UVSQ - Université Paris-Saclay le 7/5/2026

Licence 3 Informatique 2025–2026
LSIN603 – Cryptographie – CC2– 1h30

Seule une feuille A4 manuscrite est autorisée. Aucun autre document ni support numérique n'est autorisé. Toute erreur dans le sujet sera prise en compte dans la correction. La qualité de la rédaction sera prise en compte dans la notation.

Questions de cours (10 points)

1 *(1 point)* Pourquoi un chiffrement par transposition n'est pas sécurisé ?
2 *(2 points)* Énoncez le théorème de Shannon et expliquez ce qu'il implique en pratique.
3 *(2 points)* Donnez les quatre opérations utilisées dans l'AES ainsi que la taille des clefs et le nombre de tours.
4 *(1 point)* Comment garantir aujourd'hui qu'une famille de permutations est une PRP ?
5 *(2 points)* Expliquez le plus précisément possible le chiffrement ElGamal, incluant la génération de clefs, le chiffrement et le déchiffrement.
6 *(2 points)* Donnez la définition de sécurité la plus formelle possible pour une signature numérique. Expliquez avec vos mots à quoi une signature numérique peut servir.

Exercice 1 - Diffie Hellman et générateur (5 points)

Définition 1 (Ordre d'un élément) *Soit $(G, \times)$ un groupe cyclique. Pour tout $x \in G$, on appelle ordre de x le plus petit entier naturel k strictement positif tel que*

$$x^k = x \times x \times \cdots \times x = e$$

où e est le neutre pour $\times$ dans G.

On considère un groupe cyclique $(G, \times)$ d'ordre n avec n un entier. Soit $x \in G$ un élément d'ordre k. On rappelle la notion d'ordre d'un élément.

1 *(1 point)* Quelles valeurs différentes peuvent prendre le reste de la division euclidienne de a par k pour tout entier naturel a ?
2 *(1 points)* En déduire combien de valeurs différentes peuvent prendre les expressions x^a pour tout entier naturel a.
3 *(2 points)* On suppose maintenant que Alice et Bob utilisent un élément x d'ordre strictement inférieur à 2^{50} dans le protocole d'échange de clefs Diffie-Hellman. Expliquez comment un attaquant peut aujourd'hui retrouver le secret commun partagé x^{ab} où a et b son tirés de manière aléatoire selon la distribution uniforme dans $\{1, \ldots, 2^{512}\}$.
4 *(1 point)* En déduire pourquoi il est préférable d'utiliser un générateur dans le protocole d'échange de clefs de Diffie et Hellman.

Exercice 2 - Les itérés de χ (9 points)

Soit n un entier naturel impair. On considère l'application

$$\begin{array}{rccc} \chi & : & \{0,1\}^n & \to & \{0,1\}^n \\ & & (x_0, x_1, \ldots, x_{n-1}) & \mapsto & (y_0, y_1, \ldots, y_{n-1}) \end{array}$$

définie par les relations suivantes : pour tout $0 \leq i < n$, $y_i = x_i \oplus ((1 \oplus x_{i+1}) \wedge x_{i+2})$. Les indices sont pris modulo n (par exemple si $i = 4$ et $n = 5$, alors $i + 1 = 0$ et $i + 2 = 1$). Le symbole $\oplus$ est le XOR, les x_i sont des bits (0 ou 1) et $\wedge$ est le AND.

1 *(1 point)* Donner toutes les valeurs entrées/sorties pour $n = 3$ de la fonction χ.

On rappelle maintenant le critère d'avalanche vu au TD 5. Pour cela, on donne la définition de fonctions coordonnées d'une fonction de $\{0,1\}^n$ dans $\{0,1\}^n$.

Définition 2 (Fonctions coordonnées) *Soit n un entier. Pour toute fonction $F : \{0,1\}^n \to \{0,1\}^n$, on appelle fonction coordonnée de F toute fonction $f_i : \{0,1\}^n \to \{0,1\}$ pour $0 \leq i \leq n-1$ définie par*

$$x \mapsto f_i(x) = (F(x))_i$$

où $(F(x))_i$ est le i-ème bit dans la représentation binaire de $F(x)$.

2 *(1 point)* Quelles sont les fonctions coordonnées de χ

On suppose maintenant que chaque $f_i(x)$ n'a besoin que de ℓ_i bits de x pour être calculée. On note alors

$$\ell = \max_{0 \leq i \leq n-1} \ell_i = \mathrm{Avalanche}(F)$$

3 *(1 point)* Que vaut $\mathrm{Avalanche}(\chi)$?

4 *(1,5 points)* Soit $x_0, \ldots, x_{n-1} \in \{0,1\}^n$. Exprimez le n-ème bit de $\chi \circ \chi(x)$ avec des XOR, et des AND. Faire un dessin du circuit peut aider.

5 *(1,5 points)* Que vaut $\mathrm{Avalanche}(\chi \circ \chi)$? Que vaut $\mathrm{Avalanche}(\chi \circ \chi \circ \chi)$? **Indication :** on pourra remarquer que chaque bit en sortie se « comporte » de la même manière. De plus, on ne cherchera pas à prouver formellement le résultat, mais il faudra donner des éléments de réfléxion permettant d'arriver à votre résultat.

6 *(1,5 points)* D'après vous, que vaut $\mathrm{Avalanche}(\chi^j)$ pour j un entier arbitraire.

7 *(1,5 points)* À partir de quand pouvons-nous avoir une diffusion complète ?