TP5 - Chiffrements asymétriques

ING3 CS – Cryptographie

Exercice 1. Exponentiation rapide

Soient $\alpha = 119$, $e = 231$ et $n = 419$.

(1) Combien de bits faut-il environ pour écrire la valeur de α^e ?
Pour écrire la valeur de $\alpha^e \mod n$?
Est-ce raisonnable de calculer α^e puis d'effectuer l'opération modulo n sur le résultat? □

(2) En utilisant un minimum d'opérations, calculer les puissances de α modulo n suivantes :

$$\begin{aligned}
\alpha^1 &\equiv \mod n \\
\alpha^2 &\equiv \mod n \\
\alpha^4 &\equiv \mod n \\
\alpha^8 &\equiv \mod n \\
\alpha^{16} &\equiv \mod n \\
\alpha^{32} &\equiv \mod n \\
\alpha^{61} &\equiv \mod n \\
\alpha^{128} &\equiv \mod n
\end{aligned}$$

□

(3) En utilisant la décomposition binaire de e ainsi que les résultats obtenus à la question précédente, calculer $\alpha^e \mod n$. □

(4) Proposer un algorithme pour calculer $\alpha^e \mod n$ efficacement et sans dépassement de mémoire. Estimer sa complexité. □

Exercice 2. Chiffrement RSA

(5) Proposer une paire de clé RSA, avec $p = 41$ et $q = 73$.
Chiffrer le message $\mathbf{m} = 21$.
Déchiffrer le message $\mathbf{c} = 42$. □

Exercice 3. Signature RSA

On rappelle la signature RSA :

- Génération des clés :
  - choisir p et q premiers (~ 512 bits pour RSA-1024)
  - $n = pq$
  - $\varphi(n) = (p-1)(q-1)$
  - choisir e premier avec $\varphi(n)$
  - calculer d tel que $ed \equiv 1\ (mod\ \varphi(n))$
  - $\mathbf{k}_{pub}$ est constituée par le coupe (e,n).
  - $\mathbf{k}_{priv}$ est le nombre d (ou le couple (d,n)).
- Signature $(\mathbf{k}_{priv}, m) = \sigma = m^d \mod n$
- Vérification $(\mathbf{k}_{pub}, m, \sigma) = \begin{cases} \text{OUI} & \text{si } m \equiv \sigma^e \mod n \\ \text{NON} & \text{sinon} \end{cases}$

(6) ***Trivial forgery***
Soit $\sigma \in \mathbb{Z}_n^*$. Trouver un message m tel que σ soit une signature valide de m. □

(7) ***Maléabilité***
Soient (m_1, σ_1) et (m_2, σ_2) deux couples message/signature valides distincts. Trouver un troisième couple message/signature valide. □

(8) Vérifier vos réponses sur un exemple : $p = 1747$ et $q = 2131$. □

(9) Comment peut-on se prémunir des attaques évoquées dans les questions précédentes?
□