info607 : mathématiques pour l'informatique

TD 5 : cryptographie 2 (cryptographie à clé publique)

Pierre Hyvernat
Laboratoire de mathématiques de l'université de Savoie
bâtiment Chablais, bureau 22
téléphone : 04 79 75 94 22
email : Pierre.Hyvernat@univ-savoie.fr
www : http://www.lama.univ-savoie.fr/~hyvernat/

Exercice 0 : cryptographie sans clé

Rappel et notation : 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 1 : cryptographie à clé publique, système Elgamal

Rappel et notation : 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 : 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 2 : que se passe-t'il si on utilise un nombre g qui n'est pas générateur ?

Question 3 : que se passe-t'il si on utilise un nombre p non premier ?

Question 4 : 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 ?

Exercice 2 : le système RSA (Rivest, Shamir, Adleman)

Rappel et notation :

- 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 : on suppose que Bob a choisi comme clé privée les nombres $p = 3$, $q = 11$ et $d = 3$

- 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 2 : pour la preuve que RSA fonctionne, on a dit "Bob reçoit $C = M^e \pmod n$, il obtient le message en calculant $C^d \bmod n$; ça marche par le théorème d'Euler (car on a $M^{\varphi(n)} = 1 \bmod n$)." Ceci n'est pas tout à fait exact, car le théorème d'Euler demande que M soit premier avec n.
Corrigez la justification de RSA en montrant les choses suivantes :

- $M^{e*d} = M \pmod p$
- $M^{e*d} = M \pmod q$
- si $u = v \pmod p$ et $u = v \pmod q$ alors $u = v \pmod{pq}$

Question 3 : on suppose que Bob possède deux clés privées d_1 et d_2 qui engendrent deux clés publiques (e_1, n) et (e_2, n). (Par exemple ; Bob vient de changer de clé...) Alice veut lui envoyer un message M, mais pour être sûr que Bob le reçoive bien, elle l'envoie en deux exemplaires : une fois en le cryptant avec la première clé (elle envoie C_1), une fois en cryptant avec la deuxième clé (elle envoie C_2).
Si Eve écoute les communications, elle peut parfois retrouver M : il suffit que e_1 et e_2 soient premiers entre eux et que C_1 et C_2 soient premiers avec n... Comment fait-elle ?
(Indice : écrire la relation de Bezout entre e_1 et e_2.)

Que se passe-t'il si C_1 ou C_2 n'a pas d'inverse ? Est-ce que ça arrive souvent ?