UE ISEC
M1 Informatique

Partiel. Durée : 2 heures.

Les documents sont interdits
Téléphones portables éteints et rangés dans vos sacs.

Le barème est indicatif et est susceptible d'être modifié.
Toutes les réponses doivent être justifiées.
La clarté et la qualité de la rédaction seront considérées dans la notation.

Exercice 1 (5 points)

- Expliquer comment fonctionne l'authentification avec un MAC. Décrire le CBC-MAC.
- Comment chiffrer et déchiffrer avec le triple DES. Donner son niveau de sécurité (avec une justification)
- Donner la définition d'une fonction à sens unique avec trappe.
- Quelle est la fonction à sens unique avec trappe utilisée dans RSA.
- Comment construire un schéma de signature à partir d'une fonction à sens unique avec trappe.

Exercice 2 (4 points)

On considère un schéma de Feistel à deux tours sur des chaînes de 8 bits avec deux fonctions f_1 et f_2. On pose

$$f_1(a) := a \oplus 1011 \text{ et } f_2(a) := \bar{a} \oplus 0101.$$

pour toute chaîne $a \in \{0,1\}^4$.

- Calculer l'image de la chaîne 11010011 par ce diagramme de Feistel.
- Soit $M = (L_0, R_0) \in \{0,1\}^4 \times \{0,1\}^4$. Exprimer la sortie $C = (L_2, R_2) \in \{0,1\}^4 \times \{0,1\}^4$ du schéma de Feistel en fonction de $M = (L_0, R_0)$.
- Déterminer une chaîne de 8 bits dont l'image par le diagramme est elle-même.

Exercice 3 (5 points)

On considère dans cet exercice le chiffrement RSA. Soit $e = 3$ l'exposant commun de chiffrement pour envoyer à 3 personnes différentes le même message M. Chaque personne possède sa propre clé publique (e, N_i) pour $i, 1 \leq i \leq 3$. On note par C_i le chiffrement du message M avec le modulo public N_i et l'exposant de chiffrement 3. On considère le système de congruences suivant :

$$\begin{aligned} X &\equiv C_1 \mod N_1 \\ X &\equiv C_2 \mod N_2 \\ X &\equiv C_3 \mod N_3 \end{aligned}$$

— Montrer que $X = M^3$ est une solution particulière du système de congruences.
— On suppose que les $N_i, i, 1 \leq i \leq 3$ sont premiers entres eux deux à deux. Expliquer comment retrouver une solution S du système de congruences modulo $N_1N_2N_3$. Vous donnerez également l'expression de la solution en fonction des donnés publiques.
— Montrer que $S \equiv M^3 \bmod N_1N_2N_3$.
— Montrer ensuite que $S = M$.
— En utilisant les questions précédentes, proposer une technique permettant de retrouver efficacement le message M.
— Que concluez-vous sur l'utilisation du même exposant de chiffrement (mais de 3 modules distincts) pour chiffrer un même message. Il faudra justifier votre réponse.

Exercice 4 (5 points)

On considère une fonction de hachage MyHash. On note par $(\mathrm{PK_{CA}}, \mathrm{SK_{CA}})$ un couple (clef publique, clef secrète) d'une autorité de certification CA, et le même type de couple $(\mathrm{PK_{Cl}}, \mathrm{SK_{Cl}})$ pour un client Cl. Le certificat associé à la clef publique du client est :

$$\mathrm{certif} = \mathrm{Sign}_{\mathrm{SK_{CA}}}\big(\mathrm{MyHash}(\mathrm{PK_{Cl}})\big),$$

où Sign est l'algorithme de signature de l'autorité de certification. On note aussi par Verif l'algorithme de vérification associé à la clef publique de l'autorité de certification. Pour tester la validité d'un certificat certif d'une clef publique $\mathrm{PK_{Cl}}$, un utilisateur doit vérifier :

$$\mathrm{MyHash}(\mathrm{PK_{Cl}}) = \mathrm{Verif}_{\mathrm{PK_{CA}}}(\mathrm{certif}).$$

— Soient PK_1 et PK_2 des clefs publiques, et certif^* un certificat pour PK_2 généré par l'autorité de certification. On suppose que $\mathrm{MyHash}(\mathrm{PK}_1) = \mathrm{MyHash}(\mathrm{PK}_2)$. Donner un certificat valide pour PK_1 (avec une preuve).

Dans la suite, on suppose que nous effectuons le processus d'authentification **sans fonction de hachage** (c'est à dire MyHash(PK) = PK, pour tout PK). On suppose également :

$$\mathrm{Sign}_{\mathrm{SK}}(\mathrm{PK}_1 \cdot \mathrm{PK}_2) = \mathrm{Sign}_{\mathrm{SK}}(\mathrm{PK}_1) \cdot \mathrm{Sign}_{\mathrm{SK}}(\mathrm{PK}_2).$$

— Soient PK_1 et PK_2 des clefs publiques, certif_1 et certif_2 des certificats pour PK_1 et PK_2 respectivement générés par l'autorité de certification. Donner un certificat valide pour $\mathrm{PK}_1 \cdot \mathrm{PK}_2$ (avec une preuve).
— Soit (N, e) une clef publique RSA et d la clef secrète. Donner la définition de $\mathrm{SignRSA}_{N,d}$ la fonction de signature RSA (**sans fonction de hachage**) ainsi que l'algorithme de vérification correspondant $\mathrm{VerifRSA}_{N,d}$.
— Montrer que :

$$\forall (m_1, m_2) \in \mathbb{Z}_N \times \mathbb{Z}_N, \mathrm{SignRSA}_{N,d}(m_1 \cdot m_2) = \mathrm{SignRSA}_{N,d}(m_1) \cdot \mathrm{SignRSA}_{N,d}(m_2).$$