Cryptographie, HE-Arc, Automne 2025

Devoir 8 – Diffie-Hellman, RSA et théorème des Restes Chinois

Exercice 1

Considérez le protocole de Diffie-Hellman avec le groupe multiplicatif $\mathbb{Z}_{23}^*$ et le générateur $g = 5$.

1. Calculez toutes les puissances $g^x \mod p$ et vérifiez que g est un générateur. Quel est l'ordre de g ?
2. Alice choisit $a = 6$ et Bob choisit $b = 15$. Calculez les valeurs publiques y_A et y_B et calculez la clé secrète k partagée par Alice et Bob.

Exercice 2

Implémentez le protocole de Diffie-Hellman dans le langage de votre choix en incluant la génération des paramètres p, g, a, b, le calcul des valeurs publiques et la vérification que les deux parties trouvent la même clé partagée.

Exercice 3

1. Prenez deux petits nombres premiers entre 15 et 100 et calculez la clé publique et la clé privée **textbook RSA**.
2. Prenez le message $m = 88$. Calculez le texte chiffré et déchiffrez le message. Vérifiez que le message déchiffré correspond bien au message original.
3. Reprenez les mêmes clés et signez le message $m = 42$. Vérifiez la signature obtenue.
4. Illustrez la malléabilité des signatures textbook RSA en forgeant un signature valide à partir de la signature de l'exercice précédent.

Exercice 4

1. Résolvez le système $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$ et calculez la solution x modulo $m = 3 \times 5 \times 7$.
2. Résolvez le système $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 4 \pmod 9 \\ x \equiv 6 \pmod{11} \end{cases}$ et calculez la solution x modulo $m = 4 \times 9 \times 11$.
3. Résolvez le système $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 6 \\ x \equiv 3 \pmod 5 \end{cases}$ et calculez la solution x modulo $m = 4 \times 6 \times 5$.

Exercice 5

Nous avons vu en cours qu'on peut accélérer les signatures RSA avec le théorème des restes chinois. Donnez une indication du gain de performance obtenu en comparant la complexité de la géneration d'une signature avec et sans le théorème.

Exercice 6

Lors d'un échange de clés de Diffie–Hellman, un espion intercepte les données suivantes:

$n = 100565854163627669685492673611152324056537864222211881735860361612464000 1$, $g = 2$,
$A = 69434527391230101579566508447193428199794395175193812818426217103397216 1$,
$B = 45219809272265904064518788699770061112569516384310833106022960617800893$.

Cassez cet échange!