**Crittografia**

**Tre cose fondamentali:**

* **Riservatezza**: i due soggetti coinvolti in una comunicazione, i loro dati che si trasmettono rimangono riservati.
* **Integrità**: garantire che il messaggio non è stat modificato
* **Autenticità**: garantire l’identità delle persone coinvolte nella comunicazione

**Crittografia simmetrica:**

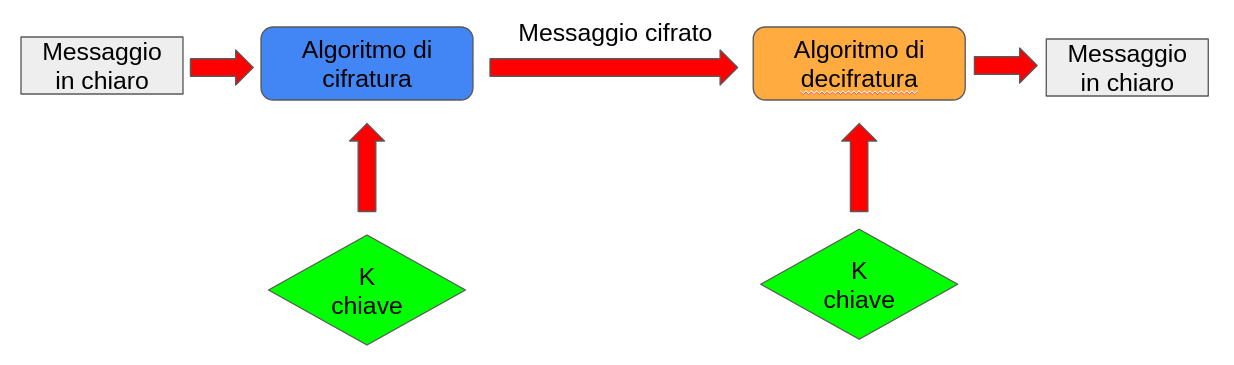
Si basa sul principio che esiste **una sola chiave per cifrare e decifrare**. Questa chiave è a **conoscenza** dei **due utenti**.

**Vantaggi:**

* **Veloce**
* Una chiave per decifrare e cifrare
* Ha una lunghezza opportuna di bit
* È **sicura** **se si rispettano certe condizioni**, come per esempio che la chiave deve essere riservata e la lunghezza in termini di bit

**Svantaggi:**

* **Problema della distribuzione della chiave**. Cioè se i due utenti sono remoti e non riescono a vedersi o ad avere un canale di comunicazione sicuro.
* **Non garantisce l’autenticità degli utenti.**



Gli **algoritmi di cifratura** sono **pubblici** per studiarle, per risolvere problemi e per eventuali migliorie.

**Algoritmo DES (Data Encryption Standard)**

Si **basa** su un **algoritmo a chiave simmetrica**, una chiave di **64 bit** ma che in realtà sarebbero 56 bit perché gli altri sono bit di controllo.

Questo algoritmo nasce con delle componenti che sono segrete e la chiave non era particolarmente lunga. Il **problema** era che dietro a questa segretezza vi fosse la NSA. Il sospetto era che la NSA avesse inserito una **backdoor**, cioè un codice all’interno dell’algoritmo di cifratura che “apre una porta sul retro”, in parole più semplici i dati che arrivano vanno anche da un’altra parte.

È considerato **insicuro**, perché con un’attacco a forza bruta è **possibile forzare una chiave** DES.

**Triplo DES**

**Richiede 3 chiavi di cifratura** che vengono utilizzate per applicare 3 volte il DES ed è diviso in 3 fasi:

1. Applicazione della chiave 1 al testo in chiaro per ottenere il testo cifrato
2. Applicazione della chiave 2 al testo cifrato per decifrarlo, ma avendo usato una chiave diversa da quella corretta si ottone un testo nuovamente cifrato
3. Applicazione della chiave 3 al nuovo testo

Il processo di decifratura è l’opposto.

Attualmente viene usato principalmente un algoritmo che deriva dal DES che si chiama **AES** (Advanced Encryption Standard)

**Crittografia asimmetrica**

I primi algoritmi asimmetrici sono stati sviluppati in segreto negli anni 70 da parte di enti governativi.

**Caratteristiche:**

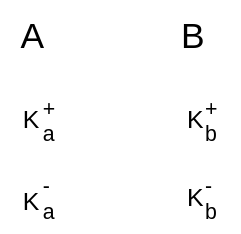
* Esistono due chiavi che sono collegate tra di loro, **chiave pubblica** e **segreta**
* Gli algoritmi sono difficili da risolvere

**Ci sono** **due principi**:

1. È **possibile risalire** alla **chiave pubblica**, ovviamente perché è PUBBLICA ma è **impossibile risalire** a quella **privata**. Gli algoritmi hanno un tempo di **esecuzione esponenziale** (esponenziale rispetto all’input), cioè che per risolverli ci vorrebbero migliaia di anni per risalire alla chiave privata conoscendo quella pubblica. ù
2. Se **cifro** con la **chiave pubblica**, **decifro** con quella **privata** e viceversa.

**Come si garantisce la riservatezza?**

Ogni interlocutore ha la rispettiva chiave pubblica dell’altro.







* Alice manda un messaggio in chiaro, il quale viene cifrato dalla chiave pubblica di Bob (Kb+) e va in rete
* L’intruso non può catturare il messaggio cifrato perché non ha la chiave privata di Bob (Kb-) che è l’unica che può decifrare il messaggio garantendo la riservatezza.

**Come si garantisce l’autenticità?**

Si **applica Ka- nel messaggio per cifrare** e quindi tutti potranno **decifrare** il messaggio perché tutti sono a conoscenza di **Ka+**. Il problema è che anche se questo **garantisce l’autenticità** perché la chiave privata di Alice può essere decifrata con la sua chiave pubblica, questa **non garantisce la riservatezza.**

**Quindi, come si garantiscono l’autenticità e la riservatezza?**



Viene decifrata Kb+ con Kb-, poi si decifra Ka- con Ka+

**Come si garantisce l’integrità?**

Vengono utilizzate le **funzioni di Hash** che **trasformano** i **messaggi** oi **dati** in un **valore di hash di lunghezza fissa**. L'integrità viene verificata confrontando il valore hash del messaggio ricevuto con il valore hash calcolato dal destinatario.

Se i due valori hash corrispondono, ciò indica che il messaggio non è stato alterato durante la trasmissione.

Esempi di funzioni crittografiche: **MD5** (obsoleto) e **SHA**-**256**

**Quindi più o meno è così che è il processo in cui vengono garantite la riservatezza, l’autenticità e l’integrità:**

1. Il mittente calcola la funzione di hash del messaggio da mandare.
2. Cifra la funzione di hash e il messaggio originale con la chiave pubblica del destinatario e lo manda.
3. Il destinatario decifra con la sua chiave privata e si garantisce la riservatezza. Poi decifra con la chiave pubblica del mittente e ha la garanzia dell’identità. Ottiene così il messaggio e la funzione di hash.
4. Calcola la funzione di hash sul messaggio e poi la confronta con la sua funzione di hash.

**Algoritmo Diffie-Hellman:**

Si riesce a concordare una chiave di sessione simmetrica tra due utenti remoti senza aver alcun canale sicuro. Le sessioni ssh sono cifrate sfruttando l’algoritmo e la chiave cambia per ogni nuova sessione.