TD2 - Chiffrement par bloc

(ECB) **Exercise 1.** *ECB and CBC*

On considère un chiffrement par bloc $\mathcal{E}$ opérant sur des blocs de n bits:

$$\begin{array}{rcl} \mathcal{E} : \mathcal{K} \times \mathcal{M} & \longrightarrow & \mathcal{C} \\ (k, m) & \longmapsto & \mathcal{E}_k(m) = \mathcal{E}(k, m) = c \end{array}$$

Le mode ECB (Electronic Code Book) est rappelé en Figure 1. Le message est divisé en blocs de n bits chiffrés séparément. Un autre mode, le mode CBC*, est décrit en Figure 2.

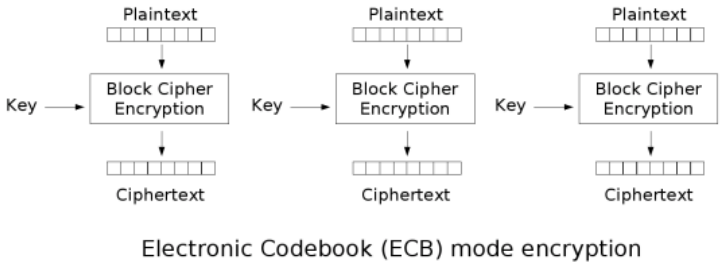

Figure 1: ECB mode

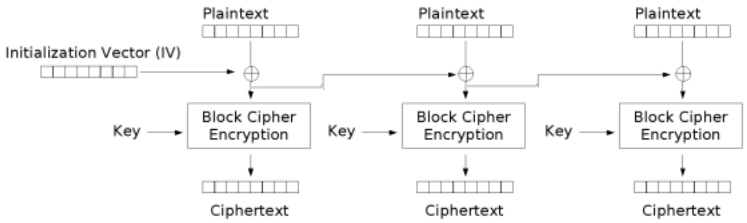

Figure 2: CBC* mode encryption

1. Montrez que le mode ECB n'est pas sémantiquement sûr.

2. Donnez une description algorithmique du mode CBC*.

3. Montrez que le mode CBC* n'est pas sémantiquement sûr, même si $\mathcal{E}$ est une PRF sûre.

(CTRSecurity) **Exercise 2.** *CTR encryption mode*

Soit $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ une PRF. Pour chiffrer un message $M \in \{0,1\}^{d \cdot n}$, CTR procède de la manière suivante :

- Write $M = M_0 \| M_1 \| \dots \| M_{d-1}$ with each $M_i \in \{0,1\}^n$.
- Sample IV uniformly in $\{0,1\}^n$.
- Return $IV \| C_0 \| C_1 \| \dots \| C_{d-1}$ with $C_i = M_i \oplus F(k, IV + i \bmod 2^n)$ for all i.

Le but de cet exercice est de prouver la sécurité du mode de chiffrement CTR contre les attaques à clair choisis, lorsque la PRF F est sûre.

1. Rappelez la définition de la sécurité d'un chiffrement contre les attaques à clairs choisis.

2. Supposons qu'un attaquant fasse q requêtes de chiffrement. Soit $IV_1, \dots, IV_q$ l'IV correspondant. Soit `Twice` l'évènement "il existe $i, j \leqslant q$ et $k_i, k_j < d$ tels que $IV_i + k_i = IV_j + k_j \bmod 2^n$." Montrez que la probability de `twice` est bornée supérieurement par $q^2 d / 2^{n-1}$.

3. Supposons que la PRF F soit remplacée par une fonction uniformément choisie $f : \{0,1\}^n \to \{0,1\}^n$. Bornez l'avantage d'un distingueur $\mathcal{A}$ contre la version idéalisée de CTR, avec une fonction de d et du nombre de requêtes q.

4. Montrez que s'il existe un adversaire PPT $\mathcal{A}$ contre CTR basé sur la PRF F, alors il existe un adversaire PPT $\mathcal{B}$ contre la PRF F. Donnez une borne inférieure sur l'avantage de la réduction.

(TripleDES) **Exercise 3.** *Triple DES*

Un *double schéma de chiffrement* consiste en le chiffrement à deux reprise du clair $m \in \{0,1\}^n$ avec deux clés indépendantes $k_1 \in \{0,1\}^\ell$ and $k_2 \in \{0,1\}^\ell$. On a $c = \mathcal{E}_{k_2}(\mathcal{E}_{k_1}(m))$.

1. On considère l'attaquant suivant $\mathcal{A}$: Supposons qu'il connaisse quelque paires clair/chiffré (m, c), il calcule $\mathcal{E}_k(m)$ et $\mathcal{D}_k(c)$ pour toutes les clés k et mémorise les résultats dans une table. Analyser la complexité de cet algorithme en mémoire et en temps, et expliquer comment l'adversaire peut trouver la paire de clé (k_1, k_2) utilisée pour le double chiffrement (comparer à une recherche exhaustive).

Cette attaque explique pourquoi on utilise le triple-DES, qui consiste en le triple chiffrement avec le chiffrement DES et 3 clés différentes $(k_1, k_2, k_3) \in \{0,1\}^{56} \times \{0,1\}^{56} \times \{0,1\}^{56}$:

$$\text{Triple-DES}_{K_1,K_2,K_3}(X) = \text{DES}_{K_3}(\text{DES}^{-1}_{K_2}(\text{DES}_{K_1}(X))).$$

2. Est-ce que l'attaque précédente peut être adaptée au Triple-DES? Est-ce pratiquement faisable? Expliquez comment on peut retrouver un DES à partir d'une implémentation Triple-DES. Pourquoi est-ce intéressant?