LSIN603 – Cryptographie – Rattrapage – 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 (9 points)

1 *(1,5 points)* Expliquer le fonctionnement de la machine Enigma en détail.
2 *(2 points)* Rappeler les 4 modèles d'attaque vus en cours et leur définition. Ces modèles sont-ils tous pertinents en pratique ? Justifier et argumenter votre réponse.
3 *(2 points)* Comment fonctionne un certificat ? À quoi sert un certificat ? Détailler précisément votre réponse et expliquer en quoi nous devons avoir confiance.
4 *(1 point)* Pourquoi l'algorithme du DES n'est-il plus recommandé aujourd'hui ?
5 *(1,5 points)* On considère que l'on a un chiffrement par bloc $E : K \times \{0,1\}^n \to \{0,1\}^n$ où K est l'espace des clefs. Donner des critères nécessaires sur n et sur la taille de l'espace K afin de permettre d'assurer une sécurité suffisante aujourd'hui. Expliquer.
6 *(1 point)* On considère un chiffrement par bloc E. Dessiner le schéma du mode CBC. À quoi faut-il faire attention avec le vecteur d'initialisation (IV) ?

Exercice 1 (6 points) - Clef et IV reliés

On considère un chiffrement par bloc E opérant sur n bits et qui utilise une clef de longueur ℓ bits.

1 *(0,5 points)* Si le mode CBC est utilisé et que deux blocs de chiffrés sont identiques, quelle information un attaquant peut-il avoir sur le message clair ?

Pour éviter le problème précédent, nous allons réaliser une variante du mode CBC. Soit α un entier. Soit $m = m_0||m_1||\cdots||m_\alpha$ le message à chiffrer où, pour tout i allant de 0 à α, $m_i \in \{0,1\}^n$. Alors $c = c_0||c_1||\cdots||c_\alpha$ sera construit comme suit. Pour tout i allant de 0 à α, $c_i = E_{k\oplus IV\oplus i}(m_i)$.

2 *(1 point)* Dessiner le schéma du déchiffrement et expliquer comment la personne qui réceptionne le message chiffré c peut bien récupérer le message initial.
3 *(1 point)* Expliquer pourquoi le problème de la question 1 ne se pose plus.

On suppose maintenant la propriété suivante. Pour tout $m \in \{0,1\}^n$ et pour tout $k, k' \in \{0,1\}^\ell$, si $E_k(m) = E_{k'}(m)$, alors $k = k'$.

4 *(1 point)* Cette propriété peut-elle être atteinte si $\ell > n$? Et si $\ell < n$?
5 *(1 point)* Si $m_i = 0$ pour tout i allant de 0 à α et qu'un attaquant calcule $E_{k_0}(0)$ pour une valeur k_0 prise aléatoirement, à quelle condition cet attaquant peut-il retrouver la clef k utilisée ?
6 *(1,5 points)* En déduire une amélioration de l'attaque par recherche exhaustive qui nécessite $\frac{2^\ell}{\alpha+1}$ calculs par l'attaquant de la fonction de chiffrement E lorsque un utilisateur a transmis le chiffré du message décrit à la question précédente, i.e. le message qui n'a que des zéros concaténés $\alpha+1$ fois ($\alpha+1$ blocs).

Exercice 2 (5 points) - Collisions sur RSA

On considère le module RSA N de taille ℓ bits. L'idée de cet exercice est d'analyser la complexité d'une autre stratégie de factorisation. Sans perdre de généralité, on suppose que $p < q$.

1 *(1 point)* A priori p est de quelle taille ? Et q ?
2 *(1,5 points)* Soient x et y deux entiers connus par un attaquant. Si $x \neq y$ et que $x = y \mod p$, montrer comment l'attaquant peut factoriser le module N.

On part du principe que si on collecte $\sqrt{p}$ entiers, alors avec grande probabilité il existera deux entiers parmis ceux-là qui vérifient la propriété précédente.

3 *(2,5 points)* En déduire une attaque sur le cryptosystème RSA avec un coût de $2^{\ell/4}$ opérations environ. Expliquer en détail.