Cryptographie et Sécurité - TD1

guillaume.postic@universite-paris-saclay.fr

Exercice 1 : *bit-flipping attack*

Alice et Bob utilisent le chiffrement *one-time pad*, et on suppose que vous êtes au courant que le message chiffré de `BUY 10 EUROS` est `372393351B25631A40028419`. Le message original est codé en 8-bit ASCII et le chiffré est écrit en hex.

Quel est le message chiffré du texte `BUY 95 EUROS` en utilisant la même clé ?

Exercice 2 : attaque statistique

On dispose d'un algorithme qui, à partir d'un texte chiffré c, est capable de trouver le i-ème bit du texte en clair m correspondant à c, avec une probabilité égale à $0{,}51$. Cet algorithme a donc 51% de chance de trouver le i-ème bit de m, et il est donc à peine meilleur qu'un algorithme qui déciderait de la valeur du i-ème bit en tirant à pile ou face (et qui aurait donc 1 chance sur 2 d'avoir raison).

On suppose que l'algorithme s'exécute en 1 seconde sur un ordinateur.

Montrer qu'il est possible de trouver le i-ème bit du message m avec une probabilité d'au moins $0{,}99$ (soit 99%) au bout de **25 heures et 36 minutes** de calcul, et qu'il est possible de trouver le i-ème bit du message m avec une probabilité d'au moins $0{,}9999$ (soit $99{,}99\%$) au bout du double de ce temps.

<u>Indication</u> : il sera utile d'utiliser l'inégalité de Chernoff ci-dessous.
Soit $X_1, X_2, \dots, X_n$ des variables aléatoires indépendantes, chacune dans l'intervalle $[0, 1]$. On note $X = X_1 + X_2 + \dots + X_n$ la somme de ces variables aléatoires et $\mathbf{E}[X] = \mathbf{E}[X_1] + \mathbf{E}[X_2] + \dots + \mathbf{E}[X_n]$ l'espérance de X (qui est toujours égale à la somme des espérances de chacune des variables X_i).
Alors pour tout $a > 0$, on a $\Pr[X \leq \mathbf{E}[X] - a] \leq e^{-a^2/2n}$.

Exercice 3 : sécurité parfaite

Soit M l'espace des messages en clair, C l'espace des messages chiffrés, et K l'espace des clés. On rappelle que dans le chiffrement OTP (*One-Time Pad*), on a $M = K = \{0, 1\}^l$, avec l une constante indiquant la longueur des messages et avec $E(k, m) = k \oplus m$, $D(k, c) = k \oplus c$.

On rappelle la définition d'un chiffrement parfaitement sûr :
$\mathbf{Pr}_{k \in K}\,[E(k, m_1) = c] = \mathbf{Pr}_{k \in K}\,[E(k, m_2) = c],\ \forall\ m_1, m_2 \in M,\ \forall\ c \in C.$

On considère maintenant 3 variantes de ce chiffrement.

1. Dans la première variante, on définit $S = \{00, 01, 10\}$, et on a $M = S^l$ et $K = \{0, 1\}^{2l}$, avec l une constante égale à la moitié des longueurs des messages. Par exemple, pour $l = 3$ on ne peut pas avoir $m = 110011 \in M$, car $11 \notin S$. On a toujours $E(k, m) = k \oplus m$ et $D(k, c) = k \oplus c$. Ce chiffrement est-il parfaitement sûr ? Si oui, le prouver, sinon trouver un contre-exemple.

2. Dans la deuxième variante, on a $M = \{0, 1\}^{2l}$ et $K = S^l$, avec l une constante égale à la moitié des longueurs des messages. On a toujours $E(k, m) = k \oplus m$ et $D(k, c) = k \oplus c$. Ce chiffrement est-il parfaitement sûr ? Si oui le prouver, sinon trouver un contre-exemple.

3. Dans la troisième variante, on a cette fois-ci $M = K = S^l$. Ce chiffrement est-il parfaitement sûr ? Si oui le prouver, sinon trouver un contre-exemple.

Exercice 4 : sécurité des PRNG

Soit $G : \{0, 1\}^s \rightarrow \{0, 1\}^n$ un générateur pseudo-aléatoire (PRG) sécurisé. Quels sont les PRG sécurisés parmi les PRGs suivants ? Dans le cas d'un PRG non sécurisé, fournir un test statistique A et calculer son avantage par rapport au générateur.

1. $G'(k) = G(k) \oplus 1^{n/2}\, 0^{n/2}$
2. $G'(k) = G(k) \| G(k) \| G(k)$ ($\|$ est la concaténation)
3. $G'(k) = G(k) \| \mathrm{XOR}(G(k))$