Crittografia delle reti
Introduzione alla crittografia simmetrica
di Tanino Rulez

== Concetti essenziali ==

La crittografia è sicuramente la tecnica più importante per la sicurezza delle reti e della comunicazione. Vengono utilizzate due forme di crittografia: qualla simmetrica detta anche convenzionale(ma anche a chiave unica o chiave segreta) oppure quella a chiave pubblica detta anche asimmetrica.

La caratteristica della crittografia/decrittografia simmetrica è l'utilizzo della stessa **chiave** sia per il mittente che per il destinatario. La chiave è quindi la stessa e comune.
Il testo in chiaro viene cifrato attraverso un algoritmo di crittografia usando proprio la **chiave segreta**. Il testo in chiaro viene poi riottenuto utilizzando un algoritmo di decrittografia e la stessa **chiave segreta**.

I tipi di attacco alla crittografia simmetrica sono l'attacco a **forza bruta** e l'**analisi crittografica**.
Le cifrature simmetriche convenzionali utilizzano tecniche a **sostituzione** e/o **trasposizione**. La sostituzione mappa elementi di testo in chiaro (caratteri,bit) con elementi del testo cifrato. La trasposizione invece appunto traspare le posizioni deglie elementi del testo in chiaro.
Esiste anche la **steganografia** che è una tecnica per nascondere un messaggio segreto all'interno di un altro messaggio in modo tale che gli altri non possano identificare la presenza o i contenuti del messaggio nascosto.

La crittografia simmetrica è tutt'ora la più utilizzata (basti pensare al DES) ed è stata anche la prima ad essere utilizzata prima della nascita della crittografia a chiave pubblica avvenuta intorno agli anni 70.

== La Cifratura Simmetrica ==

Chiariamo ora alcuni termini della cifratura simmetrica:

- **Testo in chiaro**: il messaggio originale o i dati che saranno l'input dell'algoritmo di crittografia
- **Algoritmo di crittografia**: algoritmo che esegue trasformazioni e sostituzioni sul testo in chiaro
- **Chiave segreta**: anche la chiave fa parte dell'input dell'algoritmo. Non è dipendente dal testo in chiaro e naturalmente chiavi differenti faranno produrre all'algoritmo output differenti.
- **Testo cifrato**: è l'output dell'algoritmo,quindi il nostro messaggio cifrato. Esso dipende dal testo in chiaro e dalla chiave segreta. Apparentemente quindi un testo cifrato è un flusso casuale di dati e non comprensibile.
- **Algoritmo di decrittografia**: l'algoritmo di crittografia

eseguito al contrario per ottenere il testo in chiaro dando come input la chiave e il testo cifrato

Facciamo ora due considerazioni

1. Occorre un algoritmo forte. Naturalmente l'algoritmo deve essere così forte che se anche si conosce l'algoritmo e parti di testo cifrato l'attaccante non deve essere in grado di risalire al testo in chiaro e alla chiave.
2. Come avete già capito,mittente e destinatario devono condividere la stessa chiave in modo sicuro e mantenerla al sicuro. Scoperta la chiave e conoscendo l'algoritmo... beh,avete già capito.

In altre parole,non è necessario mantenere segreto l'algoritmo ma è sufficiente tenere nascosta la chiave segreta. Proprio il fatto di non dover mantenere l'algoritmo segreto permette a produttori hardware di sviluppare delle implementazioni hardware(chip) a basso costo degli algoritmi crittografici.

Facciamo ora un esempio:

Una sorgente produce un messaggio in chiaro **X=[X1,X2,....Xm]** dove gli **m** elementi di **X** sono le lettere di un alfabeto finito. Nel caso dell'alfabeto tradizionale,ci sono 26 elementi mentre in alfabeto binario abbiamo solamente 0,1.
Viene generata poi una chiave **K=[K1,K2,...Kj]**. Naturalmente la chiave se viene generata dal mittente deve essere scambiata o fatta conoscere anche al destinatario possibilmente tramite un canale sicuro.
Come input ora abbiamo **X** e **K** e possiamo creare il nostro messaggio cifrato con un algoritmo generale del tipo:

Y=C(K,X)

Quindi,passando all'algoritmo **C** la chiave K e il testo in chiaro X otteniamo il testo cifrato **Y**.

L'algoritmo di decrittografia sarà una cosa analoga:

X=D(K,Y)

Naturalmente per avere il testo in chiaro X dobbiamo dare all'algoritmo di decrittografia **D** come input la chiave K e il testo cifrato Y.

Cosa succede se un estraneo sta " osservando " la comunicazione?
Vedrà naturalmente Y ma non ha accesso a K o a X e potrebbe tentare di ottenere X,K o entrambi.
Naturalmente si suppone il caso dove lo spione conosca gli algoritmi C e D. Esso agirà in base alle sue necessità: se vorrà sapere solo questo testo in chiaro X allora cercherà di conoscere

solo X; se invece è interessato anche a futuri scambi e messaggi cercherà di trovare la chiave K.

== Elementi della crittografia ==

I sistemi di crittografia possiamo caratterizzarli in 3 dimensioni:

- **Operazioni testo in chiaro -> testo cifrato**: gli algoritmi di crittografia si basano su due principi generali: sostituzione e trasposizione
- **Numero di chiavi utilizzate**: Se mittente e destinatario condividono la stessa chiave,allora è un sistema crittografico simmetrico altrimenti il sistema è chiamato asimmetrico
- **Modo di eleborazione del testo**: Possiamo avere una *cifratura a blocchi* dove l'input è elaborato un blocco alla volta oppure una *cifratura a flussi* dove un input è elaborato un bit alla volta in modo continuo producendo l'output man mano che si presenta l'input. Vi parlerò più in la nello specifico di queste due modalità di elaborazione

== Analisi crittografica ==

Solitamente l'obiettivo principale di un attacco ad un testo cifrato è ottenere la chiave segreta più che il testo in chiaro in se per se.

Per attaccare un cifrato vi sono due approcci:

- **Analisi crittografica**: è un attacco che si basa sulla natura dell'algoritmo e sfrutta alcune conoscenze generale del testo in chiaro (ad esempio sappiamo che il testo in input è un testo inglese,italiano,ecc).
- **Attacco a forza bruta**: si tenta ogni possibile chiave un frammento di testo in chiaro finchè non si ottiene la traduzione corretta. In media,per avere successo bisogna provare almeno la metà delle chiavi possibili.

Come potete ben capire,se si è completamente all'oscuro di qualche informazione sul testo in chiaro o addirittura sull'algoritmo di cifratura l'unica soluzione è la forza bruta ma questa non è applicabile se le chiavi sono molto grandi. Si fa quindi riferimento a dati statistici cercando di capire qualcosa sul testo in chiaro: per esempio se si tratta di un codice in C,Java o di un semplice testo in inglese,italiano ecc.

Esistono infatti vari tipi di attacco: solo testo cifrato,testo in chiaro noto,testo in chiaro scelto,testo cifrato scelto.

== Tipi di attacco ==

Esistono vari tipi di attacco a seconda delle conoscenze a disposizione:

- **Solo testo in chiaro (Known Ciphertext Attack)**: l'estraneo ha pochissime informazioni ed è facile difendersi.Solitamente è un caso raro perchè un estraneo ha almeno qualche informazione (tranne che non sia un noob o lamer :))
- **Testo in chiaro noto (Known Plaintext Attack)**: spesso viene anche detto attacco a parole probabili. In questo caso l'estraneo conosce alcune specifiche del testo in chiaro. Esempio: l'estraneo sa che il testo in chiaro è un bilancio aziendale e quindi potrebbe sapere la posizione di determinate parole chiave e cominciare quindi a capirci qualcosa. Esempio più informatico,un codice sviluppato da una certa azienza e l'attaccante potrebbe essere a conoscenza di una determinata parte di codice dove solitamente viene riservato spazio per il copyright.
- **Testo in chiaro scelto(Chosen Plaintext Attack)**: l'estraneo potrebbe ottenere la cifratura di un suo testo in chiaro scelto. Facciamo finta che siamo sun 1 canale di comunicazione dove Bob e Alice comunicano. L'estraneo potrebbe in qualche modo intromettersi tra di loro e chiedere ad uno dei due di cifrare un testo in chiaro da lui scelto. Un esempio quindi può essere l'analisi differenziale (anche di questa ve ne parlerò più in la). In questo caso quindi,chi svolge l'analisi sarà in grado di scegliere i messaggi da far crittografare e potrà scegliere alcune

sequenze che gli consentiranno si individuare la struttura della chiave.
- **Testo cifrato scelto(Chosen Ciphertext Attack)**: è una tecnica solitamente poco utilizzata ma sempre possibile. Simile al precedente ma in questo caso si chiede di decifrare del testo a scelta.

Solitamente solo algoritmi basilari soccombono ad un attacco Known Ciphertext Attack mentre un algoritmo efficiente deve essere progettato in modo da reggere anche un attacco del tipo Known Plaintext Attack.

== Riferimenti e contatti ==

Autore: Tanino Rulez
E-mail: tanino_rul3z[at]hotmail[dot]com
Website: www.taninorulez.wordpress.com