CRITTOGRAFIA: introduzione

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

Due gruppi di persone

- persone che applicano metodi di cifratura alle loro conversazioni per renderle incomprensibili ai non autorizzati
- persone che sviluppano metodi di crittoanalisi per riportare alla luce le informazioni contenute in quelle conversazioni

Terminologia

Crittografia

metodi di cifratura

Crittoanalisi

metodi di interpretazione

Crittografia + Crittoanalisi
=
CRITTOLOGIA
studio della comunicazione su
canali non sicuri e relativi problemi

Crittologia: lo scenario

- Un agente **Alice** vuole comunicare con un agente **Bob**, e deve utilizzare un canale di trasmissione **insicuro**
  - è possibile intercettare i messaggi che vi transitano.
- Per proteggere la comunicazione i due agenti devono adottare un **metodo di cifratura**

  Alice spedisce un messaggio in chiaro **m** sotto forma di testo cifrato (crittogramma) **c**, che deve essere:
  - incomprensibile al crittoanalista Eve in ascolto sul canale,
  - facilmente decifrabile da Bob.

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

$$D: \ CRITTO \rightarrow MSG$$

Schema di comunicazione

m —C→ c

c

c —D→ m

Schema di comunicazione

???

m —C→ c

TT NT V

c —D→ m

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

Cifrari storici: altri esempi

Enea Tattico, Grecia, IV secolo a.C.:

opera militare con un capitolo dedicato ai messaggi segreti

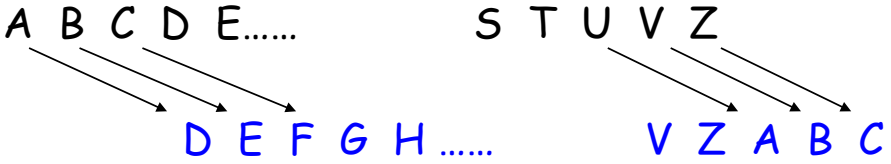
- inviare un libro qualsiasi sottolineandovi un sottoinsieme di lettere che costituiscono il messaggio
- sostituire le vocali di un testo con altri simboli grafici

Cifrario di Cesare

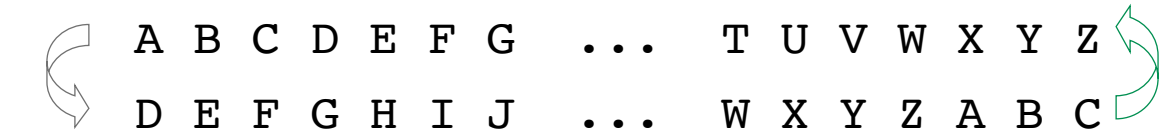
È il più antico cifrario di concezione moderna (Svetonio, *Le vite di dodici Cesari)*

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 comprometterne irrimediabilmente l'impiego

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

Cifrari per uso generale

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

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.

Cifrari per uso generale

- Tenere segreta la chiave è più semplice che tenere segreto l'intero processo di cifratura e decifrazione.
- Tutti possono impiegare le funzioni pubbliche **C** e **D** scegliendo chiavi diverse.
- Se un crittoanalista entra in possesso di una chiave occorre solo generarne una nuova, le funzioni **C** e **D** rimangono inalterate.
- Molti cifrari in uso (3DES, RC5, IDEA, AES) sono a chiave segreta.

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

Attacco esauriente

- Il crittoanalista potrebbe sferrare un **attacco esauriente** verificando la significatività delle sequenze D(c,k), ∀ chiave k.
- Se

  |Key| = 10^{20} e un calcolatore impiegasse 10^{-6} secondi per calcolare D(c,k) e verificarne la significatività,

  occorrerebbe in media più di un milione di anni per scoprire il messaggio provando tutte le chiavi possibili.

Osservazione

La segretezza può essere violata con altre tecniche di crittoanalisi.

Esistono cifrari più sicuri di altri, pur basandosi su uno spazio di chiavi molto più piccolo:

1. un cifrario complicato non è necessariamente un cifrario sicuro;
2. mai sottovalutare la bravura del crittoanalista.

Crittoanalista (Eve)

- Comportamento passivo

  Eve si limita ad ascoltare la comunicazione

- Comportamento attivo

  Eve agisce sul canale disturbando la comunicazione o modificando il contenuto dei messaggi

Attacchi a un sistema crittografico

- Hanno l'obiettivo di **forzare** il sistema.
- Metodo e livello di pericolosità dipendono dalle informazioni in possesso del crittoanalista:
  - Cipher Text Attack (solo testo cifrato)

    il crittoanalista rileva sul canale una serie di crittogrammi

    $c_1, \ldots, c_r$
  - Known Plain-Text Attack (testo in chiaro noto)

    il crittoanalista conosce una serie di coppie

    $(m_1, c_1), \ldots, (m_r, c_r)$
  - Chosen Plain-Text Attack (testo in chiaro scelto)

    il crittoanalista si procura una serie di coppie $(m_1, c_1), \ldots, (m_r, c_r)$ relative a messaggi in chiaro da lui scelti.

Attacchi "Man in-the-middle"

Il crittoanalista si installa sul canale di comunicazione

- interrompe le comunicazioni dirette tra i due utenti Alice e Bob
- le sostituisce con messaggi propri
- convince ciascun utente che tali messaggi provengano legittimamente dall'altro

Eve si finge Alice agli occhi di Bob
e Bob agli occhi di Alice

Attacchi

L'attacco al sistema può essere portato a termine con pieno successo

- *si scopre la funzione D*

o con successo più limitato

- *si scopre solo qualche informazione su un particolare messaggio*
- *L'informazione parziale può essere sufficiente per comprendere il significato del messaggio.*

Situazione attuale

Cifrari perfetti (inattaccabili)

esistono, ma richiedono operazioni estremamente complesse e sono utilizzati solo in condizioni estreme.

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

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

Situazione attuale

I **cifrari** diffusi in pratica non sono perfetti, ma sono **dichiarati sicuri** perché

- rimasti inviolati dagli attacchi degli esperti
- per violarli è necessario risolvere problemi matematici estremamente difficili.

Cifrari dichiarati sicuri

Il prezzo da pagare per forzare il cifrario è troppo alto perché valga la pena sostenerlo

l'operazione richiede di impiegare giganteschi calcolatori per tempi incredibilmente lunghi.

impossibilità pratica di forzare il cifrario

Cifrari dichiarati sicuri

Tuttavia non è noto se:

la risoluzione di questi problemi matematici richieda **necessariamente** tempi enormi

oppure se:

i tempi enormi di risoluzione siano dovuta alla nostra incapacità di individuare metodi più efficienti di risoluzione.

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)

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

e le chiavi ?

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 devono stabilirla comunicando "in sicurezza" senza poter ancora usare il cifrario...

Una intercettazione nell'operazione di scambio della chiave pregiudica il sistema

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

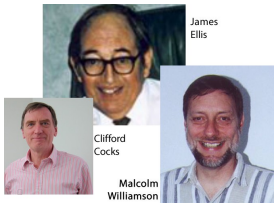
Turing Award 2015

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

Cifrari a chiave pubblica (asimmetrici)

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_{pub} per cifrare: è **pubblica**, nota a tutti;

k_{priv} per decifrare: è **privata**, nota solo a BOB

Cifrari a chiave pubblica

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

$$c = C\ (m,\ k_{pub})$$

chiave k_{pub} e funzione di cifratura sono note a tutti

La decifrazione è eseguita da BOB come

$$m = D\ (c,\ k_{priv})$$

la funzione di decifrazione è nota a tutti, ma k_{priv} non è disponibile agli altri

Cifrari a chiave pubblica

La cifratura è accessibile a tutti, perché tutti conoscono la chiave pubblica: C (m, k[pub])

La decifrazione è accessibile solo a chi possiede la chiave privata: D (c, k[priv])

Sistemi a chiave pubblica: asimmetrici

Sistemi a chiave privata: simmetrici

Crittografia a chiave pubblica

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

calcolare $c = C(m, k_{pub})$ è computazionalmente facile

decifrare c è computazionalmente difficile

a meno che non si conosca un meccanismo segreto, rappresentato da k_{priv} (trap-door)

facile da calcolare ...

e difficile da invertire ...

a meno che non si conosca la trap-door!

Adleman Shamir Rivest

RSA (1977)

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

Turing Award 2002

Comunicazione molti a uno

Schema di comunicazione molti a uno:

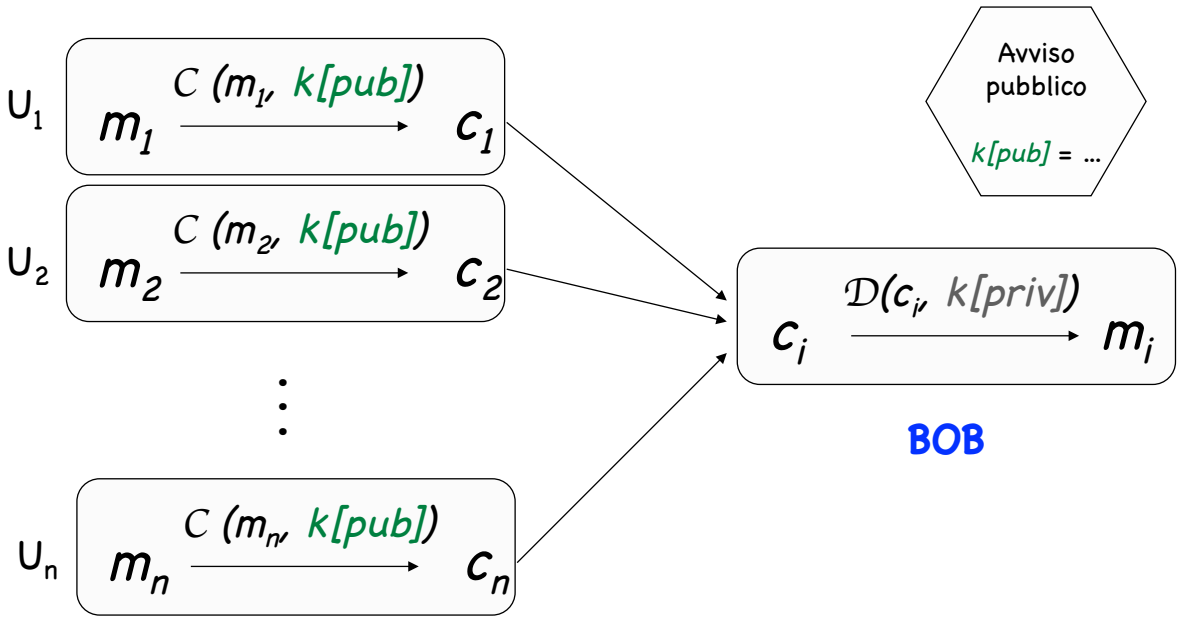
Tutti gli utenti possono inviare in modo sicuro messaggi a uno stesso destinatario

cifrandoli con la funzione C e la chiave k[pub] che sono pubbliche,

Solo il destinatario può decifrare i messaggi.

Un crittoanalista non può ricavare informazioni sui messaggi pur conoscendo C, D e k[pub]

Comunicazione molti a uno



Crittografia a chiave pubblica

VANTAGGI

- Se gli utenti di un sistema sono *n*, il numero complessivo di chiavi (pubbliche e private) è *2n* anziché *n(n-1)/2*
- Non è richiesto alcuno scambio segreto di chiavi

SVANTAGGI

- Questi sistemi sono molto più lenti di quelli basati sui cifrari simmetrici
- Sono esposti ad attacchi di tipo *chosen plain-text*

Attacchi *chosen plain-text*

Un crittoanalista può

- scegliere un numero qualsiasi di messaggi in chiaro $m_1, \ldots, m_h$
- cifrarli con la funzione pubblica C e la chiave pubblica k_{pub} del destinatario, ottenendo i crittogrammi $c_1, \ldots, c_h$
- quindi può confrontare qualsiasi messaggio cifrato c^* che viaggia verso il destinatario con i crittogrammi in suo possesso

Cifrari ibridi

- Si usa un cifrario a chiave segreta (AES) per le comunicazioni di massa
- e un cifrario a chiave pubblica per scambiare le chiavi segrete relative al primo, senza incontri fisici tra gli utenti
- La trasmissione dei messaggi lunghi avviene ad alta velocità, mentre è lento lo scambio delle chiavi segrete
  - le chiavi sono composte al massimo da qualche decina di byte
  - attacco chosen plain-text è risolto se l'informazione cifrata con la chiave pubblica (chiave segreta dell'AES) è scelta in modo da risultare imprevedibile al crittoanalista

Applicazioni su rete

Oltre alla segretezza delle comunicazioni, i sistemi crittografici attuali devono garantire:

① l'**identificazione** dell' utente

② l'**autenticazione** di un messaggio

③ la **firma digitale**

Identificazione

Il sistema deve accertare l' identità di chi richiede di accedere ai suoi servizi

Autenticazione

Bob deve accertare che il messaggio ricevuto è stato effettivamente spedito da Alice

- Un intruso non deve potersi spacciare per un altro utente

Bob deve poter stabilire che il messaggio non è stato modificato o sostituito durante la trasmissione.

Firma digitale

Una volta apposta la "firma" Alice non può ricusare la paternità di un messaggio spedito a Bob

Bob può dimostrare a terzi che il messaggio ricevuto è di Alice

Altre applicazioni

- trasmissione protetta di dati sulla rete (protocollo SSL)
- terminali per le carte bancarie
- moneta elettronica (BITCOIN)
- dimostrazioni a conoscenza zero
- applicazioni crittografiche dei fenomeni di meccanica quantistica