Crittografia

Federico Matteoni

A.A. 2020/21

Indice

Introduzione

Prof.ssa: Anna Bernasconi.
Vedremo i cifrari da un punto di vista prettamente algoritmico. Vedremo anche i cifrari storici, ormai non più utilizzabili, perché hanno "aperto la strada", per poi passare ai cifrari perfetti (soluzione ideale ma con costo elevato).
Poi esamineremo i cifrari simmetrici, a chiave pubblica, curve ellittiche, firma digitale, SSL. Protocolli zero knowledge, blockchain e crittografia quantistica.

Libro di testo: Bernasconi, Ferragina, Luccio - Elementi di Crittografia.

Esame Orali nel caso di esami a distanza, scritto nel caso di esami in presenza, closed-book.

Capitolo 1

Introduzione alla Crittografia

1.1 Introduzione

Crittografia Significa "*scrittura nascosta*", si intendono tecniche matematiche per mascherare i messaggi per non renderli leggibili a terzi (**crittografia**) o tentare di svelarli quando non si è il legittimo destinatario (**crittoanalisi**). Quindi tecniche di protezione e viceversa.
Esiste per i due mondi in contrapposizione: persone che vogliono scambiarsi privatamente informazioni e gli *impiccioni* che desiderano ascoltare o intromettersi nelle conversazioni altrui (per curiosità, investigazione o altri scopi).

Due gruppi di persone Chi vuole proteggersi userà **metodi di cifratura**, gli altri useranno **metodi di crittoanalisi**

Crittografia Metodi di Cifratura

Crittoanalisi Metodi di . . . **crittologia** studio comunicazione canali non sicuri e relativi problemi

1.1.1 Lo scenario

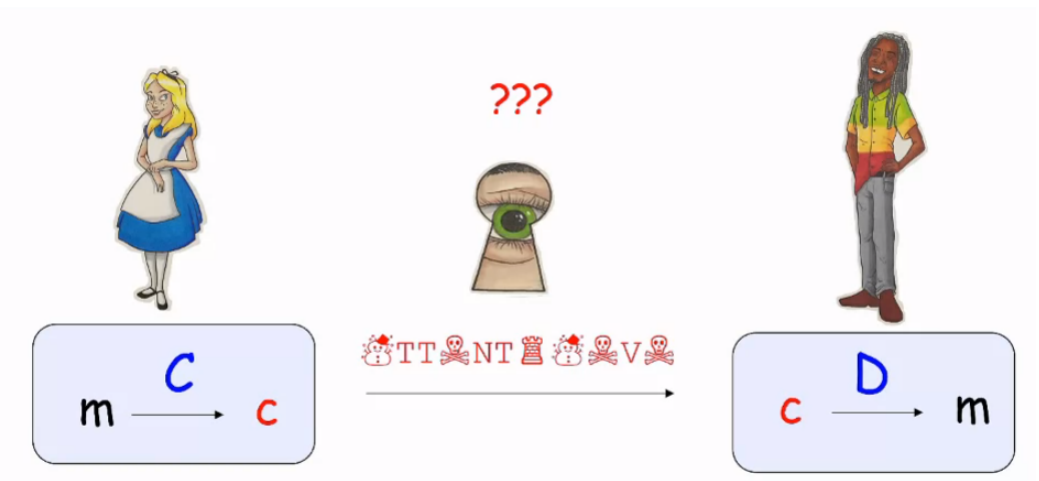
Alice vuole comunicare con Bob su un canale insicuro, quindi adottano un metodo di cifratura per spedire il messaggio in chiaro `m` sottoforma di crittogramma `c` (testo cifrato) che deve essere: incomprensibile al crittoanalista Eve (eavesdropper) in ascolto sul canale, ma facilmente decifrabile da Bob.

MSG Insieme dei messaggi in chiaro

CRITTO Insieme dei crittogrammi

$$C : MSG \to CRITTO$$
$$D : CRITTO \to MSG$$

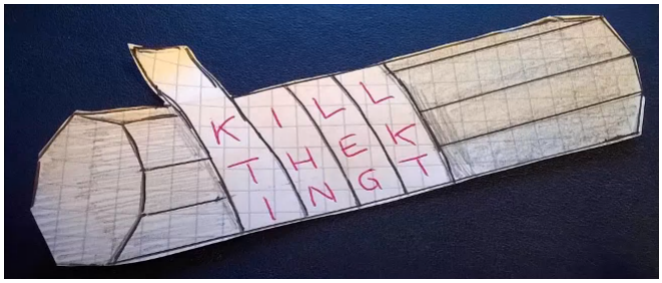
Sono operazioni da poter fare in tempo polinomiale. C e D sono una l'inversa dell'altra, ma C **deve essere iniettiva**.



1.1.2 Antichi esempi

Erodoto Nelle *Storie*, V secolo a.C.
Messaggi tatuati sulla testa, coperti dai capelli e riscoperti rasando la testa.

Scitale Spartani. Asta cilindrica in due esemplari identici. Si avvolgeva una striscia di carta attorno al cilindro e scritta. La chiave del cifrario è il diametro dello scitale.



Enea Tattico Un libro qualsiasi con un insieme di lettere segnate, o sostituire le vocali con simboli grafici.

Cifrario di Cesare Il più antico cifrario di concezione moderna. L'idea di base è che il crittogramma è ottenuto dal messaggio in chiaro `m` sostituendo ogni lettera con quella di tre posizioni più avanti nell'alfabeto.
Es. A $\to$ D, Z $\to$ C. La segretezza dipende interamente dalla conoscenza del metodo, era destinato all'uso ristretto da un piccolo gruppo di persone.

1.2 Livello di segretezza

Classificazione in base al livello di segretezza

> Cifrari per **uso ristretto**
> Le tecniche con cui si calcola e decifra il crittogramma sono tenute segrete in ogni loro aspetto. Impiegati per comunicazioni classificate (diplomatiche o militari), non adatti per uso di massa.
>
> Cifrari per **uso generale**
> Ogni codice segreto non può essere mantenuto tale per troppo a lungo. La parte segreta si limita alla chiave, nota solamente agli utenti che stanno comunicando.
> Vengono studiati dalla comunità, coinvolgendo tantissime persone. Solo la chiave deve essere segreta.
> **Il nemico conosce il sistema**.
> Quindi C e D sono note, la chiave **segretak** è usata come input sia in C che in D:
> `c = C(m, k)`, `m = D(c, k)`
> Se non si conosce `k`, anche conoscendo C e D non si possono estrarre informazioni dal crittogramma.
> Tenere segreta una sola chiave è più facile che segretare l'intero metodo. Tutti possono usare C e D pubbliche con chiavi diverse, e se un crittoanalista entra in possesso di una chiave posso generarne semplicemente una nuova.

1.2.1 Chiavi segreta

Se la segretezza dipende unicamente dalla chiave bisogna proteggersi dagli attacchi a forza bruta, quindi avere un gran numero di chiavi, così da essere immuni da chi le prova tutte.
Inoltre la chiave deve essere scelta in modo casuale e non prevedibile, sennò il crittoanalista può provare le chiavi ovvie.

Attacco esauriente Il crittoanalisa potrebbe sferrare un attacco a forza bruta verificando la significatività delle sequenze `D(c, k)` $\forall$ `k`.
Se $|\text{Key}| = 10^{20}$ e con un calcolatore che impiega 10^{-6} per calcolare `D(c, k)` servirebbe in media più di un milione di anni per scoprire il messaggi provando tutte le chiavi. Però la segretezza può essere violata con altre tecniche: esistono cifrari più sicuri di altri pur con uno spazio di chiavi più piccoli.
Un cifrario complicato non è necessariamente più sicuro e **mai sottovalutare la bravura del crittoanalista**.

1.2.2 Crittoanalista

Attacchi a un sistema crittografico Hanno l'obiettivo di forzare un sistema. Il metodo e il livello di pericolosità dipendono dalle informazioni in possesso del crittoanalista:

Cipher Text Attack: conosce una serie di crittogrammi

Known Plain-Text Attack: conosce una serie di coppie `(m, c)`

Chosen Plain-Text Attack: si procura coppie `(m, c)` relative a messaggi in chiaro da lui scelti. Tutta la crittografia a chiave pubblica è soggetta.

Man in the Middle

Esiti

Successo pieno, si scopre completamente D o si ottiene la chiave

Successo limitato, si scopre solo qualche informazione ma sufficiente per comprendere il messaggio

1.2.3 Situazione attuale

Cifrari perfetti Inattaccabili, esistono ma richiedono operazioni complesse e chiavi lunghe tanto quanto il messaggio e mai riusabili.
Shannon, 1945 (pubblicato nel 1949 per motivi di segretezza militare): `m` e `c` appaiono totalmente scorrelati, come se `c` fosse una stringa casuale di bit.
Nessuna informazione può filtrare dal crittogramma. Vedremo la teoria matematica.

One-Time Pad Anche detto blocco monouso, sicuro ma per essere usato bene richiede chiavi segrete totalmente casuali e lunghe quanto il messaggio. Come generarla e come scambiarla?

Cifrari attuali Nella crittografia di massa non si usano cifrari perfetti, ma cifrari **dichiarati** sicuri, inviolati dagli esperti e che usano algoritmi solo esponenziali per decrittare senza chiave. Il tempo per violare un cifrario è enorme e rende l'operazione insostenibile → impossibilità *pratica* di forzare il cifrario.

Dichiarati sicuri Non è noto se questi problemi matematici richiedano algoritmi *necessariamente* esponenziali o se sono dovuti all'incapacità nostra di trovare metodi più efficienti. Si riconduce a $P?NP$

1.2.4 Cifrari odierni

Advanced Encryption Standard AES, simmetrico a blocchi con chiavi di 128-256bit, pubblicamente noto e realizzabile su computer di ogni tipo. Il messaggio è diviso a blocchi lunghi quanto la chiave.

Le chiavi Sono stabilite dai mezzi elettronici (PC, smartphone, terminale...) e su Internet si scambia una chiave per ogni sessione.

Scambio delle chiavi La chiave va comunicata in sicurezza su un canale non ancora sicuro. Un'intercettazione nello scambio della chiave compromette il sistema.
Nel 1976 viene proposto un algoritmo per generare e scambiare una chiave segreta su un canale insicuro, senza necessità di scambiare informazioni o di incontrarsi in precedenza.
Si chiama **protocollo DH**, ancora largamente utilizzato nei protocolli crittografici su Internet.
Si scambiano pezzi di chiave tramite la rete e unendole a informazioni locali si costruisce la chiave.

Chiave pubblica Diffie ed Hellman hanno anche proposto la crittografia a chiave pubblica.

Cifrari simmetrici: stessa chiave per cifrare e decifrare, nota solo ai due utenti che comunicano. La scelgono di comune accordo e la tengono segreta.

Cifrari asimmetrici: chiavi pubbliche usate per cifrare e chiavi private per decifrare.
`c = C(m, k`$_{pub}$`)`
`m = D(m, k`$_{prv}$`)`
Si rende necessario che la C sia una one-way trapdoor: calcolare il crittogramma deve essere facile (polinomiale), ma decifrare `c` deve essere computazionalmente difficile (a meno di conoscere la trapdoor, la chiave privata).

RSA Rivest, Shamir, Adleman, 1977. Propongono un sistema a chiave pubblico facile da calcolare e difficile da invertire.

Vantaggi

Comunicazione molti a uno
Tutti possono inviare in modo sicuro allo stesso destinatario usando la sua chiave pubblica, ma solo lui può decifrarli. Un crittoanalista non può decifrare anche se conosce C, D e k_{pub}

Se n utenti vogliono comunicare servono solo $2n$ chiavi invece delle $n(n-1)/2$ necessarie nei cifrari simmetrici (una coppia per ogni coppia di utenti)

Non è richiesto nessun scambio

Svantaggi

Sono molto lenti rispetto ai cifrari simmetrici (polinomi di terzo grado)

Sono esposti ad attacchi di tipo chosen plain-text, perché conosco la chiave pubblica
Scelgo un numero qualsiasi di messaggi in chiaro, costruisce i crittogrammi relativi e ascolta sul canale confrontando i crittogrammi in transito e se trova un riscontro sa esattamente qual è il messaggio passato.

Come si usa Oggi 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.
Diventa lento solo lo scambio delle chiavi. Siamo anche al sicuro da attacchi chosen plain-text perché se la chiave è scelta bene risulta imprevedibile dal crittoanalista.