TD 5 : DES et Modes Opératoires

Christina Boura

1 DES

Exercice 1 DES *: Propriété de complémentarité*
Dans cet exercice on va montrer que

$$\overline{\texttt{DES}_K(m)} = \texttt{DES}_{\overline{K}}(\overline{m}).$$

Pour cela nous pouvons utiliser les trois propriétés suivantes pour deux vecteurs $x, y \in \{0,1\}^n$:

— $\overline{x} \oplus \overline{y} = x \oplus y$
— $\overline{x} \oplus y = \overline{x \oplus y}$.
— Si P est une permutation bit-à-bit alors $P(\overline{x}) = \overline{P(x)}$.

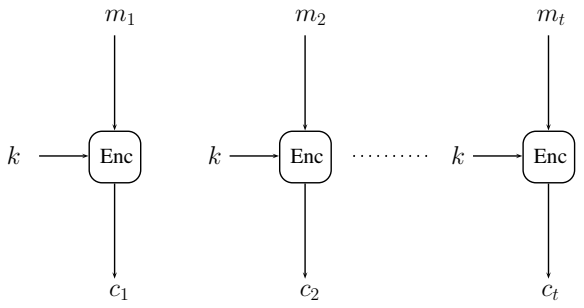
Soit $(K_1, K_2, \ldots, K_{16})$ les 16 sous-clés générées à partir de la clé maître $K \in \{0,1\}^{56}$. On peut montrer que les 16 sous-clés générées à partir de la clé $\overline{K} \in \{0,1\}^{56}$ sont les $(\overline{K_1}, \overline{K_2}, \ldots, \overline{K_{16}})$.

1. Montrer que $F(K_{i+1}, R_i) = F(\overline{K_{i+1}}, \overline{R_i})$.
2. Montrer que lorsqu'on chiffre $(\overline{L_i}, \overline{R_i})$ avec la sous-clé $\overline{K_{i+1}}$ on obtient $(\overline{L_{i+1}}, \overline{R_{i+1}})$.
3. Déduire le résultat.
4. Déduire une attaque par force brute contre DES avec une complexité en temps dans le pire cas 2^{55} chiffrements.
   Astuce : Supposer que l'adversaire qui cherche la clé K possède un bloc de message m et les valeurs $c = \texttt{DES}_K(m)$ et $c' = \texttt{DES}_K(\overline{m})$.

2 Modes opératoires

Les algorithmes de chiffrement par bloc chiffrent des messages en les découpant en blocs de taille fixe. Il existe cependant différentes manières d'utiliser un chiffrement par bloc pour chiffrer des messages de taille quelconque. Ces méthodes sont appelées modes opératoires.

Exercice 2 *Electronic Code Book*
Le mode de chiffrement ECB (Electronic Code Book) est le mode de chiffrement le plus simple : chaque bloc de données est chiffré indépendamment par la fonction de chiffrement, comme le montre la figure suivante :



1. Quels sont les avantages principaux de ce mode ?

2. Expliquer pourquoi ce mode opératoire n'est pas sûr.

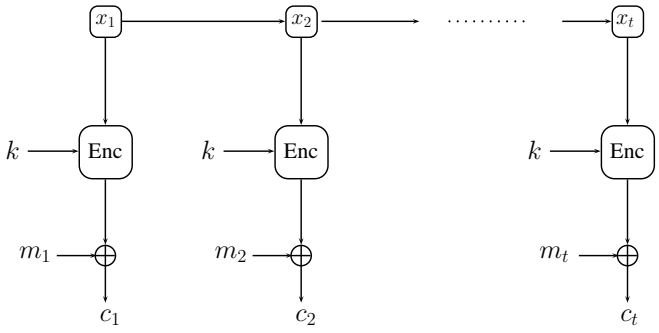
3. Jack, qui gagne 105 000 € par an a retrouvé l'entrée chiffrée qui lui correspond dans la base de données des salaires de son entreprise :

   `Q92DFPVXC9IO`

   Sachant que la fonction de chiffrement utilisée emploie 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 données :

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

Exercice 3 *Counter Mode*
Le mode de chiffrement `CTR` (mode compteur) consiste à chiffrer un compteur qui est incrémenté à chaque bloc, puis à en calculer le ou exclusif avec le message. Le compteur est initialisé à une valeur choisie au hasard appelée la *nonce*.



1. Dessiner le schéma de déchiffrement de ce mode opératoire.

2. Expliquer l'intérêt de la nonce.

3. Quel intérêt voyez-vous à ce mode de chiffrement quant à son implémentation ?

Exercice 4 *Attaque par insertion*
On considère un chiffrement par bloc utilisant le mode opératoire `CTR`. Un attaquant parvient à intercepter un chiffré $c = (c_0, c_1, \dots)$, correspondant à un message $m = (m_0, m_1, \dots)$. L'attaquant connaît uniquement c, mais pas m, ni bien sûr la clé k ou la nonce.

On suppose que l'attaquant parvient à forcer la personne qui chiffre à re-chiffrer un message m' quasiment identique à m, mais avec un bloc de zéros insérés parmi les autres blocs. On suppose en outre que l'attaquant parvient à forcer ce deuxième chiffrement à être réalisé avec la même nonce. L'attaquant obtient donc un nouveau chiffré c'.

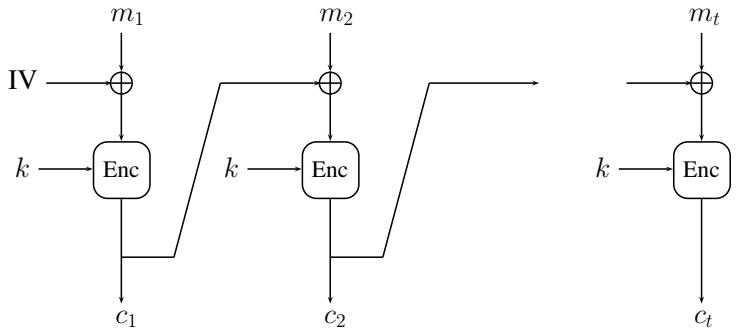
1. Comment l'attaquant peut-il déterminer le bloc à partir duquel m et m' différent ?

2. Supposons que ce premier bloc différent ait pour indice i. Que vaut alors c'_i ? Comment l'attaquant peut-il en déduire m_i ?

3. Montrer comment l'attaquant peut alors déduire les blocs suivants du message $m_{i+1}, m_{i+2}, \dots$.

4. Que doit-on en conclure comme précaution sur l'utilisation de `CTR` ?

Exercice 5 *Cipher Block Chaining*
Le mode de chiffrement CBC (Cipher Block Chaining) suit le schéma suivant



1. Dessiner le schéma de déchiffrement correspondant à ce mode de chiffrement.
2. À quoi sert le vecteur d'initialisation (IV) ? Doit-il rester secret ?
3. On suppose que lors du chiffrement, ou pendant la transmission, un bloc a été altéré. Montrer que dans ce cas, lors du déchiffrement, seulement deux blocs seront déchiffrés incorrectement.
4. (**Fuite d'information)** Qu'est-ce passe-t-il dans le cas où $c_i = c_j$ pour deux blocs chiffrés c_i et c_j distincts ?