C. Olivier-Anclin & Y. Zhao

TD 1 – Services de sécurité et chiffrement symétrique

Exercise 1 (Vrai ou faux ?)
Pour chacune des affirmations suivantes, expliquez pourquoi elle est fausse (ou discutez sa validité).

1. Il est sûr de stocker les mots de passe des utilisateurs en clair si le serveur utilise toujours HTTPS (*i.e.*, un canal chiffré et authentifié).
2. Un chiffrement par blocs avec une clé plus grande est toujours plus sûr.
3. Il n'y aura jamais de raison technologique d'utiliser des clés de chiffrement par blocs plus grandes que 128 bits.
4. Il faut toujours utiliser des clés de chiffrement par blocs plus grandes que 128 bits.
5. Il faut toujours utiliser le chiffrement par blocs publié le plus récent.

Exercise 2 (Services de sécurité)

1. Identifiez les objectifs fondamentaux (services) de la sécurité informatique et expliquez les différences entre eux.
2. Donnez deux classifications standard des attaques. Expliquez chaque classe en donnant des exemples.
3. Quels sont les services de sécurité assurés par un chiffrement symétrique ? Par un chiffrement asymétrique ?
4. Quels services de sécurité assure une fonction de hachage cryptographique ? Lequel n'assure-t-elle *pas* seule ?
5. Quels services de sécurité assure une signature électronique ?
6. Pour chaque propriété suivante, indiquez le mécanisme le plus adapté : (a) vérifier qu'un logiciel téléchargé n'a pas été altéré ; (b) prouver qu'un employé a bien signé un contrat ; (c) empêcher la lecture d'une base de données volée.

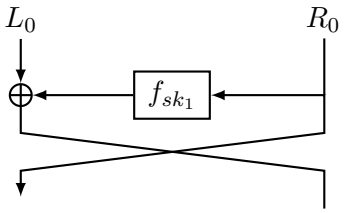
Exercise 3 (Le doublement du chiffrement augmente-t-il la sécurité ?)
On considère un schéma de chiffrement symétrique E et le double chiffrement

$$c = E_{k_2}(E_{k_1}(m)), \qquad k = k_1 \| k_2,$$

où k_1 et k_2 sont deux clés indépendantes.

1. Décrivez l'attaque *meet-in-the-middle* : quel est son coût en temps et en mémoire, comparé à la force brute sur une clé simple puis sur la clé double ?
2. Application : si E = DES (56 bits de clé), quelle sécurité effective le double DES offre-t-il ? Pourquoi a-t-on introduit 3-DES (EDE) plutôt que 2-DES ?
3. 3-DES avec trois clés indépendantes offre-t-il $3 \times 56 = 168$ bits de sécurité effective ? Discutez.
4. Avec AES, quel(s) mode(s) d'utilisation suffit(sent) aujourd'hui ? Que penser d'AES "double" ?

Exercise 4 (Complémentarité de DES)
Soit E l'algorithme de chiffrement de DES, réseau de Feistel de 16 tours. Après la permutation initiale IP et avant la permutation finale IP^{-1}, un tour fonctionne comme décrit ci-dessous.



où $f(R_{i-1}, K_i) = P\big(S(E(R_{i-1}) \oplus K_i)\big)$ avec :

- E étend l'entrée 32 bits R_{i-1} à 48 bits par permutation et duplication de bits ;
- $\oplus$ désigne le XOR avec la clé de tour 48 bits K_i ;
- S applique les huit S-boxes, réduisant 48 bits à 32 bits ;
- P est une permutation fixe sur 32 bits.

On note $\bar{X}$ le complémentaire bit à bit de X. Montrez que :

$$E_K(P) = C \Leftrightarrow E_{\bar{K}}(\bar{P}) = \bar{C}.$$

Question bonus : quelle conséquence pratique cette propriété a-t-elle sur les attaques par force brute sur DES ?

Exercise 5 (Réseaux de Feistel à 1, 2 et 3 tours)
On considère des schémas de Feistel équilibrés opérant sur $\{0,1\}^{2n}$: un bloc est vu comme un couple de demi-blocs de n bits, et r tours utilisant des fonctions de tour $f_1, \ldots, f_r : \{0,1\}^n \to \{0,1\}^n$ calculent, à partir de l'entrée $x = (L_0, R_0)$:

$$(L_i, R_i) = \big(R_{i-1},\ L_{i-1} \oplus f_i(R_{i-1})\big), \qquad i = 1, \ldots, r,$$

le chiffré étant $c = (L_r, R_r)$. On note F_r le schéma à r tours. Un adversaire accède à un oracle réalisant soit F_r (avec des fonctions de tour aléatoires et indépendantes), soit une permutation aléatoire uniforme sur $\{0,1\}^{2n}$, et doit deviner lequel.

1. Montrer qu'un adversaire faisant une seule requête distingue F_1 d'une permutation aléatoire avec probabilité $1 - 2^{-n}$.
2. Montrer qu'avec deux requêtes sur des clairs de même demi-bloc droit (R_0 fixé), les sorties de F_2 vérifient toujours une relation que ne satisfait une permutation aléatoire qu'avec probabilité environ 2^{-2n}. En déduire un adversaire distinguant F_2 avec probabilité proche de 1.

Exercise 6 (Malléabilité du mode CBC)
Les standards de chiffrement symétrique comme AES chiffrent des messages de longueur 128 bits avec une clé symétrique. Afin de chiffrer des messages plus grands, des modes de chiffrement ont vu le jour. La façon naturelle de chiffrer un grand message consiste à le scinder en blocs de 128 bits et à les chiffrer les uns après les autres. Cette technique s'appelle ECB, mais n'assure pas une grande sécurité, car deux blocs identiques sont chiffrés de la même manière.

Afin de palier ce problème, le mode de chiffrement CBC a été proposé par le NIST. Il fonctionne comme suit, où IV est un vecteur initial, K est la clé de chiffrement symétrique, $x \oplus y$ est le XOR entre x et y, et $E_K(m)$ est le chiffré du message m avec la clé K :

$$C_0 = IV \text{ et } C_i = E_K(P_i \oplus C_{i-1}).$$

Un attaquant peut attaquer un schéma de chiffrement dans différents buts. L'objectif le plus évident est de connaître les messages échangés entre deux personnes. Une autre attaque vise la perturbation par l'attaquant d'un message échangé (pour changer, par exemple, le sens d'une phrase). Ce type de perturbation s'appelle *attaque par malléabilité.*

Supposez que vous connaissez la valeur de P_1 pour un chiffré donné $IV \| C_1 \| C_2 \| C_3 \| C_4 \ldots$

Vous contrôlez aussi la valeur initiale IV'. Construisez un second message chiffré avec la même clé : $IV' \| C'_1 \| C'_2 \| C'_3 \| C'_4 \ldots$ tel que $C'_i = C_{i-2}$ pour $i \geq 3$. Votre objectif est de remplacer le texte chiffré original par un autre texte chiffré, pour lequel les valeurs de certains blocs de texte clair (P'_1 et P'_3) sont choisis par l'attaquant.

Saurez-vous trouver les valeurs de IV', C'_1, C'_2 et C'_3 telles que P'_1 et P'_3 sont fixés ?