•S3.E3

Esercizio di oggi:

Crittografia.

Dato un messaggio cifrato cercare di trovare il testo in chiaro: Messaggio cifrato: "HSNFRGH"

Svolgimento:

L'esercizio di oggi ci chiede di decriptare il messaggio cifrato "HSNFRGH", per far ecio utilizziamo il cifrario di Cesare, che si basa su uno spostamento fisso delle lettere nell'alfabeto.

Il messaggio in chiaro sarà quindi EPICODE, poichè lo spostamento e di 3 posizioni.

Crittografia

La crittografia ha lo scopo di proteggere le informazioni da accessi non autorizzati. Si suddivide in due categorie principali: simmetrica e asimmetrica.

Nella crittografia simmetrica, la stessa chiave viene utilizzata sia per criptare che per decriptare i dati. Questo tipo di crittografia è spesso impiegato in reti LAN, poiché in un contesto aziendale interno è più semplice condividere la chiave di accesso ai documenti.

I principali vantaggi della crittografia simmetrica sono:

- Velocità: è più rapida rispetto a quella asimmetrica.
- Semplicità: la gestione delle chiavi è meno complessa.

Tuttavia, presenta il limite di dover condividere la stessa chiave, rendendola meno adatta per comunicazioni al di fuori della rete locale.

Mentre la crittografia asimmetrica utilizza una coppia di chiavi:

- Chiave pubblica: usata per criptare i file.
- Chiave privata: usata per decriptarli.

In questo sistema, il destinatario genera entrambe le chiavi e invia la chiave pubblica al mittente. Il mittente utilizza la chiave pubblica per criptare il messaggio, che potrà essere decriptato solo dal destinatario, grazie alla sua chiave privata. Questo garantisce maggiore sicurezza ma comporta una maggiore lentezza rispetto alla crittografia simmetrica.

Dato che la crittografia simmetrica è più veloce ma ha limitazioni nella condivisione sicura della chiave, viene spesso combinata con quella asimmetrica in un sistema ibrido.

In questo approccio, la chiave simmetrica viene inviata in modo sicuro tramite crittografia asimmetrica. Una volta completato lo scambio della chiave, i dati vengono trasmessi usando la crittografia simmetrica per garantire efficienza e velocità. Questo metodo è tipicamente implementato all'interno di reti aziendali tramite VPN (Virtual Private Network).