

Definitions

Cryptographic algorithm

The method to do encryption and decryption

Cryptographic key

An input variable used by the algorithm for the transformation

N-bit security entropy (a.k.a. the key space)

The number of bits necessary to encode the number of possible keys (could be different than the key length)

Representing data as numbers

Cryptographic algorithms are mathematical operations

- ➡ messages and keys must be represented as numbers
for instance : ASCII encoding