

CRITTOGRAFIA

È lo studio di tecniche matematiche per

. mascherare i messaggi (crittografia); ⁽¹⁾

. tentare di svelarli (crittoanalisi). ⁽²⁾

Si ricorre a "metodi di ciphatura" ⁽¹⁾

Si ricorre a "metodi di interpretazione" ⁽²⁾

SCENARIO

Un agente Alice vuole comunicare con un agente Bob attraverso un canale non sicuro (ie è possibile intercettare i messaggi):

Alice spedisce un messaggio in chiaro in sotto forma di

crittogramma e in modo tale che:

- Eve, crittoanalista in ascolto, lo trovi incomprensibile

(tipicamente decifrabile in tempo esponenziale)

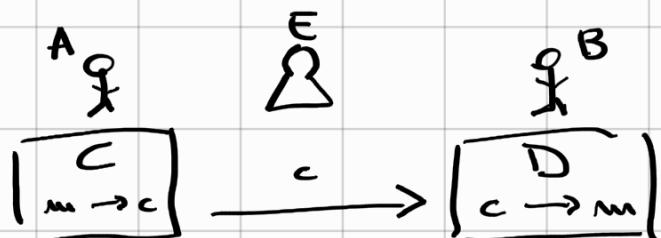
- facilmente comprensibile a Bob

(polinomiale)

La ciphatura è una funzione $C : \text{MSG} \rightarrow \text{CRITTO}$ iniettiva

decifrare

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



Vale che $D(C(m)) = m$ i.e. sono una

l'inversa dell'altra

. C e' iniettive

i.e. messaggi diversi

implicano critogrammi diversi

CIFRARIO DI CESARE

Il critogramma c e' ottenuto dal messaggio m sostituendo ogni lettera di m con quella tre posizioni più avanti

a	b	c	u	v	w
↓	↓	↓	↓	↓	↓
d	e	f	a	b	c

La segretezza dipende dalla conoscenza del metodo (se e' segreto allora la comunicazione e' sicura)

Era un cifrario per uso ristretto (poche persone lo conoscevano)

Si introduce il concetto di livello di segretezza:

- cifrari per uso ristretto ⁽³⁾

- cifrari per uso generale ⁽⁴⁾

(3): C, D vengono tenute segrete

Inadatti → crittografia a chiave

(4): La parte segreta del metodo e' limitata a una informazione aggiuntiva (chiave)

D, C pubbliche, chiave segreta

L'idea di base e' che ogni codice segreti non potra' essere mantenuto tale a lungo.

IL NEMICO CONOSCE IL SISTEMA:

Un cifrario deve restare sicuro anche se D,C sono note.

CIFRARIO PER USO GENERALE

C,D note

K chiave segreta

• diversa per ogni coppia di utenti

• parametro di D,C

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

• ha conoscenza dei sali C,D (senza K)

non deve permettere di estrarre informazioni

sul messaggio in chiaro

• Tenere segreta la chiave è più semplice

che tenere l'intero processo

• Tutti possono usare le stesse C,D

• Cambiare chiave rende i messaggi nuovamente

sicuri

Se la segretezza del messaggio dipende solo dalla chiave

• il numero delle chiavi possibili deve essere così grande da rendere impraticabile provare tutte

• Le chiavi devono essere scelte in modo casuale

ATTACCO ESAURIENTE

Se crittoanalista puo' saperne un attacco esauriente
verificando $\forall k$ la significativita' di $D(c, k)$

Avere un insieme delle chiavi grande non e' perciò
sinonimo di sicurezza

CRIPTOANALISTA

Puoi effettuare due tipi di attacchi:

attacco passivo: non interviene sul canale, osserva
il canale e non cambia le
comunicazioni

attacco: modifica il contenuto dei
messaggi, finge di essere Alice etc

L'obiettivo e' quello di fortare il sistema, si ricorrono a:

seguenti tipi di attacchi:

Cypher text attack consente un insieme di crittogrammi

known plain text attack consente alcune coppie (messaggio, crittogramma)

chosen plain text attack si procura una serie di coppie
(messaggio, crittogramma) relative a m scelti

chosen cypher text attack si procura una serie di coppie

(messaggio, crittogramma) relative a c scelti
prova tutte le chiavi

brute force attack

Man in the middle si inserisce nel sistema e

comunicazione e si finge Alice / Bob

Un attacco può portare a scoprire D o qualche
informazione su un messaggio o dei bit della chiave

Esistono CIFRARI PERFETTI (i.e. inaffidabili), richiedono
operazioni estremamente complesse e sono utilizzati
in condizioni estreme. Sono inaffidabili anche se
si dimostra che $P = NP$.

Il ciphogramma e il messaggio in chiaro risultano
completamente sconnessi; ottenere ciphogrammi
non modifica la conoscenza di Eve.

ONE TIME PAD

Richiede una chiave casuale utilizzabile una e una
sola volta, lunga quanto il messaggio.

I problemi sono generare e sconfiggere la chiave.

I cifrari moderni sono sicuri (non perfetti):

- sono inviolati da attacchi di esperti;
- il crittoanalista ha bisogno di risolvere problemi complessi.

Sono sicuri finché $P \neq NP$.

AES

- E' standard per comunicazioni riservate ma non classificate
- Usa chiavi brevi
- E' pubblico
- E' simmetrico, a blocchi (divide il messaggio in blocchi lunghi quanti le chiavi)

Esiste un sistema per scambiare chiavi segrete in chiaro (Protocollo DH).