Crypto101 Express

Stream ciphers

DaVinciCode

15/06/20

Rappel

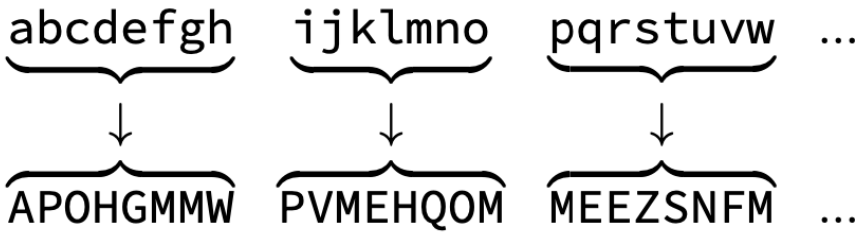
- Chiffrement par bloc
  - comment faire pour chiffrer un message de longueur indéterminée?
  - problème de transmission des clés

Rappel

- Chiffrement par bloc
  - **comment faire pour chiffrer un message de longueur indéterminée?**
  - problème de transmission des clés

Avec le chiffrement par blocs

- diviser le message par blocs et les chiffrer indépendamment

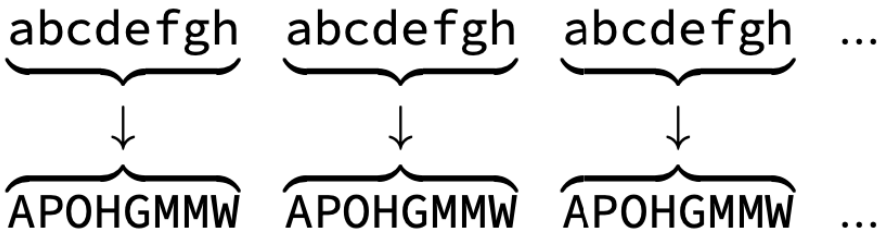


- on appelle ce mode d'opération le mode ECB (Electronic codebook)
-

$$C_i = E_k(P_i)$$

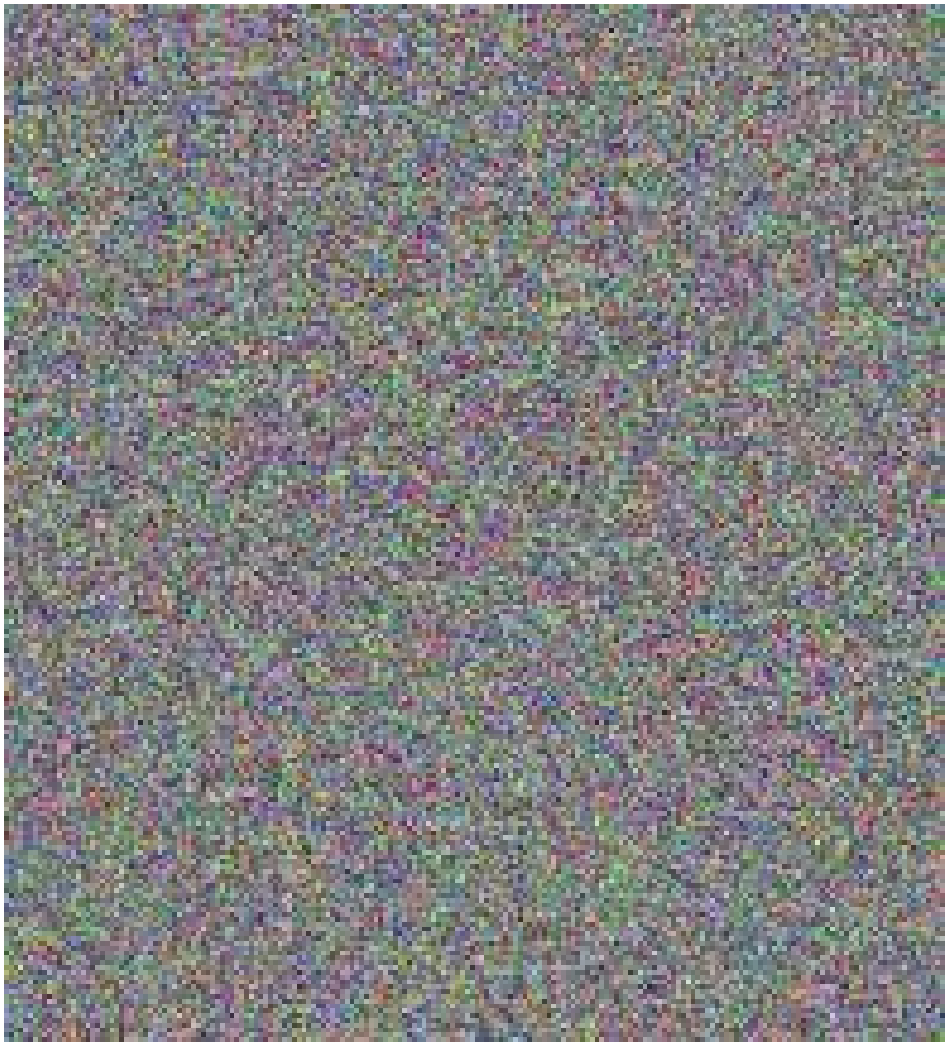
Désavantages du mode ECB

- deux blocs identiques seront chiffrés de la même manière

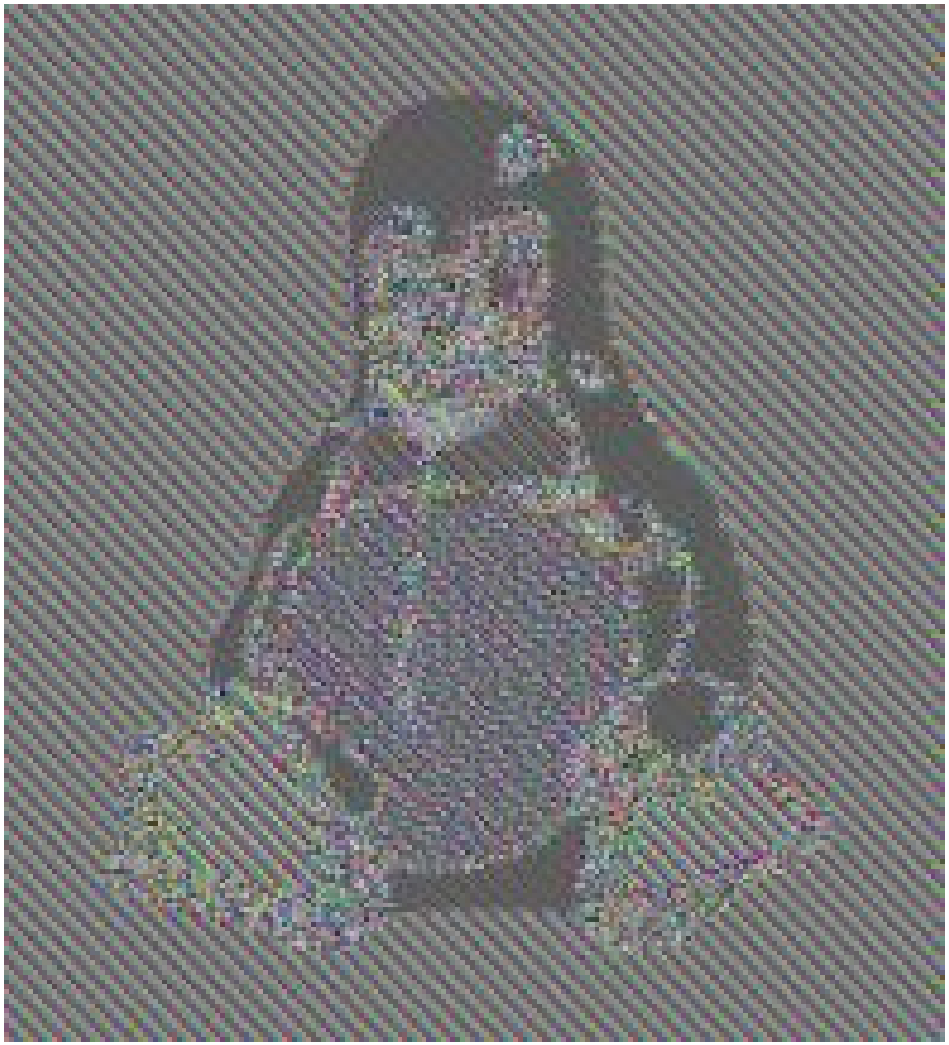


Démo - Message

Démo - Chiffrement idéal



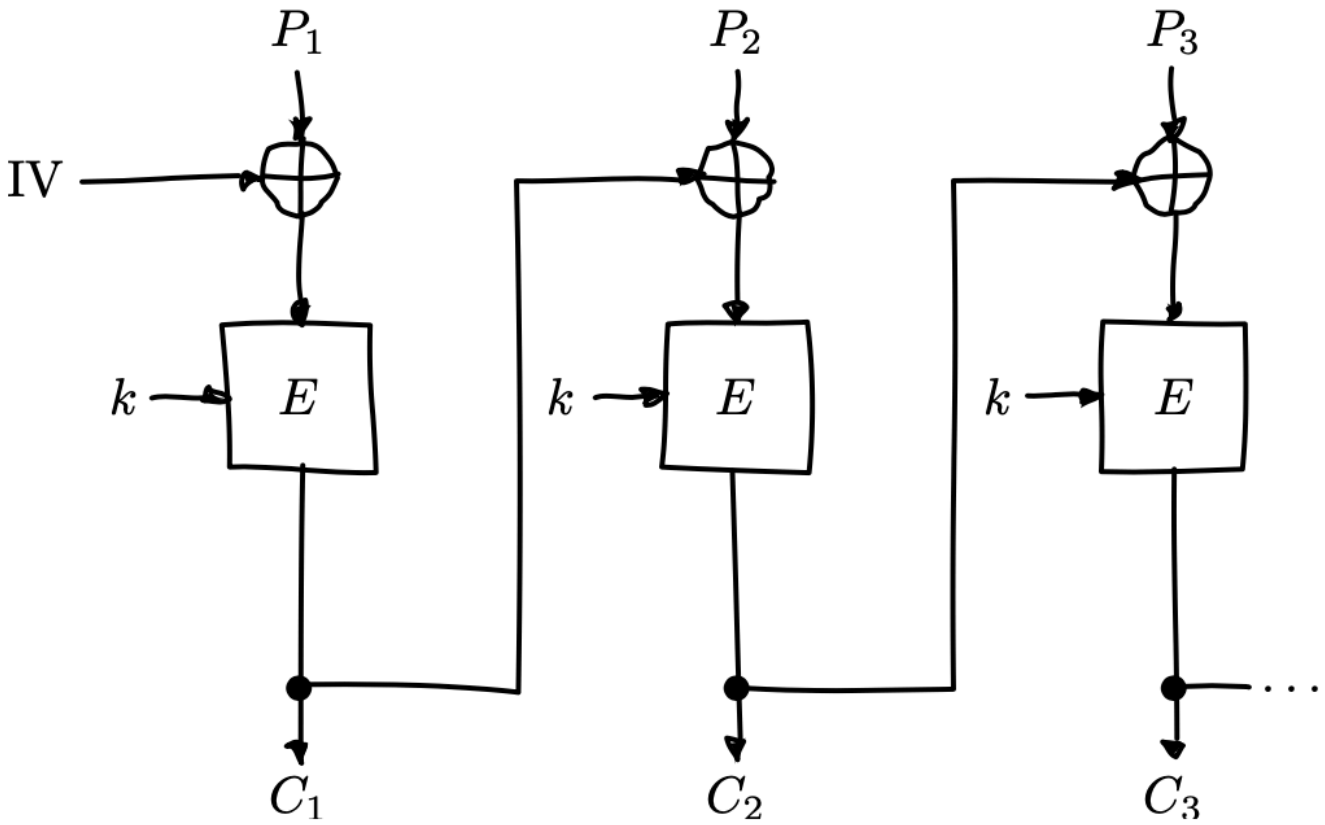
Démo - Chiffrement avec ECB



CBC mode

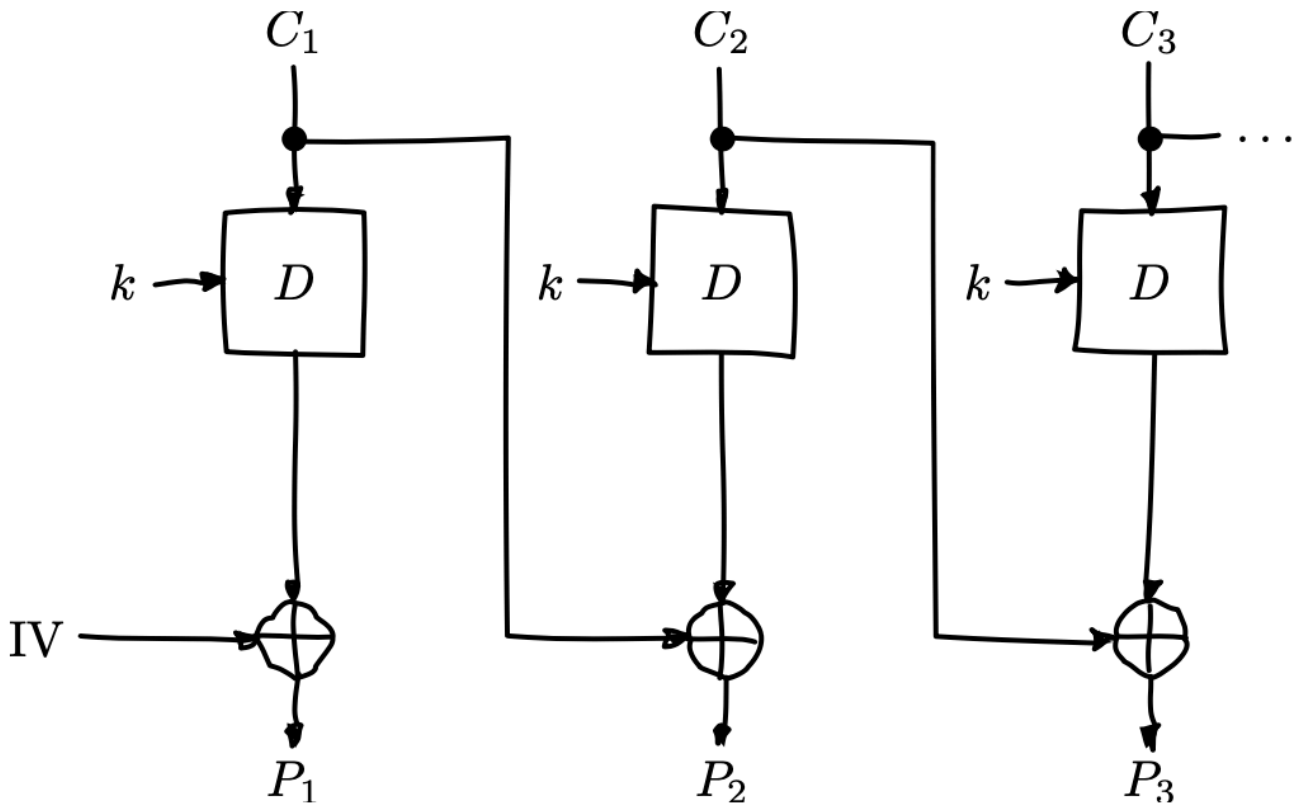
- Cipher block chaining
- $C_i = E_k(P_i \oplus C_{i-1})$
- On XOR chaque bloc P_i par le bloc chiffré C_{i-1} précédent pour brouiller les motifs
  - deux blocs égaux ne seront pas chiffrés de la même manière

Graphique - Chiffrement avec CBC



- $C_0 = IV$ (initialization vector)

Graphique - Déchiffrement avec CBC



- $P_i = D_k(C_i) \oplus C_{i-1}$

Initialization vector

- il est envoyé avec le message chiffré
- il doit être imprévisible, **mais pas secret**
  - il ne doit surtout pas être égal à la clef

Attaques si l'IV est prévisible

- imaginons le site d'une banque qui utilise le mode CBC pour chiffrer les données de ses clients
  - pour simplifier, 1 solde $\Rightarrow$ 1 bloc
  - on peut actualiser notre solde
- base de données:

Client	Solde
Alice	$C_A = E(k, IV_A \oplus P_A)$
Mallory	$C_M = E(k, IV_M \oplus P_M)$
Bob	$C_B = E(k, IV_B \oplus P_B)$

Attaques si l'IV est prévisible

- Mallory est maline
  - elle arrive à prédire les IV qui ont été utilisés pour chiffrer les données pour chaque client (IV_A, IV_M, IV_B)
  - elle a accès à la base de données chiffrées

1. elle actualise son solde $P_M = IV_M \oplus IV_A \oplus G$
2. la banque actualise la base de données: $C_M = E(k, IV_M \oplus P_M)$
   $\iff C_M = E(k, IV_M \oplus (IV_M \oplus IV_A \oplus G))$
   $\iff C_M = E(k, IV_A \oplus G)$
3. si $C_M = C_A$, alors Mallory a trouvé le solde d'Alice (G)

Remarque

Cette banque aurait aussi du avoir une clé k différente pour chaque client