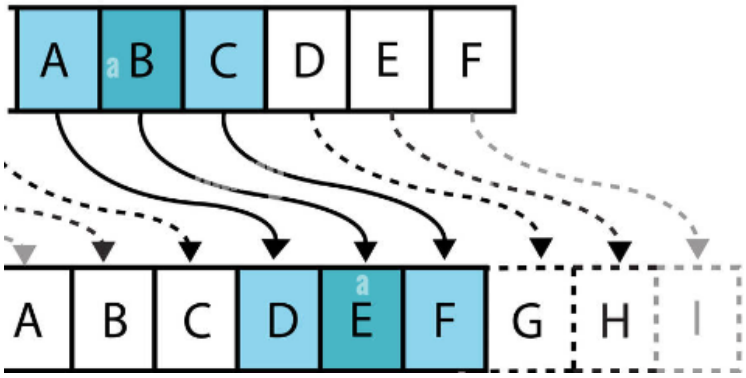
S3-E3

Esercizio di oggi: Crittografia.

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

Messaggio cifrato: "HSNFRGH"

Per risolvere questo esercizio impieghiamo il cifrario di Cesare, tale cifrario prevede una corrispondenza di lettere tra due alfabeti uguali, ma con posizioni sfalsate. Nello specifico c'è un salto di 3 lettere.



Facilmente arriviamo alla soluzione, parole decifrata: Epicode.

In questo esercizio la tematica principale è la crittografia. Fondamentale è la distinzione tra codice Hash e crittografia. La crittografia possiede una chiave di cifratura, la quale permette la reversibilità del processo. Il codice Hash al contrario non permette in alcun modo di ricostruire il file crittografato. La cifratura più famosa è il "Cifrario di Cesare" (ciò ha reso semplice la risoluzione dell'esercizio.)
Distinguiamo 2 tipologie di crittografia:

Crittografia a chiave simmetrica: processo in cui la chiave di cifratura e decifratura è la medesima. E' un processo più "semplice" in termine procedurali, ed è una comunicazione più veloce.

Crittografia a chiave asimmetrica: In cui per la cifratura c'è una prima chiave mentre per la decifratura ce n'è una seconda. Sono due chiavi distinte. Nello specifico definite "Chiave pubblica" e "Chiave privata". Il processo parte dalla creazione da parte del ricevente delle due chiavi. La chiave pubblica verrà inviata al mittente, questa decisione è mirata al prevenire un attacco Man-in-the-middle poiché qualora questa chiave venisse intercettata non rappresenterebbe alcuna minaccia. Una volta ricevuta la chiave dal mittente, quest'ultimo la impiegherà per criptare il file che verrà inviato. criptato, sarà al sicuro, una volta ricevuto dal destinatario verrà impiegata la chiave privata per decriptare il file. Questo processo ruota attorno alla univocità tra le due chiavi generate. La chiave pubblica potrà essere combinata solo con la propria chiave privata al fine di decriptare il file.