Crittografia

Come fare a nascondere le proprie informazioni

Obiettivi

Capire cos'è la Crittografia

Saper usare certi schemi di crittografia

Comprendere la crittografia e i suoi limiti

Significato

Branca della crittologia che tratta delle scritture nascoste, ovvero dei metodi per rendere un messaggio offuscato in modo da non essere comprensibile a persone non autorizzate a leggerlo

Storia

- Ebrei → atbash
- Spartani → Scitala
- Giulio Cesare → Cifrario di Cesare

Violabilità

Per diverse applicazioni di telecomunicazioni e informatica un sistema si può considerare sicuro anche se il suo sistema di cifratura risulta violabile, ma con tempi di realizzazione che renderebbero poi vani i successivi tentativi di attacco diretto.

Sicurezza

Al momento non esiste alcuna tecnica crittografica che si possa definire sicura in senso assoluto, tranne il **Cifrario di Vernam**: tutte le altre tecniche rendono sicuro il dato solo per un certo arco temporale e non possono garantire la durata della segretezza

Crittografia a chiave privata

A cosa serve

La crittografia è una tecnica usata per rendere visibili le informazioni solo alle persone a cui sono destinate

- Il messaggio che può essere letto da tutti si chiama testo in chiaro

Funzionamento

Tramite i metodi di cifratura (algoritmi di codifica) si trasforma il testo in chiaro in un testo cifrato in cui l'informazione viene resa illeggibile

Operazione inversa

L'operazione inversa viene chiamata decifrazione (eseguita tramite algoritmi di decodifica) serve per ricomporre il testo in chiaro a partire dal testo cifrato


Testo in chiaro
Codifica algoritmo+chiave
Testo cifrato
Decodifica algoritmo+chiave
Testo in chiaro

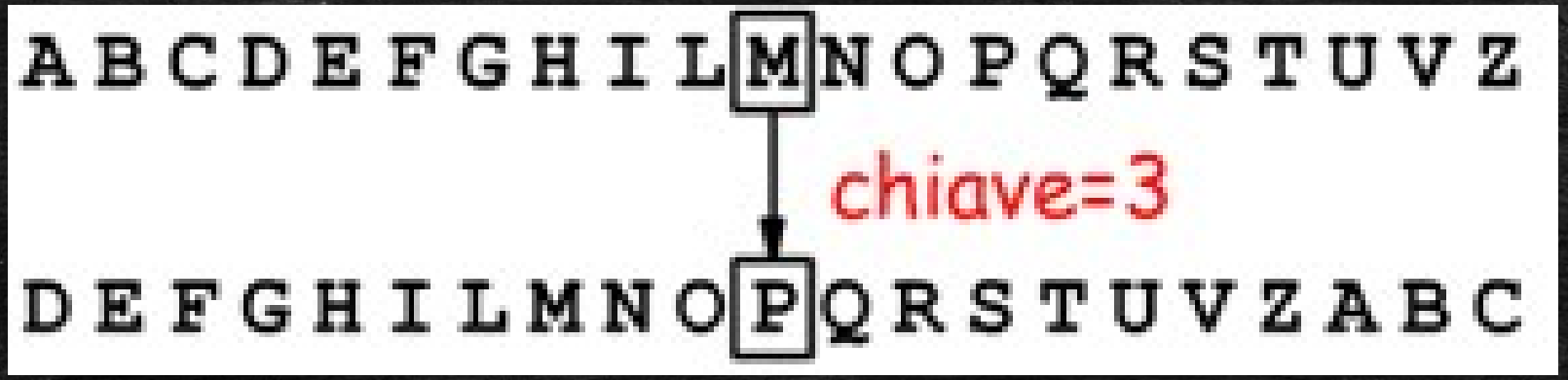
Cifrario di Cesare

Cifrario di Cesare

Tutte le occorrenze di una lettera vengono sostituite da una lettera che dista k posizioni nell'alfabeto

k corrisponde dunque alla chiave di cifratura

Cifrario di Cesare



Cifrario di Cesare – K=3

- Scelgo la chiave pari a 3
- Tutte le ricorrenze della lettera A nel testo vengono sostituite dalla lettera D
- Quelle della lettera B con la lettera E
- Quelle della lettera C con la lettera F

Esercizio

GIULIO CESARE

- Chiave k=3

Soluzione

LNAONR FHVDUH

Esercizio

FAMMI COPIARE

- Chiave k=6

Soluzione

MFRRP HTUFZL

Esercizio senza chiave

Decifra la seguente parola:

- BNLOIHLDMSH, AQZUN

Cifrario di Cesare

Questo tipo di codice viene chiamato anche **cifrario a sostituzione**

Ovviamente il numero di chiavi possibili è molto limitato e la possibilità che la chiave possa essere dedotta è elevato

L'algoritmo di Giulio Cesare non è dunque un cifrario sicuro: esso può essere violato facilmente anche senza conoscere la chiave.

Cifrario a trasposizione

Cifrario a trasposizione

La chiave è una parola che serve per spezzare il messaggio su più righe e successivamente per ordinare le colonne risultanti ottenendo il testo cifrato

Proviamo

Parola:
AVANZARE
FINO AL
FIUME

Chiave:
CAMPO

Cifrario a trasposizione

Si crea una tabella con un numero di colonne uguale al numero di caratteri della parola chiave, e si posiziona sulla prima riga la parola chiave. I caratteri del messaggio vengono distribuiti sulle righe sottostanti, sotto ogni lettera della parola chiave

C	A	M	P	O
A	V	A	N	Z
A	R	E	F	I
N	O	A	L	F
I	U	M	E	.

Cifrario a trasposizione

Se l'ultima riga non è completa, si aggiungono dei caratteri di riempimento (ad es.il punto .)

Il messaggio cifrato viene generato prendendo le colonne della tabella seguendo l'ordine alfabetico

Cifrario a sostituzione

A					C					M					O					P			
V	R	O	U		A	A	N	I		A	E	A	M		Z	I	F	.		N	F	L	E

Cifrario a sostituzione

Il destinatario del messaggio conoscendo la parola chiave è in grado di ricomporre il testo in chiaro individuando le colonne e posizionandole in modo corretto nella tabella

Esercizio

Frase: Nel Dark Web gira di tutto

Chiave: Thanos

Soluzione

T	H	A	N	O	S
N	E	L	D	A	R
K	W	E	B	G	I
R	A	D	I	T	U
T	T	O	.	.	.

Soluzione

T					N				
N	K	R	T		D	B	I	.	
H					O				
E	W	A	T		A	G	T	.	
A					S				
L	E	D	O		R	I	U	.	

One-Pad

Criterio fondamentale

La sicurezza di un sistema informatico deve dipendere solo dalla chiave e non dell'algoritmo usato

One-Pad

Implementazione di cifrari di tipo **one-time pad** dove si utilizza un blocco(pad) di chiavi che vengono generate casualmente che cambiano ad ogni lettera

Lo sviluppo di queste tecniche ha portato al giorno d'oggi alla creazione di generatori di chiavi 'usa e getta' soprattutto nel settore delle transazioni bancarie (o-key)

One-Pad

Regola fondamentale

La chiave utilizzata può essere interpretata come un numero molto grande e la sua dimensione viene misurata in un numero di bit: più grande è la chiave e più difficile sarà il compito di chi vuole infrangere i messaggi cifrati

Regola fondamentale

Una chiave di 40 bit è ritenuta abbastanza sicura

Chi volesse decifrare i messaggi dovrebbero cercare tra 2^{40} possibili chiavi

AES

AES

Progettato sulla base di tre specifiche fondamentali:

- resistenza contro tutti gli attacchi
- velocità e compattezza del codice su un'ampia gamma di piattaforme
- semplicità progettuale

AES

AES è stato il primo standard approvato da NSA per comunicazione crittate ed è tuttora il cifrario a chiave segreta più usato negli ambienti informatici: a oggi non sono conosciuti attacchi in grado di violarlo in tempi accettabili

Punto debole

Il punto debole della crittografia simmetrica rimane, comunque, il fatto che i due interlocutori devono essere in possesso della stessa chiave

Crittografia a chiave pubblica

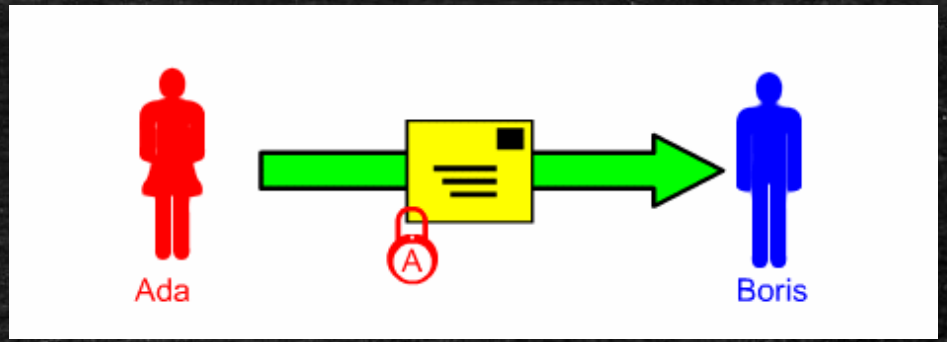
Crittografia asimmetrica

L'idea alla base della crittografia asimmetrica è quello di avere due chiavi diverse

- una pubblica per la criptazione
- una privata per la decriptazione, che deve essere mantenuta segreta

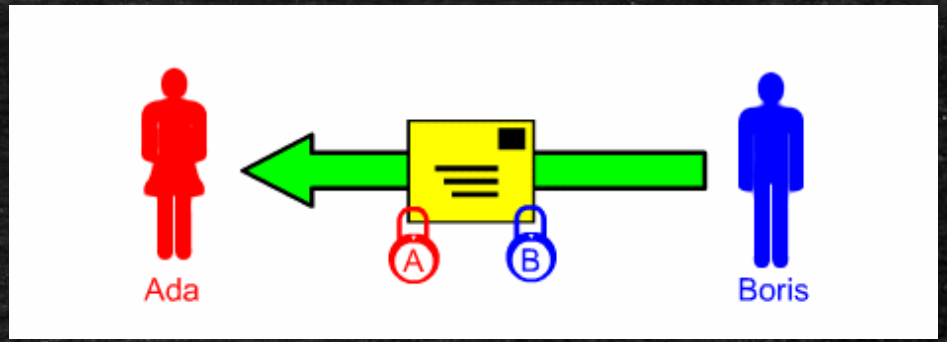
Esempio

1) Ada manda a Boris il messaggio contenuto in una scatola chiusa con un lucchetto: né Boris né eventuali intrusi possono aprirlo



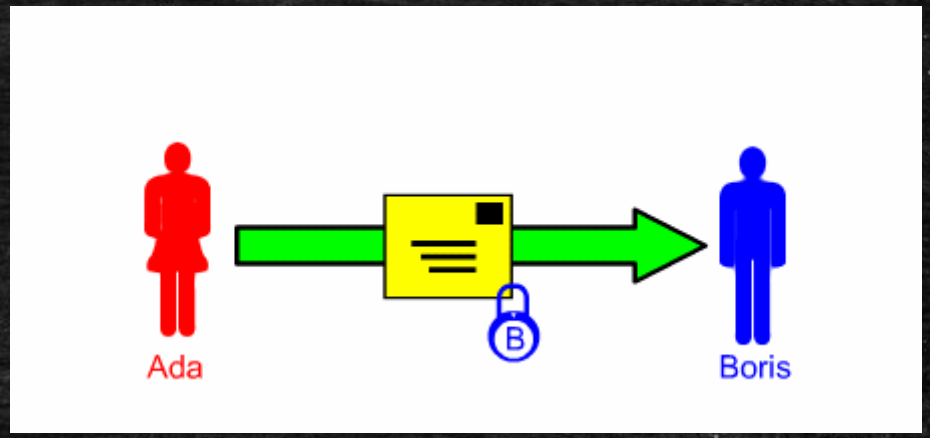
Esempio

2) Boris lo rispedisce ad Ada aggiungendo un suo lucchetto B: nessuno ora è in grado di aprirlo



Esempio

3) Ada toglie il suo lucchetto e rimanda il pacco a Boris, che ora ha solo il suo lucchetto e che alla sua ricezione può aprirlo e leggere il messaggio

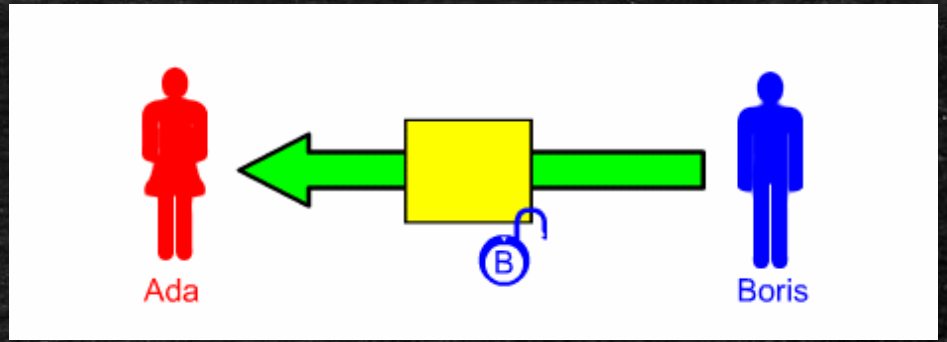


Esempio

Come si vede Ada e Boris non si sono scambiati le chiavi (e non hanno una chiave in comune) , però la procedura è piuttosto macchinosa perché ci sono 3 trasmissioni

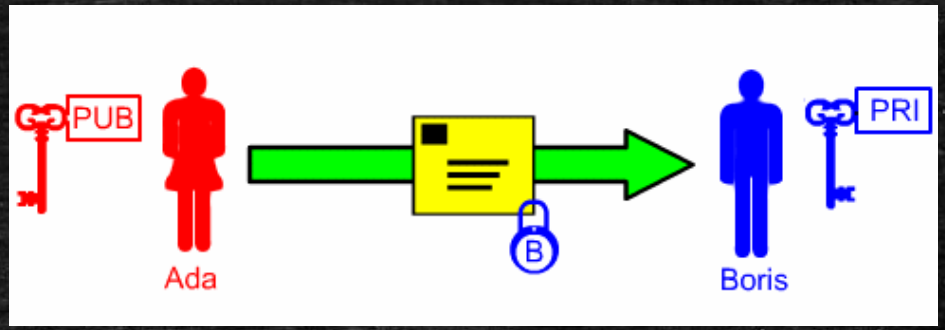
Esempio 2

1) Boris manda ad Ada il proprio lucchetto aperto e questa lo conserva fino a che ha neccesità di spedire qualcosa a Boris



Esempio 2

2) Quando Ada deve spedire un messaggio a Boris, lo chiude con il suo lucchetto e glielo invia



Crittografia asimmetrica

La chiusura del lucchetto viene effettuata con una determinata chiave pubblica che ciascun utente mette a disposizione di tutti gli altri utenti che necessitano di trasmettergli messaggi: la chiave privata è invece segreta, in possesso a ogni utente, che la utilizza per "aprire" il lucchetto e leggere il messaggio

Crittografia asimmetrica

Formalmente è necessario trovare una funzione (il lucchetto) la cui trasmissione su canali insicuri non comprometta l'algoritmo, che sia facile da computare (parte pubblica che chiude il lucchetto) ma difficile da invertire (parte privata che apre il lucchetto)

RSA (difficile)