Licence 3 Informatique 2025–2026
LSIN603 – Cryptographie – CC1– 1h30 – Sujet A

Seule une feuille A4 manuscrite est autorisée. Tout support numérique est interdit. 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 *(1,5 points)* Quelle technique de cryptanalyse permet de « casser » un chiffrement par substitution ? Expliquez son principe.
2 *(1,5 points)* Un cryptosystème est dit inconditionnellement sûr si la connaissance d'un chiffré n'apporte aucune information sur le message clair. Comment ceci se formalise **mathématiquement** ?
3 *(1,5 points)* Énoncer le théorème de Shannon vu en cours.
4 *(1 point)* Donner un contexte pratique (réaliste) où un attaquant est dans un modèle à clair connu. Détaillez.
5 *(1 point)* Comment garantir aujourd'hui qu'une famille de permutations paramétrée par une clef est une PRP ?
6 *(1 point)* On suppose qu'un utilisateur sur internet ne change jamais le nonce et utilise le mode compteur. Quelle propriété n'est plus atteinte par le chiffrement ? Donner un contexte critique en pratique dans ce contexte (soyez précis).
7 *(1 point)* Qu'est-ce que la diffusion au sens de Shannon ?
8 *(1,5 points)* Expliquez avec vos mots le principe de l'attaque « Meet-in-the-Middle ». Dans quel modèle d'attaque fonctionne-t'elle ?

Exercice 1 - Cryptanalyse du chiffre de Vigenère (6 points)

Alice a chiffré un message écrit en français à l'aide du cryptosystème de Vigenère et Eve a récupéré ce message chiffré sur un bout de papier.

`MKNUUJFVBYTKTKDXFZFYULWAKCHN`

1 *(1,5 points)* Expliquez pourquoi il y a de grandes chances que la longueur de la clef soit de 2.
2 *(2,5 points)* Déchiffrez le message. Quel est le code secret d'Alice ?
3 *(1 point)* La stratégie d'Alice est-elle bonne si elle cache le type de chiffrement qu'elle utilise ?
4 *(1 point)* On suppose que le code secret d'Alice lui sert à s'authentifier sur un site internet qui ne limite pas le nombre d'essais d'authentification. Le code secret d'Alice contient-il suffisamment d'entropie (est-il suffisamment grand) ? Justifier.

Exercice 2 - des mauvais PRGs (6 points)

On rappelle la définition d'un PRG (Générateur Pseudo Aléatoire). Il s'agit d'une fonction $G : \{0,1\}^s \to \{0,1\}^{n+s}$ telle que la sortie y, de longueur $n+s$ bits est indistinguable d'une suite aléatoire sans connaître l'entrée x (de s bits). Les trois PRGs suivants ne sont pas sûrs. Notations en bas de page [1].

Pour chacun des PRGs suivants g_1, g_2 et g_3, décrire la faiblesse et donner ce qu'un adversaire doit calculer (en fonction de la sortie) afin de distinguer la sortie d'une sortie aléatoire. Justifier.

$$\begin{array}{rcccc} g_1 & : & \{0,1\}^{256} & \to & \{0,1\}^{384} \\ & & x=(x_1||x_2) & \mapsto & (x_1 \ll 0)||(x_2 \ll 42)||(x_1 \oplus x_2) \end{array}$$

$$\begin{array}{rcccc} g_2 & : & \{0,1\}^{256} & \to & \{0,1\}^{384} \\ & & x=(x_1||x_2) & \mapsto & (x_1)||(x_1 \oplus x_2)||(\texttt{AES}_{x_2}(x_1)) \end{array}$$

$$\begin{array}{rcccc} g_3 & : & \{0,1\}^{32} & \to & \{0,1\}^{128} \\ & & x=(x_1||x_2) & \mapsto & \texttt{AES}_{x_1||0^{112}}(x_2||0^{112}) \end{array}$$

1. Dans la description de chacune de ces fonctions, l'entrée est découpée en deux parts égales (notées à chaque fois x_1 et x_2). $||$ est l'opérateur de concaténation, $\ll$ désigne un décalage cyclique (les bits de poids forts sont remis dans les bits de poids faibles). $\oplus$ est l'opérateur XOR et `AES` le chiffrement par bloc considéré ici comme une permutation pseudo-aléatoire, et $\texttt{AES}_a(b)$ est l'AES appliqué à l'entrée b et avec comme clef secrète a. 0^n désigne la chaîne de bits constituée de n zéros consécutifs.