LSIN603 – Cryptographie – Examen – 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)* Décrire entièrement le chiffrement de Vernam ou One-Time-Pad. Quelle propriété ce chiffrement permet-il d'atteindre ? Pourquoi ce chiffrement n'est pas utilisé ?
2 *(1,5 points)* À quoi sert la construction Feistel ? Quelle propriété cette construction permet-elle d'atteindre ?
3 *(1,5 points)* Comment fonctionne un certificat ? À quoi sert un certificat ?
4 *(1,5 points)* Le gouvernement français souhaite concevoir son propre système de chiffrement pour l'utilisation de ses services. Afin d'améliorer la sécurité de ses services, le gouvernement demande à deux cryptographes français et reconnus de le concevoir. Un cryptographe a la tâche de concevoir l'algorithme et l'autre cryptographe analyse sa sécurité. Le deuxième cryptographe ne trouve pas de failles dans le système. L'état décide donc d'utiliser ce chiffrement. Pour éviter d'autres failles, l'état ne publie pas l'algorithme cryptographique et le garde secret, ainsi que le rapport du cryptographe ayant réalisé l'analyse du chiffrement. Que pensez-vous de cette stratégie ? Détailler précisément.
5 *(1,5 point)* Donner un système de *padding* (bourrage) injectif, permettant de transformer n'importe quelle chaîne de bits, de longueur arbitraire en n'importe quelle chaîne de bits de longueur multiple de 128.
6 *(1,5 points)* On considère un chiffrement par bloc E. Dessiner le schéma du mode CBC. À quoi sert le vecteur d'initialisation (IV) ?

Exercice 1 (7 points) - Le Meta-Feistel

Pour tout n et pour toute fonction $F : \{0,1\}^n \to \{0,1\}^n$, on définit classiquement la construction en Feistel, avec la formule suivante.

$$\begin{array}{rccc} \mathsf{Feistel}[F] & : & \{0,1\}^{2n} & \to & \{0,1\}^{2n} \\ & & L||R & \mapsto & R||(L \oplus F(R)) \end{array}$$

On définit aussi la construtions en Feistel mais sans l'échange de branche. On la note $\mathsf{Feistel}_0$. Plus précisément, on a

$$\begin{array}{rccc} \mathsf{Feistel}_0[F] & : & \{0,1\}^{2n} & \to & \{0,1\}^{2n} \\ & & L||R & \mapsto & (L \oplus F(R)||R) \end{array}$$

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

Soit n un entier et f une fonction de $\{0,1\}^n$ dans $\{0,1\}^n$. On souhaite, avec cette fonction et les constructions Feistel définies précédemment, être capable de concevoir un chiffrement par bloc sur $4n$ bits. On considère une suite de clefs secrètes $k_0, k_1, \ldots, k_\ell$ dans $\{0,1\}^n$. Plus précisément, pour tout i compris entre 0 et ℓ, on définit la fonction de tour $R_i = \mathsf{Feistel}[\mathsf{Feistel}_0[g_{k_i}]]$, où $g_{k_i}(x) = f(x \oplus k_i)$ pour tout $x \in \{0,1\}^n$.

1 *(2 points)* Dessiner le schéma de la fonction de tour R_0.
2 *(2 points)* Soit $x_0^0||x_1^0||x_2^0||x_3^0$ le bloc de message clair donné en entrée. Pour tout i compris entre 0 et ℓ, on note $x_0^{i+1}||x_1^{i+1}||x_2^{i+1}||x_3^{i+1} = R_i(x_0^i||x_1^i||x_2^i||x_3^i)$. Donner l'expression mathématique de $x_0^{i+1}||x_1^{i+1}||x_2^{i+1}||x_3^{i+1}$ en fonction de $x_0^i||x_1^i||x_2^i||x_3^i$, de la clef de tour k_i et de la fonction f.
3 *(1 point)* Soit $i \geq 0$. Montrer que si x_1^i et x_3^i sont ne dépendent pas de la clef secrète, alors x_1^{i+1} et x_3^{i+1} ne dépendent pas non plus de la clef secrète.
4 *(1 point)* Montrer que ce chiffrement n'est pas sûr peu importe le nombre de tours.

Exercice 2 (7 points) - Cryptanalyse de RSA

On considère le module RSA N de taille ℓ bits. Une manière d'attaquer RSA consiste à chercher à factoriser le module N et à trouver les entiers p et q tels que $N = pq$. L'idée de cet exercice est d'analyser la complexité des stratégies de factorisation. Sans perdre de généralité, on suppose que $p < q$.

1 *(1 point)* Donner le pseudo-code de l'algorithme réalisant les divisions successives pour factoriser N.
2 *(1 point)* Donner une borne sur la complexité de cet algorithme (en nombre de divisions euclidiennes) en fonction de ℓ. Votre borne doit être la plus précise possible.
3 *(1,5 point)* Donner un algorithme efficace qui permet de dire si un entier est un carré parfait.
4 *(1,5 points)* En supposant l'existence d'un entier t tel que $N + t^2$ soit un carré parfait (i.e. il existe a tel que $N + t^2 = a^2$), montrer comment, à partir de t et de a, on peut retrouver les entiers p et q.
5 *(2 points)* En déduire un algorithme qui factorise RSA et est efficace quand $q - p$ est petit. Donner son pseudp-code.