Azzolini Riccardo 2021-02-25

Tecniche di crittografia

1 Crittografia e crittoanalisi

La **crittografia** è l'insieme di tecniche che permettono di scrivere messaggi in un codice che può essere compreso solo da chi conosce la *chiave*.

La **crittoanalisi** è lo studio dei metodi per decifrare i messaggi cifrati *senza* conoscere la chiave. Essa è una disciplina fondamentale per valutare la robustezza degli algoritmi crittografici esistenti e per determinare come progettare nuovi algoritmi robusti.

2 Scenario di base

Lo scenario tipicamente utilizzato per illustrare le tecniche di crittografia è quello in cui due entità peer, chiamate Alice e Bob (A e B), vogliono inviarsi un messaggio in segreto su un *canale non protetto*. In generale, un canale è un qualsiasi segnale che permette di trasmettere messaggi/dati da una parte all'altra, e il fatto che in questo caso esso sia non protetto significa che un attaccante può avere il controllo totale su di esso, ovvero può intercettare, modificare e cancellare i messaggi che vi transitano.

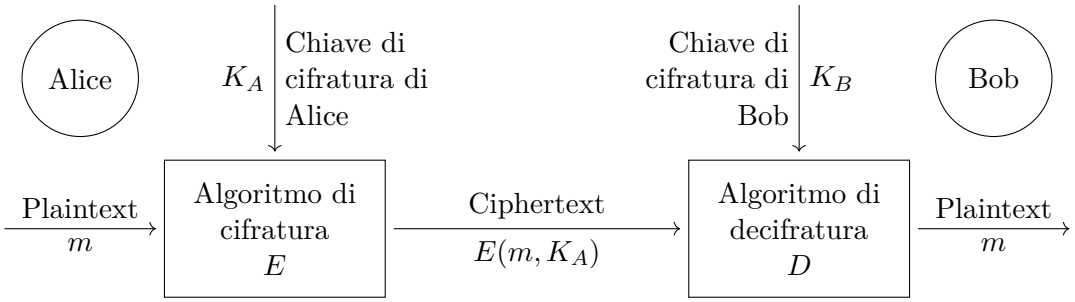
Il messaggio originale che Alice vuole inviare a Bob è chiamato **testo in chiaro** (**plaintext**). Per evitare che un attaccante possa leggerlo, Alice cifra il messaggio usando un apposito **algoritmo di cifratura** (**cipher**), che produce come output un messaggio codificato, detto **testo cifrato** (**ciphertext**). Il testo cifrato prodotto dipende non solo dal testo in chiaro, ma anche da un secondo input dell'algoritmo, una **chiave** di cifratura (che in genere è una sequenza di bit, ed è indipendente dal messaggio da cifrare).

Una volta ottenuto il testo cifrato, Alice lo invia a Bob tramite il canale. Infine, Bob dà il testo cifrato e una chiave di decifratura in input a un **algoritmo di decifratura**: esso annulla le trasformazioni fatte dall'algoritmo di cifratura, ridando in output il testo in chiaro, ovvero consentendo a Bob di leggere il messaggio. Un eventuale attaccante, invece, non potrebbe decifrare il messaggio perché non sarebbe in possesso della chiave di decifratura.

In notazione formale, si indicano:

- con m il testo in chiaro del messaggio;
- con E e D gli algoritmi di cifratura e decifratura, rispettivamente;

- con K_A la chiave di cifratura di Alice, e con K_B la chiave di decifratura di Bob, che può essere uguale o diversa rispetto a K_A;
- con $E(m, K_A)$ o $E_{K_A}(m)$ il testo cifrato con la chiave K_A;
- con $m = D(E(m, K_A), K_B)$ o $D_{K_B}(E_{K_A}(m))$ il testo in chiaro ottenuto decifrando con la chiave K_B il testo cifrato $E(m, K_A)$.



3 Sistemi crittografici

Un **sistema crittografico** comprende un algoritmo di cifratura, un algoritmo di decifratura, un metodo per la generazione delle chiavi, ecc.

I sistemi crittografici sono caratterizzati da vari aspetti. Un aspetto molto importante è il numero di chiavi utilizzate:

- se un sistema utilizza un'unica chiave, si parla di **cifratura simmetrica**;
- se invece un sistema utilizza due chiavi, si parla di **cifratura asimmetrica**.

4 Cifratura simmetrica

La cifratura simmetrica si basa su una *singola chiave segreta*, *condivisa da mittente e destinatario*, che viene usata sia per cifrare che per decifrare i messaggi. Questo tipo di cifratura, che fino alla fine degli anni '70 era l'unico conosciuto, può essere implementato con algoritmi molto efficienti, ma per poterlo impiegare è necessario un modo sicuro di condividere la chiave segreta, il che storicamente era molto difficile.

4.1 Esempio

Un semplice algoritmo di cifratura simmetrica è costituito dall'operatore XOR (OR esclusivo, indicato con il simbolo $\oplus$), la cui tabella di verità è:

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Esso ha infatti una proprietà molto utile: se $A \oplus B = C$, allora $C \oplus B = A$. Di conseguenza, se si vedono il plaintext m e la chiave K come sequenze di bit, il ciphertext può essere ottenuto facendo lo XOR di ciascun bit del plaintext con il corrispondente bit della chiave, dopodiché il plaintext può essere riottenuto facendo una seconda volta lo XOR con la chiave. Ad esempio:

$$\begin{array}{rr} m = & 0\ 1\ 0\ 1\ 1 \\ & \oplus\ \oplus\ \oplus\ \oplus\ \oplus \\ K = & 1\ 0\ 0\ 1\ 1 \\ \hline E(m,K) = & 1\ 1\ 0\ 0\ 0 \end{array} \qquad \begin{array}{rr} E(m,K) = & 1\ 1\ 0\ 0\ 0 \\ & \oplus\ \oplus\ \oplus\ \oplus\ \oplus \\ K = & 1\ 0\ 0\ 1\ 1 \\ \hline D(E(m,K),K) = m = & 0\ 1\ 0\ 1\ 1 \end{array}$$

Il problema di quest'algoritmo è che la chiave deve essere *lunga quanto il messaggio*, quindi scambiare in modo segreto la chiave diventa tanto più difficile quanto più il messaggio è grande. Comunque, l'operatore XOR rimane un elemento molto utilizzato negli algoritmi di cifratura simmetrici più complessi e pratici.

5 Cifratura asimmetrica

La cifratura asimmetrica prevede che ciascun utente abbia una *coppia di chiavi diverse*: una **chiave pubblica** e una **chiave privata**. La chiave privata è segreta, conosciuta solo dal singolo utente, mentre la chiave pubblica non è segreta, e viene in distribuita a chiunque voglia comunicare con l'utente. Le due chiavi sono diverse, ma legate matematicamente: un messaggio cifrato con la chiave privata può essere decifrato solo con la corrispondente chiave pubblica, e viceversa. Il legame tra le chiavi non deve però permettere di risalire da quella pubblica a quella privata.

La cifratura asimmetrica può essere impiegata per fornire segretezza senza la difficoltà della condivisione della chiave segreta che si ha con la cifratura simmetrica: se Alice vuole mandare un messaggio a Bob, lo cifra con la chiave pubblica di Bob, così solo Bob ha la corrispondente chiave privata per decifrarlo.

Nella pratica, gli algoritmi di cifratura asimmetrica sono spesso troppo costosi per poterli applicare a interi messaggi, poiché si basano su operazioni matematiche complesse. Allora, in molti casi, si usa la cifratura asimmetrica solo per inviare in modo segreto una chiave di cifratura simmetrica, che viene poi usata per cifrare la comunicazione "vera e propria" con un algoritmo molto più efficiente.

Infine, la cifratura asimmetrica può essere usata per garantire invece l'autenticazione (dei dati d'origine) e la non ripudiabilità. Infatti, se Alice cifra un messaggio con la propria chiave privata, allora Bob, o chiunque altro, può decifrarlo con la chiave pubblica di Alice, quindi non viene fornito alcun tipo di segretezza, ma se il messaggio viene decifrato correttamente si ha la prova del fatto che esso sia stato effettivamente cifrato con la chiave privata di cui solo Alice è in possesso, ovvero che sia stato inviato da Alice.