Licence 3 Informatique 2024–2025
LSIN603 – Cryptographie – CC2– 1h10

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 (11 points)

On considère un chiffrement par bloc E qui opère sur des blocs de 64 bits et qui utilise une clef de taille 128 bits.

1 *(1 point)* Donner les espaces d'entrée et de sortie du chiffrement par bloc.
2 *(1 point)* Indépendamment de sa sécurité, quelle propriété mathématique doit vérifier la fonction E ?
3 *(1 point)* Afin de pouvoir utiliser le chiffrement par bloc E en pratique, il est nécessaire que la construction assure deux propriétés définies par Claude Shannon. Énoncez ces propriétés et leur signification.
4 *(1 point)* Expliquer dans quel modèle d'attaque fonctionne la recherche exhaustive. Combien de données sont nécessaires ici pour garantir (avec grande probabilité) que l'algorithme de la recherche exhaustive renvoie uniquement la clef secrète utilisée ?
5 *(1 point)* Donner le pseudo-code de la recherche exhaustive.
6 *(1 point)* Décrire avec vos mots le principe d'un algorithme de chiffrement asymétrique.
6 *(2 points)* Donner la description complète de la fonction de chiffrement du cryptosystème RSA.
7 *(1 point)* Parmi tous les paramètres de RSA, donner tous ceux qui sont publics et tous ceux qui doivent rester secret.
8 *(2 points)* Expliquer en détail le coût algorithmique de la fonction de chiffrement RSA (on supposera ici que le module RSA est de taille ℓ bits).

Exercice 1 (5 + 1 points) - Des tours de Feistel

Le but de cet exercice est d'analyser la sécurité d'un schéma de Feistel sur 4 tours. On essaye de construire un chiffrement par bloc où la taille des blocs est de 64 bits et la clef est de taille 128 bits. Soit f une fonction de $\{0,1\}^{32}$ dans $\{0,1\}^{32}$. Soit k_i une clef de tour. Un tour de Feistel est alors défini par la fonction suivante.

$$\begin{array}{rccc} F_{k_i} & : & \{0,1\}^{64} & \to & \{0,1\}^{64} \\ & & L||R & \mapsto & R||(L \oplus f(R \oplus k_i)) \end{array}$$

où L et R sont respectivement les parties gauche et droite de la valeur en entrée de la fonction, de longueur 32 bits et $||$ est l'opérateur de concaténation.

Pour réaliser notre chiffrement par bloc, on découpe la clef de taille 128 bits en 4 clefs de taille 32 bits : $K = k_1||k_2||k_3||k_4$. Le chiffrement par bloc est alors défini par

$$E_K(m) = F_{k_4} \circ F_{k_3} \circ F_{k_2} \circ F_{k_1}(m)$$

1 *(1 point)* Dessiner le schéma (circuit) complet du chiffrement par bloc défini juste au dessus.
2 *(1 point)* En considérant un modèle à clair connu, dessiner, sur votre schéma quelles parties du circuit un attaquant peut avoir accès.
3 *(1 point)* En déduire une attaque nécessitant presque aucune mémoire et dans le modèle à clair connu qui coûte environ 2^{96} opérations (une analyse plus fine de la complexité de l'attaque peut donner un point bonus).
4 *(2 points)* Proposer une autre attaque sur ce chiffrement par bloc. Pour cette question, des mots-clefs ne seront pas suffisant, il faudra décrire vos idées en les justifiant.

Exercice 2 (5 points) - Signatures sur RSA

On considère le module RSA $N = 323$.

1 *(2 points)* Donner une clef secrète valide pour ce module. Justifier.
2 *(2 points)* Calculer la signature pour le message $m = 18$ avec votre clef secrète.
3 *(1 point)* Donner la clef publique permettant la vérification.