CRITTOGRAFIA

La crittografia è la scienza che si occupa di rendere incomprensibile un messaggio a chiunque non sia autorizzato a leggerlo. Essa trasforma un messaggio in chiaro in un testo cifrato, in questo modo l'unico modo per leggere il messaggio è avere la chiave di decriptazione. Il primo metodo di crittografia venne inventato da Giulio Cesare, che mandava i messaggi ai suoi generali spostando le lettere di una parola di tre lettere ad esempio la **A** diventava **D**, la **B** diventava **E** e così via. Questo metodo di cifratura si chiama **cifratura di cesare**. Con questo metodo anche se un messaggero veniva catturato i nemici non conoscendo la chiave di cifratura non potevano decifrare il messaggio. Ad oggi si usano due metodi di crittografia ovvero:

- Crittografia simmetrica.
- Crittografia asimmetrica.

Nella **crittografia simmetrica** si usa una singola chiave d'accesso, un esempio potrebbe essere il pin del wi-fi. Il vantaggio principale di questo tipo di crittografia è la sua velocita. Questo metodo è molto usato per criptare file all'interno di un'azienda che non deve condividere troppo la chiave d'accesso ad esempio all'interno di un'azienda il direttore chiede la chiave d'accesso alla segretaria e questo scambio di informazioni avviene e resta all'interno dell'azienda. Mentre se dobbiamo inviare il nostro file criptato ad un'azienda di un'altra città questo metodo non sarà più molto efficiente, perché insieme al file dobbiamo inviare anche la chiave di decriptazione e in caso di attacco man-in-the-middle la nostra chiave verrebbe rivelata e anche il messaggio. In questo caso si usa il secondo metodo ovvero la **cifratura asimmetrica,** Questo metodo di cifratura usa due chiavi d'accesso matematicamente correlate fra loro. Praticamente quando noi vogliamo inviare un messaggio cifrato ad un'azienda gli comunichiamo del messaggio, lei genererà due chiavi d'accesso, una privata e una pubblica. Invierà all'azienda mittente la chiave pubblica e tiene lei la privata. Cosi l'azienda mittente inserisce la chiave pubblica all'interno del file e l'ho invia. In questo modo anche in caso di man-in-the-middle (con man-in-the-middle si intende che tra due utenti che si scambiano informazioni ce n'è un altro nel mezzo che ascolta e le ruba per rivenderle) il file non potrà essere letto ne compromesso perché solo chi possiede la chiave privata può aprire il file. Questo metodo è sicuro per lo scambio di file pero è più lento della cifratura simmetrica, infatti un modo più veloce può essere inviare un file che contiene la chiave d'accesso simmetrica e criptare il file con la crittografia asimmetrica in modo da poter scambiare file in modo più veloce tramite VPN aziendali. Una VPN aziendale è una tecnologia che crea un tunnel sicuro e crittografato attraverso internet, permettendo ai dipendenti di accedere alla rete interna dell'azienda.

La firma digitale viene usata per accertarsi che il file non sia stato modificato e che il mittente sia chi dice di essere. Con questo metodo io invio il file in chiaro e invio un file criptato che contiene il codice hash del file più la mia chiave privata, questo secondo file è detto firma digitale, in questo caso il destinatario apre il secondo file usando la chiave pubblica e controlla il codice hash dei due messaggi per sapere se il messaggio è stato corrotto e vede la mia chiave privata cosi capisce che sono stato io ad inviare il file. Inviare la chiave privata è un'eccezione di questo metodo, dobbiamo ricordarci che normalmente non si invia la chiave privata ma la pubblica.

La certificazione digitale viene rilasciato da un ente C.A che fa richiesta al governo. La C.A garantisce l'identità online di un utente. Questo metodo è un po' più sicuro della firma digitale. In questo caso la mia chiave pubblica diventa la mia certificazione digitale quindi quando invio un file, invierò anche la certificazione (ovvero la chiave pubblica). Quando il destinatario controlla la certificazione e chiede alla C.A se siamo effettivamente noi, l'ente dara la risposta.

ESERCIZIO DI DECRIPTAZIONE.

In questo esercizio andremo a decriptare il messaggio: **HSNFRGH.** Questo messaggio è stato cifrato usando la tecnica del cifrario di cesare quindi dovremmo tornare in dietro di 3 lettere:

H = E

S = P

N = I

F = D

R = O

G = D

H = E

Risposta: EPICODE.