TD2 : chiffrements symétriques

1. **ECB.**

   Le mode de chiffrement ECB (Electronic Code Book ou Dictionnaire de code) est le mode de chiffrement le plus simple que l'on puisse imaginer : chaque bloc de données est chiffré indépendamment par la fonction de chiffrement.

   (a) Ce mode n'est pas sûr, pourquoi ?

   (b) Jack, qui gagne 105000 euros par an, a retrouvé l'entrée chiffrée qui lui correspond dans la base de données des salaires de son entreprise :

   `Q92DFPVXC9IO`

   Sachant que la fonction de chiffrement utilisé a des blocs de deux caractères et que le service informatique de son entreprise ne comprend aucun expert en cryptographie (entendre par là, utilise le mode ECB !), retrouver le salaire de Jane la patronne de Jack parmi le reste de la base de donnée :

   `TOAV6RFPY5VXC9`, `YPFGFPDFDFIO`, `Q9AXFPC9IOIO`, `ACED4TFPVXIOIO`, `UTJSDGFPRTAVIO`

2. **Chiffrement par bloc et fonction de compression**

   Soit $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ un système de chiffrement par blocs qui utilise des clés de n bits pour chiffrer des messages de n bits. Montrer que les trois fonctions de compression f_1, f_2 et f_3 ne sont pas résistantes à la pré-image.

   (a) $f_1 : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n, f_1(h,m) = E_m(h)$

   (b) $f_2 : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n, f_2(h,m) = E_h(m) \oplus h$

   (c) $f_3 : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n, f_3(h,m) = E_h(h) \oplus m$

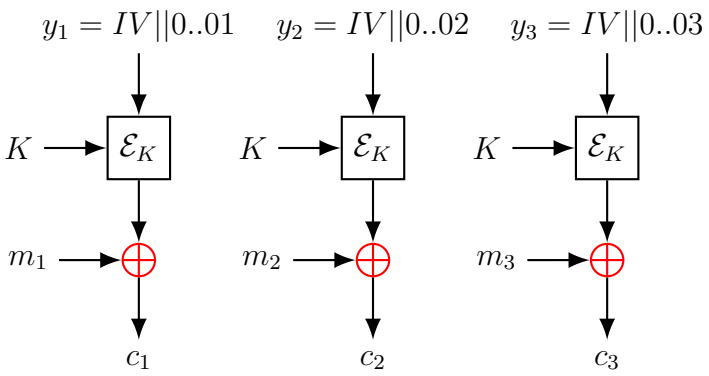
3. **Modes et vecteur d'initialisation**

   Nous considérons dans cet exercice un chiffrement par bloc E paramétré par une clé secrète K. Notons n la taille (en bits) des blocs en question.

   Nous nous intéressons tout d'abord au cas du mode CTR (Counter), dont nous rappelons ici la définition. Étant donné un vecteur d'initialisation IV de $n - 64$ bits, nous notons $y_i = IV||i$, pour tout $0 < i < 2^{64}$, la concaténation de cet IV avec l'entier i, représenté sur 64 bits. Le chiffrement du ième bloc en clair m_i est alors donné par la formule :

   $$c_i = m_i \oplus E_K(y_i), \text{ pour tout } 0 < i < 2^{64}$$

   Comme représenté sur le schéma suivant :



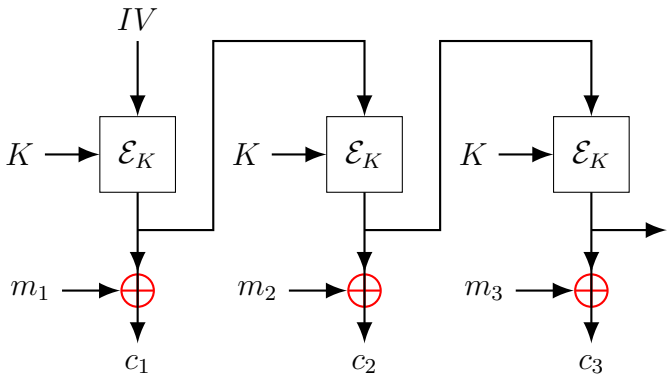
(a) Donnez le schéma de déchiffrement et la formule correspondante pour calculer chaque m_i en fonction de la clé K, du vecteur d'initialisation IV et du bloc c_i.

(b) Supposons alors qu'un utilisateur décide d'utiliser toujours le même vecteur d'initialisation IV pour chiffrer plusieurs messages. Supposons de surcroît que vous, l'attaquant, disposiez d'un couple clair/chiffré (M, C). Quelle est le nom de ce type d'attaque ?

(c) Pouvez-vous utiliser la connaissance de M et C afin de décrypter d'autres messages chiffrés avec la même clé K et le même vecteur d'initialisation IV ? Si oui, comment faites-vous ?

(d) Quel intérêt voyez-vous à ce mode de chiffrement quant à son implémentation ?

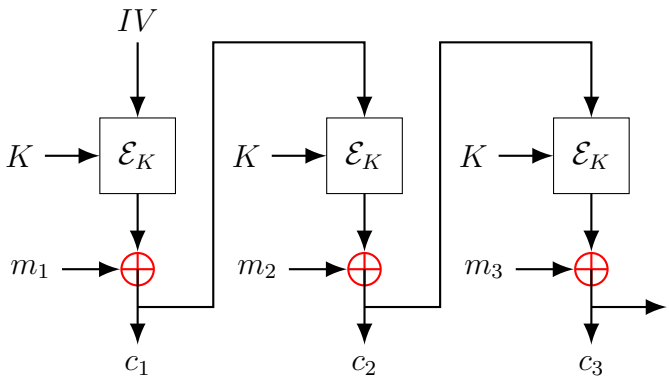
(e) Considérons le mode OFB (Output Feedback) suivant :



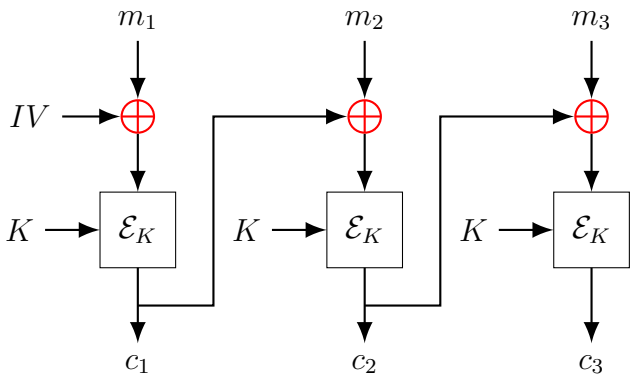
(f) Donnez les formules de chiffrement/déchifrement de ce mode.

(g) Est-ce qu'une attaque à clair connu est possible sur le mode OFB si un même vecteur d'ini- tialisation IV est utilisé pour tous les messages ?

(h) Même question pour le mode CFB suivant :



(i) Même question pour le mode CBC suivant :



(j) À quoi sert le vecteur d'initialisation (IV) ? Doit-il rester secret ?

(k) Que se passe-t-il lors du déchiffrement si l'un des blocs chiffrés a été altéré ?