math202 : mathématiques pour le numérique
TD 5 : cryptographie asymétrique, arithmétique

Pierre Hyvernat
Laboratoire de mathématiques de l'université de Savoie
bâtiment Chablais, bureau 17, poste : 94 22
email : Pierre.Hyvernat@univ-savoie.fr
www : http://www.lama.univ-savoie.fr/~hyvernat/

Exercice 1 : arithmétique modulaire, puissances

Question 1. Faites les calculs suivants (sans calculatrice)
- $3^{16} \bmod 79$,
- $3^{20} \bmod 79$,
- $5^{32} \bmod 47$,
- $5^{41} \bmod 47$.

Question 2. En utilisant la formule

$$\begin{cases} g^0 = 1 \\ g^{2n} = g^n \times g^n \\ g^{2n+1} = g^n \times g^n \times g \end{cases}$$

et une fonction récursive, programmez une méthode efficace pour calculer le résultat de $g^n \bmod m$, même lorsque n est très grand.

Question 3. Estimez le nombre d'opérations faites pour calculer $3^n \bmod 10^{100}$ lorsque $n = 1024$, $n = 1023$, $n = 10^6$ et $n = 10^9$.

Exercice 2 : échange de clés de Diffie Hellman

Méthode :
- Alice et Bob choisissent un nombre premier p et un nombre g générateur de $\mathbf{Z}_p$, c'est à dire

$$\{g^1 \bmod p, g^2 \bmod p, g^3 \bmod p, ..., g^{p-1} \bmod p\} = \{1, 2, ..., p-1\}$$

- Alice choisit un nombre aléatoire a dans $\mathbf{Z}_p$ et envoie $g^a \bmod p$ à Bob
- Bob fait la même chose et envoie $g^b \bmod p$ à Alice
- Alice reçoit B et calcule $B^a \bmod p$ et Bob reçoit A et calcule $A^b \bmod p$
- ils tombent sur le même résultat.

Question 1. Faites tourner l'algorithme d'échange de clé de Diffie-Hellman avec les valeurs suivantes
- $p = 11$ comme nombre premier
- $g = 2$ comme générateur de $\mathbf{Z}/p\mathbf{Z}$
- $a = 4$ comme nombre secret choisi par Alice
- $b = 8$ comme nombre secret pour Bob

Détaillez les calculs en mettant en avant les messages échangés par Alice et Bob. Quelle est la clé ainsi obtenue ?

Question 2. Rappelez pourquoi Bob et Alice trouvent toujours le même résultat.

Question 3. Que se passe-t'il si le canal de communication est compromis et qu'un observateur malveillant (Eve) écoute les communications ?

Comment est-ce que Eve pourrait trouver le résultat partagé par Alice et Bob ?

Pourquoi n'est-ce pas raisonnable ?

Question 4. Adaptez l'échange de clé de Diffie-Hellman au cas où n personnes veulent échanger une clé commune.

Exercice 3 : attaque "man in the middle"

Les systèmes cryptographiques mentionnés jusqu'à présents sont sûrs, même si quelqu'un écoute les communications.

Par contre, si un attaquant peut en plus modifier les messages, de nombreux systèmes sont vulnérables à une attaque "man in the middle" : un attaquant (Eve) intercepte les message entre Alice et Bob et se fait passer pour eux.

Question 1. Décrivez en détail le fonctionnement d'une telle attaque où Eve arrive à décrypter tous les messages entre Alice et Bob, sans qu'ils ne s'en rendent compte.

Question 2. Chercher des solutions pour contrer ce type d'attaques.