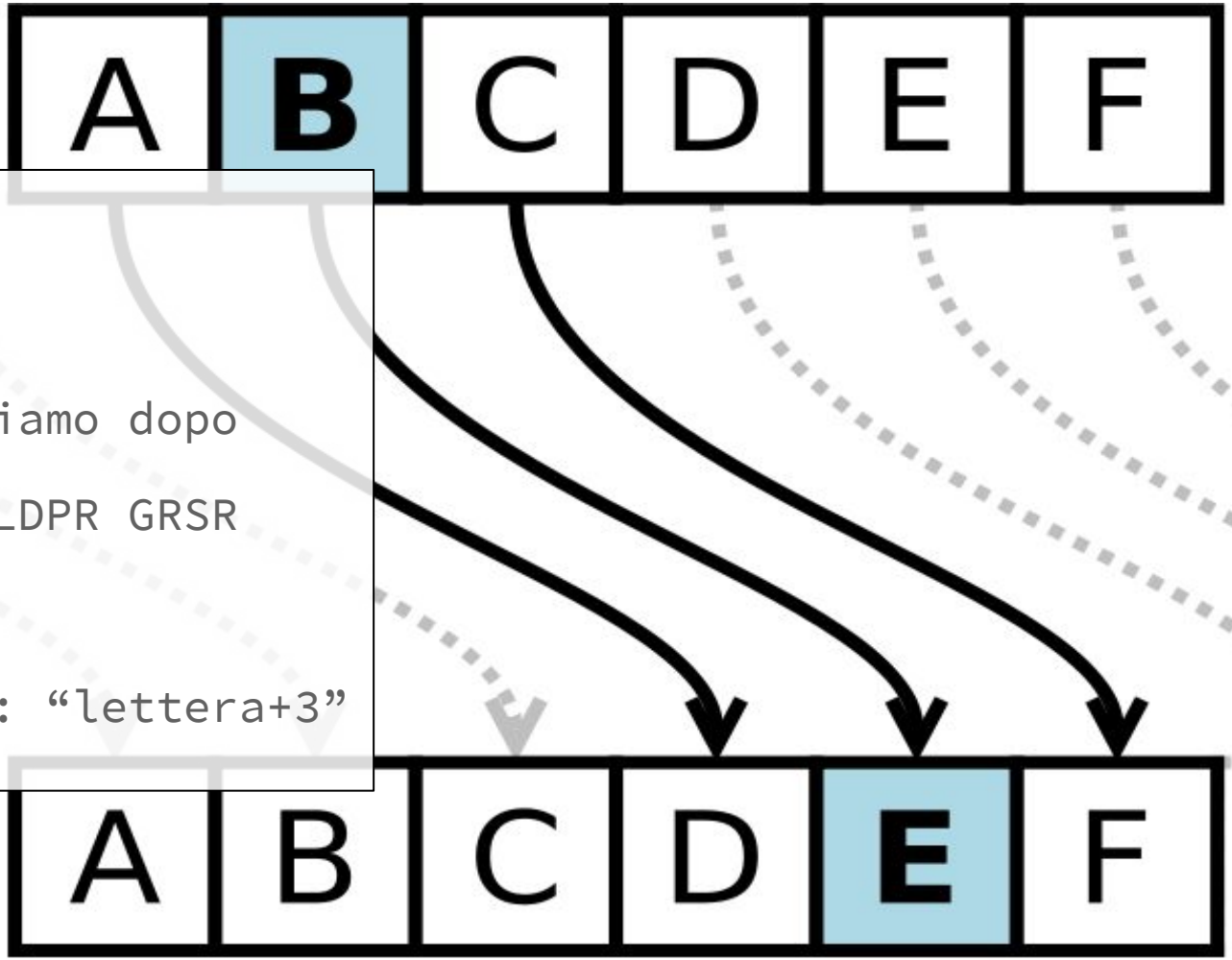
a → D, b → E, … z → C

Esempio

Ci vediamo dopo

FL YHGLDPR GRSR

Regola: “lettera+3”



Sicurezza ?

Un cifrario che sostituisce lettera a lettera non sarà mai sicuro: non nasconde la regolarità della lingua, bastano poche righe di testo per attaccarlo.

ESEMPIO:

Oh exjlh kdqqr oh jdpeh fruwh

- La H è la lettera più frequente ed è sempre a fine parola: sarà probabilmente una tra le vocali più frequenti.
- Le due lettere “OH” formano una parola a sé stante e piuttosto frequente: sarà un articolo o una preposizione.

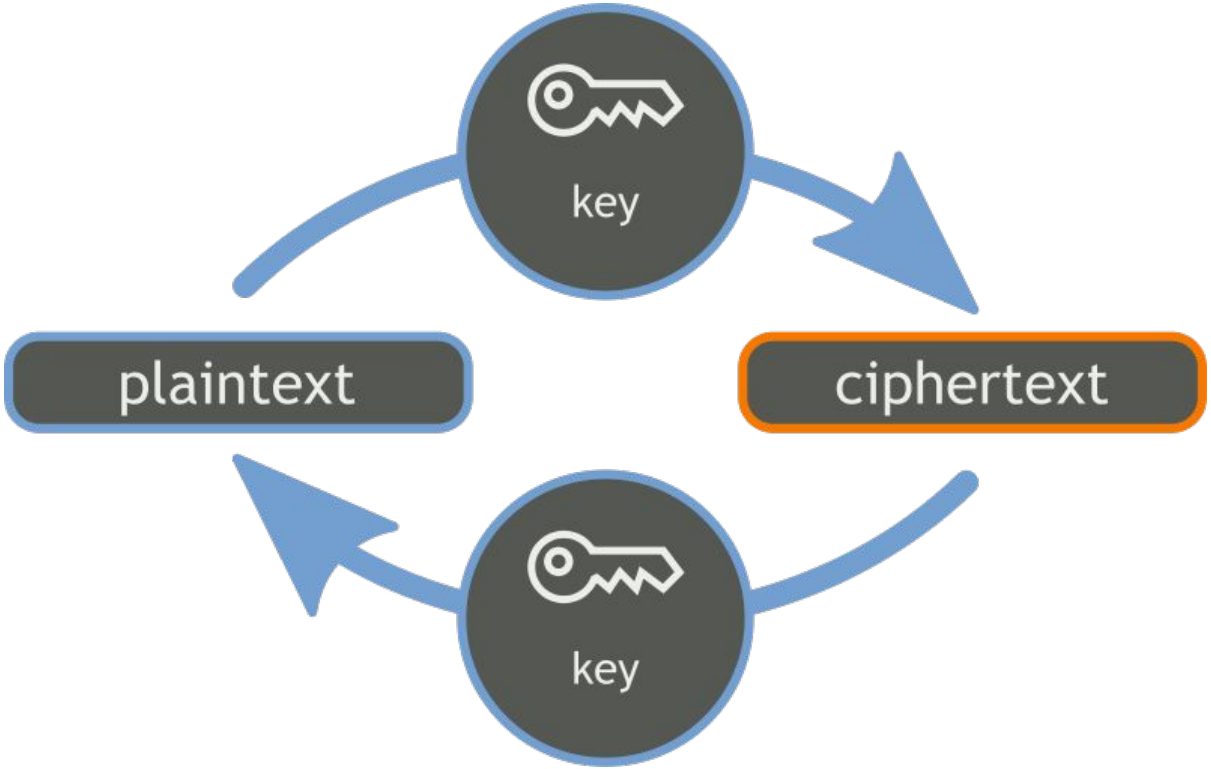
SOLUZIONE:

Le bugie hanno le gambe corte

Crittografia a chiave pubblica

Crittografia Tradizionale o Simmetrica

Nella crittografia tradizionale, Alice e Bob hanno una chiave segreta in comune che usano per cifrare & decifrare

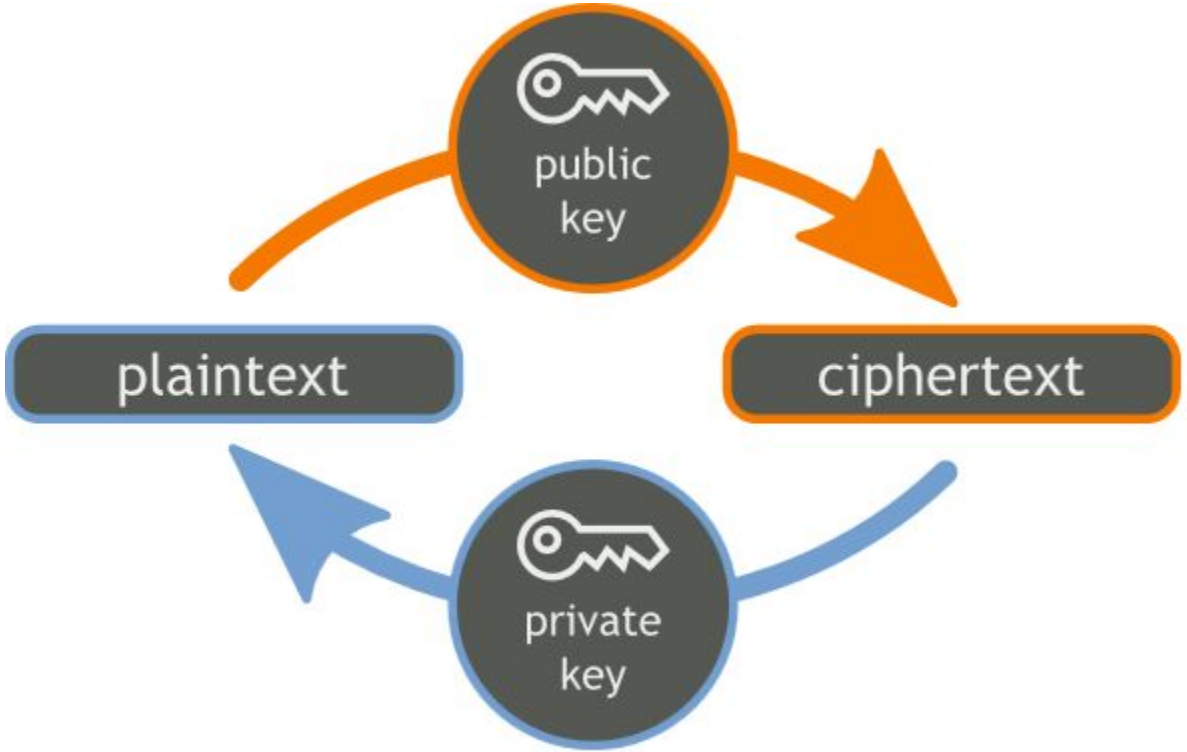


Come Condividere la Chiave?

Prima di cominciare a comunicare, Alice e Bob devono scegliere una chiave segreta comune tramite un canale sicuro - se l'attaccante intercetta la chiave, sono fritti!

Crittografia a chiave pubblica o asimmetrica

Nella crittografia a chiave pubblica si utilizzano due chiavi diverse. Alice ha una chiave pubblica per cifrare il messaggio per Bob e Bob ha una chiave privata per decifrarlo.



Funzioni unidirezionali (one way)

Vogliamo che sia facile cifrare e difficile decifrare, cosicché tutti possano scrivere a Bob ma solo lui possa capire i messaggi.

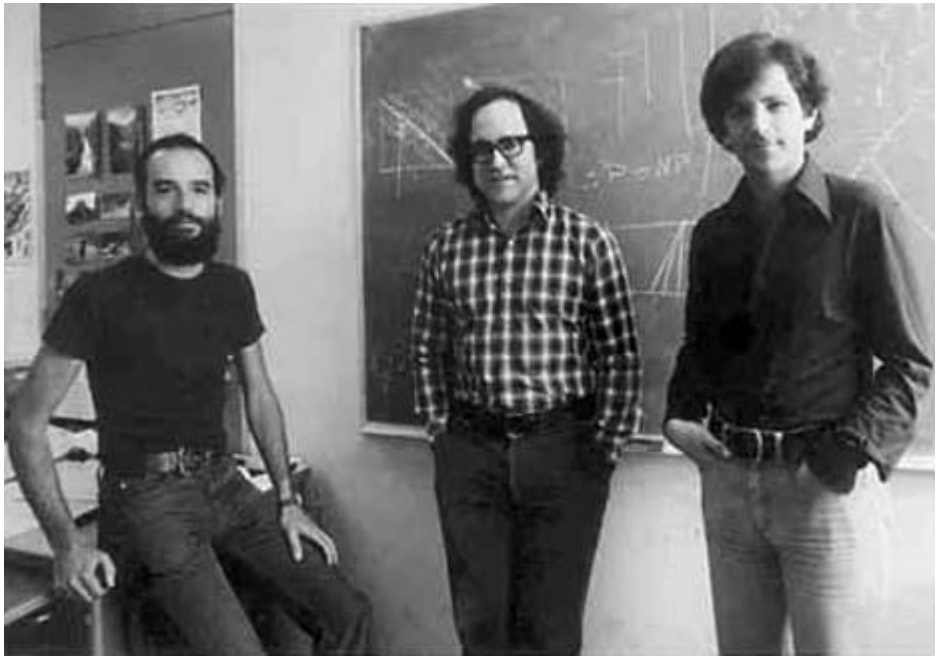
Cerchiamo una funzione unidirezionale: una funzione con cui è facile calcolare la cifratura, ma è difficile tornare indietro, svolgere l'operazione inversa.

Esempio: dati due numeri p e q, è facile calcolare il prodotto N=pq (c'è un algoritmo efficiente)

Ma se si ha un numero grande N trovare i suoi fattori primi è difficile (non si conosce un algoritmo efficiente)

RSA

- Nasce nel 1977 e segna una svolta nella storia della Crittografia; tutti i cifrari precedenti sono a chiave segreta e simmetrica.
- Ron Rivest, Adi Shamir e Leonard Adleman (MIT) definiscono un metodo chiamato con l'acronimo dei tre cognomi: RSA.



Come Funziona l'RSA?

Immaginiamo che Alice debba spedire un messaggio segreto a Bob.

1. Bob sceglie un numero intero **N** che viene reso pubblico: CHIAVE PUBBLICA.
2. **N** è il prodotto di due numeri primi **p** e **q** che devono restare segreti: CHIAVE PRIVATA.
3. Bob invia il numero **N** ad Alice. Chiunque può vedere questo numero.
4. Alice usa questo numero **N** facendo delle operazioni per cifrare il messaggio e manda il messaggio a Bob. Chiunque può vedere ma non comprendere il messaggio cifrato.
5. Bob riceve il messaggio e utilizzando i due numeri primi **p** e **q**, che solo lui conosce, decifra il messaggio.

CHIAVE PUBBLICA: N
CHIAVE PRIVATA: p e q

Alice usa la chiave pubblica di Bob: N

Bob usa la propria chiave privata: p e q

Nota:
E' facile calcolare $p \cdot q$ ma non è facile risalire a p e q conoscendo soltanto il loro prodotto N.
Se Mr X conosce p e q può leggere i messaggi di Alice per Bob!

Che Matematica c'è dietro l'RSA?

L'idea di base è quella di sfruttare la difficoltà di fattorizzare un numero intero; la chiave pubblica è un numero N ottenuto moltiplicando due numeri primi p e q molto grandi (centinaia di cifre decimali - 1024 o 2048 bit) che restano segreti. Il sistema si basa anche su due risultati matematici dovuti a Fermat e a Eulero: la funzione di Eulero e il teorema di Eulero-Fermat.

RSA è ancora oggi il cifrario a chiave pubblica più usato. Quasi tutte le operazioni sicure sul web (protocollo https) usano oggi certificati basati su RSA.

Qualche Dettaglio

1. Si generano due numeri primi distinti **p** e **q** e si moltiplicano tra di loro ottenendo il numero **N** che viene reso pubblico, mentre **p** e **q** devono restare segreti.
2. Si calcola **Φ(N)** che è la funzione di Eulero di **N**: **Φ(N) = (p-1)(q-1)**. Anche **Φ(N)** deve restare segreto.
3. Si calcola un intero **e** che sia coprimo con **Φ(N)** cioè **MCD(e, Φ(n)) = 1**. Il numero **e** è la chiave pubblica.
4. Si calcola il numero **d** inverso di **e** nell'aritmetica modulo **Φ(n)**, che è il più piccolo **x** per cui sia **ex** = 1 (mod **Φ(n)**); **d** è la chiave segreta, utilizzata per decifrare.

Sfide di fattorizzazione

- **RSA-129**
  114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541
  (Fattorizzato da Atkins e al. nel 1994 usando 1600 computer connessi a Internet in 8 mesi di lavoro.)

- **RSA-576 (174 cifre decimali):**
  188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059
  (Fattorizzato nel 2003 da J. Franke et al.)

- **RSA-640 (193 cifre decimali):**
  310741824049004372135075003588856793003734602284272754572016194882320644051808150455634682967172328678243791627283803341547107310850191954852900733772482278352574238645401469173660247765234660 9
  (Fattorizzato nel 2005 da J. Franke et al.)

Esempio di Modulo RSA

N=5252850926371312949132893768414846544129719246335883878610433587140772648450922320745138
2238978301675398113686917315853597854687126444571483534209745434339415180300493325133401213
8285186482618602382722839180746649136437721396100086885726057024201273106179359692692111712
7519314839251630027808673937042050143293544837282791585278683158643312580930071305968097076
2553211510589226743689006085474394180768946785088082921493881380000114531494045583163820205
4360630938738654295104326266409615768076227919017351522537328753682332646865654068128160807
0107743760542895596928518131298174056944360783322515997278071937923189689731271109406598795
6270071408289484630392569773648667781430800973928830944008451953785837649339616266276502108
2648569046939773144713482748934341516440422693040837484626644252705936380347688442995736683
0714607657848202341079773686442119828972525197058524655012016393603773702840234131582824960
7659143722591961922939708293878377085605342124524468319228285480224266994819525028985564743
3925101281982991020740888224340538912760488246293843737108337289119854407001229130504960254
1444920955860988720109702295608179211515563006193073986607489733458661653628684186970719955
5031796816907312733151 97;