Introduzione

Crittografia

Luciano Margara

Unibo

2022

Introduzione e cenni storici

Crittografia significa "scrittura nascosta"

Introduzione e cenni storici

Due mondi in contrapposizione tra loro: da una parte troviamo persone che vogliono scambiarsi privatamente delle informazioni, dall'altra un nugolo di impiccioni che desiderano ascoltare o intromettersi nelle conversazioni altrui per semplice curiosità, o per legittima investigazione, o peggio per scopi malvagi.

Introduzione e cenni storici

Dire chi siano i "buoni" e chi i "cattivi" è però difficile. A seconda dei casi i buoni possono essere coloro che conversano segretamente o coloro che cercano di intercettarne la comunicazione.

Introduzione e cenni storici

Da un lato abbiamo persone che applicano metodi di cifratura alle loro conversazioni per renderle inintelligibili a chiunque desideri intercettarle senza autorizzazione, dall'altro abbiamo persone che sviluppano metodi di crittoanalisi per riportare alla luce le informazioni contenute in quelle conversazioni.

Introduzione e cenni storici

Non esistono cifrari inattaccabili e facili da utilizzare.

Introduzione e cenni storici

I cifrari più diffusi nella pratica non sono inattaccabili ma possono essere dichiarati sicuri in quanto sono rimasti inviolati agli attacchi degli esperti, oppure perché, per violarli, è necessario risolvere alcuni problemi matematici difficilissimi.

Introduzione e cenni storici

Questo secondo criterio ci lascia naturalmente più tranquilli circa la segretezza della comunicazione, ma è anche più difficile da applicare e implica solo una impossibilità pratica di forzare il cifrario: difficoltà di risoluzione significa in sostanza che il prezzo da pagare (tempo di calcolo) per forzare il cifrario è troppo alto perché valga la pena di sostenerlo.

Crittologia

La crittografia con i suoi metodi di cifratura, e la crittoanalisi con i suoi metodi di interpretazione, sono indissolubilmente legate tra loro e costituiscono di fatto due aspetti di una stessa scienza: la crittologia.

Scenario

Il problema centrale di questa scienza è schematicamente il seguente: un mittente *Mitt* vuole comunicare con un destinatario *Dest* utilizzando un canale di trasmissione insicuro, cioè tale che altri possono intercettare i messaggi che vi transitano per conoscerli o alterarli.

Scenario

Per proteggere la comunicazione i due agenti devono adottare un metodo di cifratura che permetta a *Mitt* di spedire un messaggio m sotto forma di crittogramma c, incomprensibile a un ipotetico crittoanalista X in ascolto sul canale, ma di cui sia facile la decifrazione da parte di *Dest*.

Cifratura e decifrazione

- MSG = spazio dei messaggi
- CRT = spazio dei crittogrammi
- Cifratura (codifica) del messaggio. Operazione con cui si trasforma un generico messaggio in chiaro m in un crittogramma c applicando una funzione $C : MSG \rightarrow CRT$
- Decifrazione (decodifica) del crittogramma. Operazione che permette di ricavare il messaggio in chiaro m a partire dal crittogramma c applicando una funzione $D : CRT \rightarrow MSG$.

Cifratura e decifrazione

Matematicamente $D(C(m)) = m$ e le funzioni C e D sono una inversa dell'altra. Il termine "spazio" usato per definire MSG e CRT indica un insieme cui appartengono i messaggi o i crittogrammi, senza richiedere che la funzione C o D sia definita sull'intero insieme. Infatti i messaggi effettivamente scambiabili costituiscono in genere un sottoinsieme di MSG e i relativi crittogrammi costituiscono in genere un sottoinsieme di CRT

Il crittoanalista

Il crittoanalista X può essere animato da diversi propositi: scoprire il contenuto della comunicazione, disturbare la comunicazione modificando c, modificare il contenuto del messaggio agendo su c in modo che $Dest$ riceva un'informazione diversa da m. In genere si distingue tra comportamento passivo, se X si limita ad ascoltare la comunicazione, o attivo se X agisce sul canale disturbando la comunicazione o modificando i messaggi, intrusione in genere più pericolosa e difficile da contrastare.

Tipologie di attacchi

L'attacco a un sistema crittografico ha l'obiettivo di forzare il sistema, ma il metodo scelto e il suo livello di pericolosità dipendono dalle informazioni in possesso del crittoanalista.

Cipher Text Attack

Il crittoanalista ha rilevato sul canale una serie di crittogrammi $c_1, \ldots, c_r$.

Known Plain-Text Attack

Il crittoanalista è venuto a conoscenza di una serie di coppie $(m_1, c_1), \ldots, (m_r, c_r)$ contenenti messaggi in chiaro e loro corrispondenti crittogrammi.

Chosen Plain-Text Attack

il crittoanalista si è procurato una serie di coppie $(m_1, c_1), \ldots, (m_r, c_r)$ relative a messaggi in chiaro che lui ha opportunamente scelto.

Man in-the-middle Attack

Il crittoanalista riesce a installarsi sul il canale di comunicazione interrompendo le comunicazioni dirette tra due utenti e sostituendole con messaggi propri, convincendo ciascun utente che tali messaggi provengano legittimamente dall'altro.

Tipologie di cifrari

- Cifrari per uso ristretto (comunicazioni diplomatiche o militari) in cui le funzioni di cifratura C e di decifrazione D sono tenute segrete in ogni loro aspetto.
- Cifrari per uso generale, C e D sono pubblicamente note. Uso di una chiave segreta k diversa per ogni coppia di utenti. La chiave è inserita come parametro nelle funzioni C e D. La conoscenza esplicita di C, D e di un crittogramma c carpito sul canale insicuro, non consente a un intruso che non conosca la chiave k di estrarre utili informazioni sul messaggio originale m.

Cifrari a chiave segreta o simmetrici

- $C(m, k)$ per la cifratura
- $D(c, k)$ per la decifrazione.
- Occorre un canale sicuro per scambiarsi la chiave.

Cifrari a chiave segreta o simmetrici

- Tenere segreta la chiave è più agevole che tenere segreto l'intero processo di cifratura e decifrazione
- Tutti possono impiegare le funzioni C e D a patto che scelgano chiavi diverse
- Se un crittoanalista entra in possesso di una chiave occorre soltanto generarne una nuova, il che consente di realizzare e mantenere efficientemente in software o in hardware le funzioni C e D che rimangono pertanto inalterate.

Spazio delle chiavi e attacchi esaustivi

Lo spazio KEY entro cui la chiave viene scelta deve essere molto ampio. Infatti tale spazio è, o potrebbe essere, noto al crittoanalista che per ricostruire il messaggio dovrebbe solo verificare la significatività delle sequenze di caratteri prodotte con il calcolo di $D(c, k)$, per ogni possibile chiave k. Questo attacco è detto attacco esaustivo.

La chiave pubblica

L'anno 1976 ha segnato una svolta nella storia della crittografia. Diffie e Hellman, e indipendentemente Merkle, introdussero la crittografia a chiave pubblica, con l'obiettivo di eliminare l'obbligo di condivisione della chiave tra mittente e destinatario

La chiave pubblica

Nella crittografia a chiave segreta due utenti sono in grado di cifrare qualsiasi messaggio con la chiave condivisa k, e decifrarlo con la stessa chiave. Nella crittografia a chiave pubblica le operazioni di cifratura e decifrazione utilizzano due chiavi diverse $k[pub]$ per cifrare, e $k[prv]$ per decifrare: la prima chiave è pubblica, cioè nota a tutti, la seconda è privata, cioè nota soltanto al destinatario del messaggio.

La chiave pubblica

C e D sono di pubblico dominio, identiche per tutti gli utenti, e si calcolano inserendovi una chiave come parametro. Quindi la cifratura è accessibile a tutti, perché a tutti è nota la relativa chiave, mentre la decifrazione è accessibile solo a chi possiede la chiave privata. Per tale motivo i sistemi a chiave pubblica sono detti asimmetrici, mentre quelli a chiave segreta sono detti simmetrici per la pari funzionalità attribuita a mittente e destinatario.

Funzioni one-way con trap-door

In un sistema a chiave pubblica la funzione C deve possedere una proprietà forte detta one-way con trap-door. Calcolare C per la cifratura deve essere facile, ma il calcolo inverso D per la decifrazione deve risultare difficile (funzione one-way) a meno che non si conosca un meccanismo segreto (trap-door) che ne semplifichi il calcolo.

Funzioni one-way con trap-door: esempio

Dati due numeri p e q primi, calcolare il loro prodotto n è facile.
Dato n, calcolare i suoi fattori p e q è difficile, ma diventa facile se conosciamo uno dei due.

Facile e Difficile

Cosa è facile e cosa è difficile ?

Applicazioni

La segretezza delle comunicazioni (confidenzialità) è certamente fondamentale ma non è l'unica caratteristica richiesta ai sistemi crittografici attuali. Vi sono tre requisiti importantissimi nelle applicazioni su rete che è bene mettere in evidenza.

Identificazione

Identificazione dell'utente: attraverso la quale un sistema è messo in grado di accertare l'identità di chi richiede di accedere ai suoi servizi.

Autenticazione

Autenticazione di un messaggio: attraverso la quale un destinatario *Dest* accerta che il messaggio stesso sia stato effettivamente spedito da *Mitt*. In questa fase *Dest* deve anche poter stabilire che il messaggio non sia stato modificato o sostituito nella trasmissione.

Firma digitale

Firma digitale: apposta la quale *Mitt* non può ricusare la paternità di un messaggio spedito a *Dest*, e questi può dimostrare a terzi che proprio ciò è avvenuto.