Licence 3 Informatique 2024–2025
LSIN603 – Cryptographie – CC1– 1h30

Les documents ne sont pas autorisés. Tout support numérique est interdit. Toute erreur dans le sujet sera prise en compte dans la correction. Le barème est donné à titre indicatif. La qualité de la rédaction sera prise en compte dans la notation.

Questions de cours (10 points)

On considère l'ensemble $A = \{0, 1, 2\}$.

1 *(1 point)* Donner la définition complète de la fonction de chiffrement de Vernam (ou one-time-pad) sur cet ensemble en utilisant des notations mathématiques.

2 *(1 point)* Expliquer en français ce qu'est un chiffrement inconditionnellement sûr.

3 *(2 points)* Que faut-il faire pour que le chiffrement de Vernam (ou one-time-pad) soit inconditionnellement sûr ? Détailler précisément.

Soient M, C et K trois ensembles dénotant respectivement l'ensemble des messages clairs possibles (M), l'ensemble des chiffrés (C) et l'ensemble des clefs possibles (K). On considère maintenant une fonction de chiffrement E : $K \times M \to C$.

4 *(2 points)* Indépendamment de sa sécurité, quelle propriété mathématique doit vérifier la fonction E ? Écrire cette propriété sous forme de prédicat (en langage mathématique).

5 *(1 points)* Dans quel modèle d'attaque fonctionne la recherche exhaustive ? Expliquer.

6 *(1 point)* Expliquer avec vos mots pourquoi la recherche exhaustive ne fonctionne pas sur le one-time-pad lorsque celui-ci vérifie la propriété de chiffrement inconditionnellement sûr.

7 *(2 points)* Donner le pseudo-code correspondant à l'attaque par recherche exhaustive sur la fonction de chiffrement E définie plus haut. Préciser les entrées et les sorties de l'algorithme ainsi que tout ce qui est connu par l'attaquant pour pouvoir réaliser l'attaque.

Exercice 1 (5 points)

Soient M, C et K trois ensembles dénotant respectivement l'ensemble des messages clairs possibles (M), l'ensemble des chiffrés (C) et l'ensemble des clefs possibles (K). On considère maintenant une fonction de chiffrement E : $K \times M \to C$. On note $N_k = \#K$ et $N = \#M = \#C$ (on considère que l'espace des messages clairs et l'espace des chiffrés sont de même taille). Un attaquant observe un chiffré noté $c \in C$.

1 *(1 point)* Dans un contexte de chiffrement **pratique**, donner un critère nécessaire pour garantir la sécurité du chiffrement aujourd'hui sur N_k.

2 *(1 point)* Dans quel contexte un attaquant peut-il obtenir un chiffré seul en pratique ?

3 *(1 point)* Dans quel contexte un attaquant peut-il obtenir un couple clair-chiffré en pratique ?

4 *(2 points)* Combien de messages $m \in M$ peuvent correspondre au chiffré $c \in C$ observé ? La réponse doit être la plus précise possible en fonction des hypothèses et définitions de cet exercice.

Exercice 2 (5 points)

On considère un chiffrement qui opère sur $\{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}^7$ qui réalise d'abord une substitution de l'alphabet puis une transposition. La clef est ici la donnée de la substitution et de la transposition. On rappelle qu'une substitution consiste à remplacer chaque lettre de l'alphabet par une (autre) lettre de l'alphabet. On rappelle qu'une transposition consiste à déplacer les positions des lettres selon une application bijective (ici de $\{1, \ldots, 7\}$ vers $\{1, \ldots, 7\}$).

1 *(1 point)* Combien y'a t'il de clefs pour ce chiffement ?

2 *(4 points)* On observe les couples clairs chiffrés suivant. Quel est le message clair correspondant à `BCGMMHN` ?

clairs	chiffrés
MGNQSCO	JOANZGY
EFMJGOT	ZGMATFB
DBIHRWU	CKHLIUR
VKULDAP	HXWUSPE