info528 : Mathématiques pour l'informatique
TD 3 : 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/

Exercice 1 : arithmétique

Question 1.
- expliquez pourquoi 0 divise n,
- est-ce que 0 divise 0 ?
- quels sont les multiples de -1 ?
- pourquoi est-ce que $\text{pgcd}(0,0)$ est indéfini ?

Question 2. Appliquez l'algorithme d'Euclide pour calculer les nombres de Bezout associés à
- $\text{pgcd}(5,9)$,
- $\text{pgcd}(8,38)$,
- $\text{pgcd}(6,21)$,
- $\text{pgcd}(22,75)$.

Question 3. Montrer que si $a \times x + b \times y = 1$ alors on a forcément $\text{pgcd}(a,b) = 1$.

Question 4.
- on a $1 = 3 \times 7 - 4 \times 5$, que pouvez-vous déduire sur 3, 7, 4 et 5 ?
- on a $4 = 6 \times 9 - 5 \times 10$, que pouvez-vous déduire sur 6, 9, 5 et 10 ?

Question 5. Les nombres 537138 et 412923 ont les représentations suivantes comme produits de facteurs premiers :

$$537138 = 2 \times 3^2 \times 7^3 \times 29 \quad \text{et} \quad 412923 = 3 \times 7^2 \times 53$$

Quel est leur pgcd ?

Question 6. Les équations suivantes ont-elles des solutions ? Si oui, donnez l'ensemble des solutions...
- $3x \equiv 5 \pmod 7$
- $2x - 3 \equiv 0 \pmod 4$
- $5x + 2 \equiv 0 \pmod 6$

Question 7. Montrez que $(3^{77} - 1)/2$ est un nombre impair. Montrez que ce même nombre est divisible par $(3^7 - 1)/2$ pour conclure qu'il n'est pas premier.

Montrez que si k n'est pas premier, alors $2^k - 1$ (nombre de Mersenne) n'est pas premier non plus.

Question 8. Quand est-ce que $2^n - 1$ est un multiple de 3 ?

Question 9. "Pour savoir si un nombre est divisible par 9, il suffit de vérifier si la somme de ces chiffres est divisible par 9".

Expliquer pourquoi cette règle par 9 fonctionne.

Exercice 2 : cryptanalyse simple

Décryptez le code suivant :

```
VI ! FSF ! Q'LZT XF KLX QSXNT, RLXFL ISGGL !
SF KSXYVUT PUNL. . .SI ! PULX !. . .JULF PLZ QISZLZ LF ZSGGL. . .
LF YVNUVFT HL TSF,--KVN LDLGKHL, TLFLO:
VCNLZZUA: "GSU, GSFZULXN, ZU R'VYVUZ XF TLH FLO
UH AVXPNVUT ZXN-HL-QIVGK MXL RL GL H'VGKXTVZZL !"
VGUQVH: "GVUZ UH PSUT TNLGKLN PVFZ YSTNL TVZZL !
KSXN JSUNL, AVUTLZ-YSXZ AVJNUMXLN XF IVFVK !"
PLZQNUKTUA: "Q'LZT XF NSQ !. . .Q'LZT XF KUQ !. . .Q'LZT XF QVK !
MXL PUZ-RL, Q'LZT XF QVK ?. . .Q'LZT XFL KÉFUFZXHL !"
QXNULXD: "PL MXSU ZLNT QLTTL SJHSFCXL QVKZXHL ?
P'ÉQNUTSUNL, GSFZULXN, SX PL JSÎTL À QUZLVXD ?"
CNVQULXD: "VUGLO-YSXZ À QL KSUFT HLZ SUZLVXD
MXL KVTLNFLHHLGLFT YSXZ YSXZ KNÉSQQXKÂTLZ
PL TLFPNL QL KLNQISUN À HLXN KLTUTLZ KVTTLZ ?"
TNXQXHLFT: "ÇV, GSFZULXN, HSNZMXL YSXZ KÉTXFLO,
HV YVKLXN PX TVJVQ YSXZ ZSNT-LHHL PX FLO
ZVFZ MX'XF YSUZUF FL QNUL VX ALX PL QILGUFÉL ?"
KNÉYLFVFT: "CVNPLO-YSXZ, YSTNL TÊTL LFTNVÎFÉL
KVN QL KSUPZ, PL TSGJLN LF VYVFT ZXN HL ZSH !"
TLFPNL: "AVUTLZ-HXU AVUNL XF KLTUT KVNVZSH
PL KLXN MXL ZV QSXHLXN VX ZSHLUH FL ZL AVFL !"
KÉPVFT: "H'VFUGVH ZLXH, GSFZULXN, MX'VNUZTSKIVFL
VKKLHHL IUKKSQVGKLHLKIVFTSQVGÉHSZ
```

(Plus d'info sur ma page web ; et un paquet de bonbons pour le premier qui m'envoie la réponse...)

Exercice 3 : Échange de clés de Diffie-Hellman

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

Question 4. Pouvez-vous généraliser le protocole d'échange pour partager une clé entre trois personnes ? Entre quatre ?

Exercice 4 : 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. 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 2. 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 ?

Exercice 5 : système Elgamal

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. 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 ?