

Crittografia

Leonardo Bizzoni

November 4, 2023

Un sistema crittografico si può rappresentare come:

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P$$

Dove:

- P è l'insieme dei messaggi in chiaro, siano essi lettere dell'alfabeto, blocchi di lettere, coppie di lettere, ecc, tradotti in forma numerica (*il modo in cui ciò accade può non essere segreto*)
- C è l'insieme dei messaggi crittati
- f è la funzione critta i messaggi
- f^{-1} è la funzione inversa ovvero che decritta i messaggi