info528 : Mathématiques pour l'informatique
TD 4 : cryptographie

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

Rappels :

- si a et b sont premier entre eux, alors il existe x et y vérifiant $ax + by = 1$. Dans ce cas, on dit que x est l'inverse de a modulo b. (Car $ax = 1 \pmod b$.)
- si p est un nombre premier, alors $\mathbf{Z}_p = \{0, 1, \dots, p-1\}$ avec l'addition et la multiplication modulo p est un *corps*. Chaque nombre non nul a donc un inverse que l'on peut calculer avec l'algorithme d'Euclide pour le pgcd.
- si p est premier et $a \in \mathbf{Z}_p$, alors $a^{p-1} = 0 \pmod p$.

Exercice 1 : cryptographie sans clé

Méthode : p est un nombre premier

- pour envoyer $M < p - 1$, Alice choisit un nombre a secret premier avec $p - 1$ et envoie $X = M^a \bmod p$ à Bob
- Bob choisit un nombre b premier avec $p - 1$ et renvoie $Y = X^b \bmod p$ à Alice
- Alice renvoie $Z = Y^{a'} \bmod p$ à Bob, où a' est l'inverse de a modulo $p - 1$
- Bob calcule $Z^{b'}$ où b' est l'inverse de b modulo $p - 1$. Le résultat est le message M

Question 1. En utilisant ce système, encryptez le nombre 9 en partant du nombre premier 13. Alice et Bob utiliseront les nombres $a = 5$ et $b = 11$. Que constatez-vous ?

Question 2. Même question en utilisant $a = 3$ et $b = 7$ pour coder le message 7. Que constatez-vous ?

Question 3. En utilisant vos calculatrices / ordinateurs, utilisez les nombres $p = 1367$ $a = 129$ et $b = 1201$ pour transmettre $M = 666$.

Exercice 2 : Échange de clés de Diffie-Hellman

Méthode :

- Alice et Bob choisissent un nombre premier p et un nombre g générateur de $\mathbf{Z}_p$
- 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. Expliquez pourquoi Bob et Alice trouvent le même résultat.

Question 2. 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 3. 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 4. Vérifiez que 2 est bien un élément générateur de $\mathbf{Z}/p\mathbf{Z}$. Est-ce que 3 est générateur ? Que se passe-t'il si g n'est pas générateur ?

Question 5. Pouvez-vous généraliser le protocole d'échange pour partager une clé entre trois personnes ? Entre quatre ?

Exercice 3 : système Elgamal

Méthode : p est un nombre premier et g est un générateur du groupe $\mathbf{Z}_p$;
- Bob choisit un nombre b secret et publie sa clé $K_B = g^b \bmod p$
- pour envoyer M, Alice choisi un nombre k secret et envoie $(g^k, K_B^k * M \bmod p)$ à Bob
- à la réception de (C_1, C_2), Bob calcule C_2/C_1^b et obtient M.

Question 1. Justifier le système en montrant que Bob récupère bien le message d'Alice.

Question 2. En prenant $p = 13$ et $g = 2$, faites les calculs et vérifications suivantes
- g est un élément générateur de $\mathbf{Z}_p$
- quelle est la clé publique de Bob si sa clé privée est $b = 9$?
- comment Alice code-t'elle le message 10 si elle choisit une clé temporaire $k = 6$?
- comment Bob décode-t'il le message ? Est-ce que ça a marché ?

Question 3. Que se passe-t'il si on utilise un nombre g qui n'est pas générateur ?

Question 4. Que se passe-t'il si on utilise un nombre p non premier ?

Question 5. Supposons qu'Alice utilise tout le temps la même clé k pour coder son message. Un observateur malveillant Eve peut alors obtenir des informations précieuses... Si Alice encode M_1 et M_2 avec k et Eve parvient à écouter les communications, elle pourra connaître la valeur de M_1/M_2. Comment ?

Comment est-ce que Eve peut mettre cette connaissance à profit ?