

# Crypto101 Express


## Block ciphers

DaVinciCode

11/6/2020



- OTP pas pratiques
  - taille des données = taille de la clef
  - problème de transmission des clés

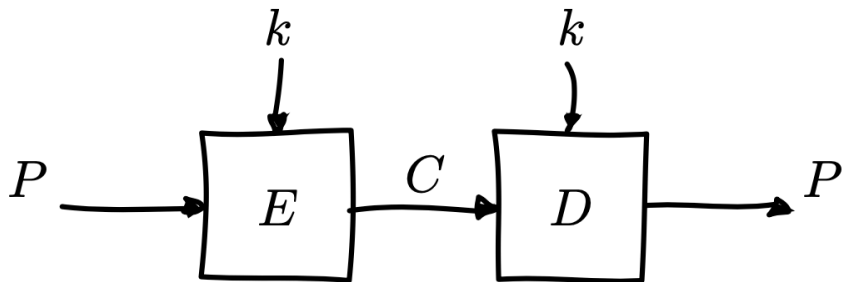
- OTP pas pratiques
  - taille des données = taille de la clef 
  - problème de transmission des clés

## Définition

Algorithmes qui permettent de chiffrer/déchiffrer des blocs de taille fixe (e.g. 16 bytes)

$$C = E(k, P)$$

$$P = D(k, C)$$



## Remarque

Les algorithmes de chiffrement par bloc font partie de la cryptographie symétrique du fait que la même clef est utilisée pour le chiffrement et le déchiffrement.