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. **Attention :** Tout doit être clair et précis. Ce qui n'est pas clair sera considéré comme faux.

Questions de cours (10 points)

1 *(2 points)* Donner deux applications des fonctions de hachage cryptographiques. Détaillez dans chacune de ces applications pourquoi il est nécessaire d'avoir une fonction de hachage cryptographique.

2 *(1 point)* Que se passe-t-il si un chiffrement par bloc de type SPN utilise les mêmes clefs de tours. Est-ce problématique si la taille du bloc du chiffrement est de 256 bits ? Justifiez.

4 *(2 points)* Dessinez les schémas du chiffrement et du déchiffrement du mode CBC (Cipher Bloc Chaining) qui utilise un chiffrement par bloc noté E. On veillera à faire apparaître tous les éléments, de telle sorte que le chiffrement qui en résulte soit sécurisé.

5 *(2 points)* Décrire le cryptosystème RSA, et en particulier la génération des clefs privées et publiques. Quelles tailles (en bit) doivent avoir ces clefs pour garantir une sécurité suffisante aujourd'hui ?

6 *(2 points)* Justifiez pourquoi le chiffrement RSA est correct (pourquoi le déchiffrement appliqué au résultat du chiffrement redonne le message d'origine). On se restreindra au cas m premier avec le module N.

7 *(1 point)* RSA est l'algorithme asymétrique le plus utilisé aujourd'hui. Expliquez pourquoi cet algorithme cryptographique n'est pas sécurisé.

Exercice 1 - Complexité du cryptosystème d'El-Gamal (7 points)

Le but de cet exercice consiste à analyser la complexité du problème du logarithme discret face à la complexité du chiffrement El-Gamal pour un utilisateur honnête. On se place dans un groupe $(G, \times)$, d'ordre $n = |G|$. On suppose que l'on connaît un générateur g de G. **Important :** On ne précise pas dans quel groupe on se trouve.

1 *(1 point)* Donnez en pseudo-code l'algorithme de génération de clefs (publiques et privées) pour le cryptosystème d'El-Gamal et donnez la fonction de chiffrement.

2 *(1 point)* On suppose que les éléments du groupe G peuvent s'encoder sur $\ell = \lceil \log_2(n) \rceil$ bits. Quelle taille font les chiffrés dans le cryptosystème d'El-Gamal ?

On note C_{mul} le coût algorithmique d'une multiplication (la loi du groupe G, notée $\times$). On note C_{alea} le coût de générer un bit aléatoire.

3 *(3 points)* Justifiez et détaillez pourquoi on peut dire que la complexité de génération de clef ainsi que le chiffrement est en $\mathcal{O}(\ell \times (C_{mul} + C_{alea}))$

4 *(2 points)* (a) Rappelez le problème du logarithme discret.

(b) On suppose qu'un adversaire est en mesure de casser le log discret. Sous cette hypothèse, montrer que El-Gamal n'est pas sécurisé.

Exercice 2 - Authentification avec du padding (4 points)

Un ancien étudiant (qui n'a pas suivi le cours de cryptographie LSIN603) est responsable de donner une solution de chiffrement authentifié à son entreprise. Après plusieurs recherches, cet étudiant se rend compte que l'on peut utiliser du padding, chiffrer et utiliser le padding comme vérification d'une potentielle altération du message par un attaquant actif. L'ancien étudiant propose d'utiliser un chiffrement par bloc E opérant sur 128 bits et avec une clef secrète de 128 bits sécurisé : l'AES-128. Puis, il explique que :

1. Alice applique un padding injectif au message m afin que $\texttt{pad}(m)$ ait une longueur multiple de 128. Pour garantir une sécurité de 128 bits, l'ancien étudiant propose le padding suivant : il faut toujours rajouter un 1 puis que des zéros pour avoir un message de longueur multiple de 128 **et** rajouter exactement 128 zéros.
2. Alice applique ensuite le mode CBC à $\texttt{pad}(m)$ ce qui donne un chiffré c.

La procédure de vérification va être la suivante :

1. Bob déchiffre c avec le déchiffrement de CBC.
2. Si Bob ne trouve pas 128 zéros à la fin du message, il dit qu'il détecte un attaquant actif au milieu du canal de communication.

L'ancien étudiant se justifie en expliquant que « tout est chaîné vers la fin » et donc une modification à n'importe quel endroit, engendrera une modification sur toute la chaîne et qu' il y a une probabilité de 2^{-128} que le dernier bloc ne contienne que des « zéros » s'il y a eu modification.

Question : Expliquez pourquoi l'ancien étudiant à tout faux et pourquoi ce qu'il propose ne permet pas de garantir l'authenticité et l'intégrité des messages transmis.