Crittografia - introduzione

**Crittografia**: dal greco kriptos ("cripto", nascosto) + grafein ("grafein", scrivere) Arte di progettare algoritmi (o cifrari) che, con l'utilizzo di altri parametri (chiave) consente di **Cifrare un messaggio** e **Decifrare un messaggio**

Lo scopo principale della crittografia è quello di rendere illeggibile un testo in chiaro a chi non è stato autorizzato dall'autore, mediante un'operazione nota come cifratura.

* **Testo cifrato:** un testo ottenuto secondo qualche tecnica della crittografia. Detto anche crittogramma
* **Cifrario**: indica tutto il procedimento utilizzato per ottenere il testo cifrato partendo dal testo in chiaro
* **Decifrazione**: operazione (eseguita dal destinatario) che riporta nella sua forma in chiaro il testo cifrato

Quintupla (E, D, M, K, C):

* **M**: testo in chiaro
* **K**: insieme delle chiavi
* **C**: testo cifrato
* **E**: funzioni di crittografia: M x K -> C
* **D**: funzioni di decifratura: C x K -> M

Uno schema di cifratura è detto **incondizionatamente sicuro** se il testo cifrato generato non contiene abbastanza informazioni per determinare il testo in chiaro, indipendentemente da quanto testo cifrato sia disponibile.

Tutti i metodi utilizzano una chiave per eseguire la crittazione e una chiave per eseguire la decrittazione. Per alcuni algoritmi le due chiavi sono uguali, mentre per altri le chiavi sono diverse. In base a questa sostanziale differenza, i cifrari "moderni" vengono suddivisi in:

* **Algoritmi simmetrici**
* **Algoritmi asimmetrici**

Elementi per determinare la sicurezza:

1. **Numero di simboli** utilizzati nella combinazione (es: una serratura a 4 posizioni richiederebbe in media 5000\*2=10000s, circa 3h)
2. **Numero di possibilità** per ogni posizione (es: una serratura alfabetica richiederebbe 26\*26\*26 possibilità, in media 5 ore invece di 17 minuti)
3. **Tempo** richiesto per ogni tentativo (es: se invece di 2s fossero necessari 20s la situazione cambierebbe notevolmente, ma ancora di più se fossero necessari solo 2ms per tentativi)

Steganografia - introduzione

Arte di proteggere i dati **nascondendoli**, a differenza della crittografia che mira a manipolare i dati rendendoli in tal modo incomprensibili.

La steganografia non trasforma il contenuto ma nasconde l'esistenza stessa del messaggio agli occhi di un osservatore qualsiasi.

L'obiettivo della steganografia è quello di **nascondere** un messaggio segreto **dentro** un messaggio contenitore dall'aspetto innocuo e fuorviante.

Stenografia moderna: codifica binaria

Due interlocutori possono utilizzare la steganografia per inviarsi messaggi nascosti all'interno di messaggi contenitori chiamati **file di copertura**. Tipicamente, i file di copertura moderni sono file multimediali (foto, audio, video).

Una delle tecniche impiegate dai programmi di steganografia consiste nel sostituire i "bit meno significativi" delle immagini digitalizzate con i bit che costituiscono il file segreto. I bit meno significativi sono infatti assimilabili ai valori meno significativi di una misura, cioè quelli che possono contenere errori di scarso rilievo.

Ammesso che da un confronto con l'originale si rilevi una differenza, a occhio (od orecchio) nudo è praticamente impossibile determinare se eventuali perdite di qualità siano dovute a:

* Presenza di informazioni nascoste
* L'errore causato dall'impiego di una codifica poco precisa
* Effettiva qualità dell'immagine originale o della registrazione sonora prima di essere digitalizzata