TD 2 : Chiffrements symétriques

Exercice 1. * OFB

Voici le mode de chiffrement OFB, avec IV un vecteur initial, M_i les messages en clair et C_i les chiffrés.

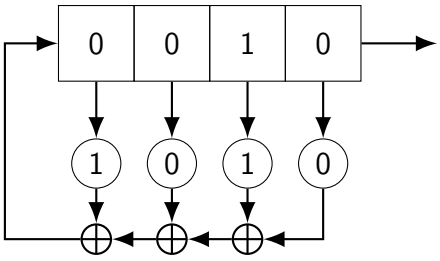
$$C_i = M_i \oplus O_i$$

$$O_i = E_K(O_{i-1})$$

$$O_0 = \text{IV}$$

1. Donner une représentation graphique de ce mode de chiffrement.
2. Donner le mode de déchiffrement correspondant.

Exercice 2 (LSFR*). Soit le LSFR avec la graine $s^{(0)} = 0010$ et les coefficients $c_1 = 1$ $c_2 = 0$, $c_3 = 1$ et $c_4 = 0$



- Calculer les 10 premiers bits de sortie

Exercice 3 (LFSR).

1. * On considère le LFSR de longueur $\ell = 3$ avec $(c_1, c_2, c_3) = (1, 0, 1)$, initialisé à $(z_2, z_1, z_0) = (0, 0, 1)$. Représentez l'état $s^{(i)}$ du LFSR pour $1 \leq s^{(i)} \leq 7$. Donnez la sortie de ce LFSR et sa période.
2. ** Pourquoi les sorties du LFSR sont-elles périodiques ? Quelle est la plus longue période possible pour un LFSR de longueur ℓ ?

Exercice 4. ** Meet in the middle

Les algorithmes de chiffrement symétrique et de déchiffrement symétrique sont publics, et la sécurité repose sur une clé secrète K, qui sert à la fois à chiffrer et à déchiffrer.

Pour chiffrer le message M à l'aide de la clé secréte K, Alice calcule le chiffré $C = ENC(K, M)$. Pour déchiffrer le message chiffré C à l'aide de la clé K, Bob calcule $M = DEC(K, C)$[1]. Un attaquant a découvert M et C, mais le chiffrement ne permet pas d'en déduire K. Or l'attaquant voudrait connaître la clé K pour pouvoir lire les prochains messages chiffrés d'Alice. Il sait seulement que K est un nombre composé de n bits en binaire.

Pour découvrir K, l'attaquant décide d'essayer de chiffrer M avec toutes les valeurs possibles de la clé pour tenter de retrouver C : c'est une attaque par recherche exhaustive. Puisqu'il sait que la longueur de la clé qu'il cherche est de n bits, il devra tester, dans le pire des cas, tous les nombres composés de n bits, et il y en a 2^n.

Pour avoir une meilleure sécurité, Alice a l'idée de chiffrer deux fois son message avec deux clés différentes K_1 et K_2 :

$$C = ENC(K_2, ENC(K_1, M))$$

De cette façon, elle se dit que, en supposant que K_1 et K_2 comportent toutes les deux n bits, l'attaquant devra effectuer dans le pire des cas $2^n \times 2^n = 2^{2n}$ tests pour découvrir les deux clés.

- Saurez-vous vous montrer un attaquant astucieux, et trouver un moyen pour découvrir les deux clés beaucoup plus efficacement ?

Exercice 5. * OTP

Le principe de Kerckhoff dit que la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clé. Ainsi la connaissance du chiffrement et du protocole utilisés ne doivent pas nuire à la sécurité. Voici un exemple de cryptosystème qui ne respecte pas ce principe essentiel de la cryptographie moderne.

Alice et Bob utilisent une méthode de chiffrement extrêmement sûre où ils choisissent simplement ensemble à l'avance un nombre K qui leur servira de clé secrète partagée. Pour chiffrer un nombre M, Alice calcule $M \oplus K$ et communique le résultat obtenu à Bob. Celui-ci déchiffre en calculant $(M \oplus K) \oplus K = M$. Ne connaissant pas K, un intrus n'aurait aucun moyen de découvrir M. Dans la suite de cette énigme, le message M chiffré avec la clé K est noté $\{M\}_K$.

L'opération qui permet de chiffrer et de déchiffrer les messages s'appelle le *ou exclusif* et se note $\oplus$. Le message M et la clé K sont tous deux écrits en binaire et ont le même nombre de bits. Le calcul du message chiffré $M \oplus K$ se fait bit par bit, avec les règles suivantes : $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$, comme dans l'exemple ci-dessous.

$$\begin{array}{cccccccc} & 1 & 0 & 0 & 1 & 1 & & M \\ \oplus & 0 & 0 & 1 & 1 & 0 & & K \\ \hline & 1 & 0 & 1 & 0 & 1 & & M \oplus K \end{array}$$

Pour qu'Alice communique un nombre secret M à Bob, ils choisissent chacun une clé secrète (KA pour Alice et KB pour Bob) et échangent trois messages :

1. Les notations $ENC(K, M)$ et $DEC(K, C)$ pour représenter le résultat de la procédure de chiffrement d'un message M avec une clé K (respectivement de déchiffrement d'un chiffré C avec une clé K) sont classiques en cryptographie. *ENC* est l'abréviation de *to encrypt*, qui signifie *chiffrer* en anglais, et *DEC* est celle de *to decrypt*, qui signifie *dechiffrer*.

- Alice chiffre le message M avec sa clé KA et envoie le résultat à Bob : $\{M\}_{KA}$ qui vaut 0011 1101 ;
- Bob ne peut pas déchiffrer ce message car il ne connaît pas KA, mais il chiffre le message reçu avec sa clé secrète KB et envoie le résultat à Alice $\{\{M\}_{KA}\}_{KB}$ qui vaut 1001 1100 ;
- Alice déchiffre le message reçu avec sa clé KA et envoie le résultat à Bob : $\{M\}_{KB}$ qui vaut 1111 1011.
- Saurez-vous découvrir le nombre secret M en décimal ?

Exercice 6 (Déchiffrement DES **). À partir du chiffré C, avec les clés dans l'ordre inverse : $K'_0 = K_{15}, \ldots, K'_{15} = K_0$ et les règles $R'_{i+1} = L'_i$ et $L'_{i+1} = R'_i \oplus f(L'_i, K'_i)$, montrez que le déchiffrement DES est correct.