

Esercizio S3L3 - Criptazione, cifrario di Cesare ed esercizi in Python

La lezione di oggi si concentrava sui vari tipi di crittografia, simmetrica e asimmetrica, come si relazionano alle proprie chiavi, con un breve excursus riguardante il cifrario di Cesare: quest'ultimo, che prende il nome da Giulio Cesare, utilizzava lo spostamento di tutte le lettere della parola o del messaggio da crittografare secondo un numero precedentemente definito che fungeva da vera e propria chiave di crittografia. L'esercizio di oggi verteva proprio su questo: la parola HSNFRGH infatti utilizza il cifrario di Cesare per rendere incomprensibile a chi non conosce la chiave il vero significato del messaggio da trasmettere. Il numero più comune per l'utilizzo della chiave del cifrario di Cesare è uno spostamento di 3 lettere dell'alfabeto. Se infatti proviamo a spostarci di 3 lettere indietro sull'alfabeto per ciascuna di queste lettere otteniamo il seguente messaggio:

H - 3 posizioni = E
S - 3 posizioni = P
N - 3 posizioni = I
F - 3 posizioni = C
R - 3 posizioni = O
G - 3 posizioni = D
H - 3 posizioni = E

Otteniamo quindi così la parola EPICODE, e il messaggio è stato correttamente decifrato secondo le regole precedentemente descritte.

—

Da aggiornare con esercizio facoltativo.