info607 : Mathématiques pour l'informatique
TD 5 : cryptographie

Pierre Hyvernat
Laboratoire de mathématiques de l'université Savoie Mont Blanc
bâtiment Chablais, bureau 17, poste : 94 22
email : Pierre.Hyvernat@univ-smb.fr
www : http://www.lama.univ-smb.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 $a^{p-1} = 1 \pmod p$.

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 vos calculatrices / ordinateurs, utilisez les nombres $p = 1367$ $a = 129$ et $b = 1201$ pour transmettre $M = 666$ pour tester le protocole.

Solution :
- $M^a \bmod 1367 = 1043$
- $1043^{1201} \bmod 1367 = 34$
- $a^{-1} = 593 \pmod{1366}$ et $b^{-1} = 505 \pmod{1266}$
- $34^{593} \bmod 1367 = 483$
- $483^{505} \pmod{1367} = 666$

Question 2. Prouvez que le protocole est correct.

Question 3. Pourquoi ce protocole n'est il pas utilisé ?

Solution : trop d'échanges entre Alice et Bob...

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. Rappelez pourquoi Bob et Alice trouvent toujours 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

Solution : $2^4 \bmod 11 = 5$, $5^8 \bmod 11 = 4$ $2^8 \bmod 11 = 3$ $3^4 \bmod 11 = 4$

Question 4. Vérifiez que 2 est bien un élément générateur de $\mathbf{Z}/p\mathbf{Z}$. Est-ce que 3 est générateur ?

Solution : 3 n'est pas générateur car $3^5 = 1 \pmod{11}$.

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. Justifiez 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 ?

Solution :

- g est bien générateur
- la clé publique de Bob est 5
- le code est $(12, 3)$
- comme l'inverse de 12 est 12 ; Bob trouve $M = 3 * 12 \pmod{13} = 10$.

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

Solution : ça marche, mais une cryptanalyse est plus facile (moins de nombres à tester pour le logarithme discret)

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

Solution :

- si g n'est pas premier avec p, alors on risque de tout collapser car $g^n = 0 \pmod{p}$ si n est grand
- sinon, le groupe engendré par g est plus petit (au plus de taille $\varphi(p)$) mais ça va marcher quand même.

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 ?

Solution : si Eve voit passer (K_1, C_1) et (K_2, C_2), alors on a $M_1/M_2 = C_1/C_2$.

Exercice 4 : le système RSA (Rivest, Shamir, Adleman)

Méthode :

- Bob choisit deux nombres premiers différents p et q et un nombre d premier avec $(p-1)(q-1)$. Il publie les nombres $n = pq$ et $e = d^{-1} \bmod (p-1)(q-1)$
- pour lui envoyer M, Alice calcule $C = M^e \bmod n$. Elle envoie C à Bob.
- pour décrypter, Bob calcule $C^d \bmod n$ et obtient M

Question 1.

Question 2. On suppose que Bob a choisi comme clé privée les nombres $p = 5$, $q = 11$ et $d = 17$

- quelle est la clé publique de Bob ?
- comment Alice s'y prend elle pour envoyer le message 12 à Bob ?
- comment Bob décrypte-t'il le message d'Alice ?

Question 3. Sur quel problème difficile est basé le système RSA ?

Exercice 5 : man in the middle

Question 1. 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".

Décrivez une telle attaque où Eve arrive à décrypter les messages entre Alice et Bob.

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

Solution :

- annuaire clé publiques avec réseau de confiance (pgp et autre)
- signature (avec l'infrastructure précédente)
- contraintes de temps
- certificats délivrés par un organisme sûr