Université de Lille 1 SCIENCES ET TECHNOLOGIES

L1 - SESI - 2016–2017

Arithmétique et Cryptographie

DS2 – Durée 2h
12 mai 2017

Toutes les réponses doivent être justifiées et vous soignerez votre rédaction.

Les documents son interdits, ainsi que les appareils électroniques (téléphones, ordinateurs portables, etc...). Seules les calculatrices sont autorisées.

Notez le numéro de votre groupe sur la copie.

Exercice 1

Dix individus souhaitent communiquer électroniquement de manière chiffrée. Il est important pour eux que chacun d'entre eux puissent communiquer avec une autre personne du groupe sans qu'aucune des huit autres personnes ne puissent lire le message.

1. S'ils utilisent un système de cryptographie symétrique (par exemple le chiffre de Vigenère), combien de clés au total doivent être fabriquées ?
2. Qu'en est-il s'ils utilisent un système de cryptographie à clé publique ?

Exercice

1. Énoncez le théorème de Fermat ainsi que son corollaire.
2. Calculez $3^{1082} \pmod{41}$.
3. Si p est un nombre premier, et a un nombre non divisible par p, expliquez pourquoi a est inversible modulo p et donner un entier $k > 0$ tel que $a^{-1} \equiv a^k \pmod{p}$.

Exercice 2

Partie I

Soient n_1 et n_2 deux entiers naturels premiers entre eux, c_1 et c_2 deux entiers.

1. Montrer que si $z \in \mathbb{Z}$ vérifie
$$\begin{cases} z \equiv 0 \mod n_1 \\ z \equiv 0 \mod n_2 \end{cases}$$
alors $z \equiv 0 \mod (n_1 n_2)$.
2. Énoncer le théorème de Bézout.
3. Montrer que les systèmes d'équations
$$(S_1) : \begin{cases} x \equiv 1 \mod n_1 \\ x \equiv 0 \mod n_2 \end{cases} \qquad (S_2) : \begin{cases} y \equiv 0 \mod n_1 \\ y \equiv 1 \mod n_2 \end{cases}$$
ont des solutions. On note x_0 une solution de (S_1) et y_0 une solution de (S_2).
4. (**Lemme des restes chinois**)
Montrer que $x = c_1 x_0 + c_2 y_0$ est solution du système d'équations
$$(S) : \begin{cases} x \equiv c_1 \mod n_1 \\ x \equiv c_2 \mod n_2 \end{cases}$$
Montrer que si y est une autre solution de (S) alors il existe $k \in \mathbb{Z}$ tel que $y = x + k n_1 n_2$, $k \in \mathbb{Z}$.

Partie II

Alice, Bruno et Corentin communiquent avec un système de cryptographie RSA. Leurs clés publiques sont (n_1, e), (n_2, e) et (n_3, e) : trois modulus différents mais à chaque fois le même exposant. Corentin veut envoyer à Alice et Bruno le même message m. Pour cela, il calcule $c_1 = m^e \mod n_1$ et l'envoie à Alice puis il calcule $c_2 = m^e \mod n_2$ et l'envoie à Bruno. Eve intercepte c_1 et c_2.

4. Si n_1, n_2 et n_3 ne sont pas deux à deux premiers entre eux, expliquer comment Eve peut déchiffrer le message.
5. Est-il probable que n_1, n_2 et n_3 ne soient pas deux à deux premiers entre eux ? Justifier.
6. Application : Si $n_1 = 221$, $n_2 = 299$, $n_3 = 391$, $e = 35$, $c_1 = 115$ et $c_2 = 271$, factoriser n_1 et trouver la clé privée d'Alice. En utilisant l'algorithme d'exponentiation modulaire, déchiffrer le message.

On suppose maintenant que n_1, n_2 et n_3 sont deux à deux premiers entre eux.

7. Montrer qu'il existe un unique $x \in \{0, \ldots, n_1 n_2 - 1\}$ tel que
$$\begin{cases} x \equiv c_1 \mod n_1 \\ x \equiv c_2 \mod n_2 \end{cases}$$
8. En déduire que si $m^e < n_1 n_2$ alors $m^e = x$.
9. Application : Avec $n_1 = 943$, $n_2 = 3233$, $n_3 = 1207$ et $e = 3$, Eve intercepte les messages chiffrés $c_1 = 328$ et $c_2 = 1892$. Retrouver le message clair.

Exercice 3

Soient p et q deux nombres premiers, $n = pq$, $\phi = (p-1)(q-1)$.

Partie I

1. Énoncer le théorème de Fermat amélioré.
2. Soit $m \in \mathbb{Z}$ tel que $\text{pgcd}(m, n) = 1$. Montrer que l'ensemble $M = \{k \in \mathbb{N}^* / \ m^k \equiv 1 \mod n\}$.

On pose $\mu_0 = \min M$. Le nombre μ_0 est appelé ordre de m modulo n.

3. Montrer que pour tout $s \in \mathbb{N}$, $m^{s\mu_0} \equiv 1 \mod n$.
4. Soit $\mu \in \mathbb{N}^*$ tel que $\mu^k \equiv 1 \mod n$. On note s et r respectivement le quotient et le reste de la division euclidienne de μ par μ_0. Montrer que $m^r \equiv 1 \mod n$. En déduire que μ est un multiple de μ_0.

Partie II

Alice et Bruno communiquent au moyen d'un système cryptographique RSA. La clé publique de Bruno est (n, e) où e est premier avec ϕ. On note (n, d) la clé privée de Bruno. Alice chiffre le message m et envoie $c = m^e \mod n$ à Bruno. Eve intercepte c et parvient à déterminer k tel que $c^{e^k} \equiv c \mod n$.

6. Si c n'est pas premier avec n, expliquer comment Eve peut factoriser n et retrouver m.
7. Donner tous les messages m tels que c n'est pas premier avec n. Combien y en a-t-il ? Si tous les messages sont équiprobables, quelle est la probabilité d'avoir un message m tel que c n'est pas premier avec n ?
8. Application : Si $(n, e) = (1271, 343)$ et $c = 186$. Factoriser n, déterminer la clé privée de Bruno. En utilisant l'algorithme d'exponentiation modulaire rapide, déchiffrer de le message.

On suppose à partir de maintenant que c est premier avec n.

7. Soit s un nombre premier. Montrer que si s divise m alors s divise c. En déduire que $\text{pgcd}(m, n) = 1$.
8. On note μ_0 l'ordre de m et ν_0 l'ordre de c. Montrer que $c^{\mu_0} \equiv 1 \mod n$ et $m^{\nu_0} \equiv 1 \mod n$. En utilisant la question (4) de la partie I, montrer que $\nu_0 = \mu_0$.
9. Montrer que $e^k - 1$ est un multiple de μ_0.
10. Montrer que $d' = e^{k-1}$ est l'inverse de e modulo $e^k - 1$.
11. Montrer que $m^{d'e} \equiv m \mod n$ (on pourra écrire $d'e = (e^k - 1) + 1$).
12. En déduire que Eve peut déchiffrer le message.
13. Application :
    La clé publique de Bruno est $(527, 3)$. Eve intercepte le message $c = 15$ et calcule

$$c^{e^2} \mod n = 525,$$
$$c^{e^3} \mod n = 519,$$
$$c^{e^4} \mod n = 15.$$

    Déchiffrer le message.