Université de Lille 1 SCIENCES ET TECHNOLOGIES

L1 - SESI - 2014–2015

Arithmétique et Cryptographie

DS2 – Durée 2h
19 mai 2015

Toutes les réponses doivent être justifiées et vous soignerez votre rédaction. Le barème est indicatif.

Les documents et appareils électroniques (calculatrices, téléphones portables, etc. . .) sont interdits.

Notez le numéro de votre groupe sur la copie.

1 Lemme chinois (4pts)

Dans cet exercice p et q sont deux entiers premiers entre eux.

1. Montrez que si $a \in \mathbb{Z}$ vérifie les deux équations :
$$\begin{cases} a & \equiv & 0 \pmod{p} \\ a & \equiv & 0 \pmod{q} \end{cases}$$
alors $a \equiv 0 \pmod{pq}$.
2. En déduire le *lemme chinois* : si $b \in \mathbb{Z}$ vérifie les deux équations
$$\begin{cases} b & \equiv & 1 \pmod{p} \\ b & \equiv & 1 \pmod{q} \end{cases}$$
alors $b \equiv 1 \pmod{pq}$.
3. Alice veut transmettre à ses deux filles un nombre secret a, qui nécessite qu'elles s'unissent pour le découvrir. Pour cela,
   — elle choisit deux nombres premiers entre eux p et q tels que $a < pq$,
   — elle calcule $a_p = a \pmod{p}$ et $a_q = a \pmod{q}$,
   — et elle transmet le couple (p, a_p) à Barbara, et (q, a_q) à Bérénice.
   Barbara reçoit $p = 7$ et $a_p = 6$. Bérénice reçoit $q = 13$ et $a_q = 3$. Quel est le nombre secret a ?

2 Autour de Fermat (4pts)

1. Énoncez le petit théorème de Fermat « classique » dans le cas d'un entier $a \in \mathbb{Z}$ et d'un nombre premier p tel que p ne divise pas a.
2. Prouvez le petit théorème de Fermat « amélioré » :
   Théorème : Pour $a \in \mathbb{Z}$, pour p, q deux nombres premiers distincts tels que p et q ne divisent pas a et en posant $n = p \times q$, alors
   $$a^{(p-1)(q-1)} \equiv 1 \pmod{n}$$
   Indications. Vous appliquerez deux fois le petit théorème de Fermat « classique » et le lemme chinois du premier exercice.
3. Application : Calculez 3^{63} modulo 77 en détaillant les étapes de calcul.

3 Remise de notes avec RSA (7pts)

3.1 DS1 : chiffrement simple

Les notes du DS1 du module d'Arithmétique et Cryptographie étaient transmises par les enseignants au secrétariat en utilisant le protocole RSA tel que vu en cours.

La clé publique du secrétariat (n_S, e_S) est $(33, 3)$.

1. L'enseignant veut transmettre la note $m = 10$ au secrétariat. Quel nombre chiffré x doit-il envoyer au secrétariat ?
2. Quelle est la clé privée d_S du secrétariat ? Détaillez les étapes du calcul.
3. Un étudiant tricheur a voulu frauder et a envoyé le message chiffré suivant $x_{triche} = 28$ au secrétariat. Calculez la note déchiffrée m_{triche} en appliquant l'algorithme d'exponentiation rapide et en détaillant les calculs.

3.2 DS2 : signature

Le secrétariat ne pouvant pas différencier les notes venant des enseignants de celles envoyées par l'étudiant tricheur, il a été décidé d'utiliser le protocole d'authentification suivant pour l'envoi des notes du DS2 :

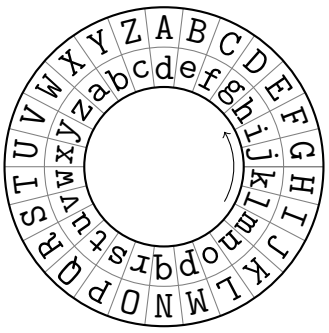
(1) L'enseignant génére sa clé publique (n_E, e_E) et sa clé privée (d_E) suivant le protocole RSA, et publie sa clé publique.
(2) Le secrétariat génére sa clé publique (n_S, e_S) et sa clé privée (d_S) suivant le protocole RSA, et publie sa clé publique.
(3) L'enseignant veut envoyer la note m au secrétariat.
(4) L'enseignant chiffre la note avec la clé publique du secrétariat en calculant $c \equiv m^{e_S} \pmod{n_S}$.
(5) L'enseignant *signe* la note avec sa clé privée en calculant $s \equiv m^{d_E} \pmod{n_E}$.
(6) L'enseignant envoie le couple (c, s) au secrétariat.
(7) Le secrétariat calcule $m_1 \equiv c^{d_S} \pmod{n_S}$.
(8) Le secrétariat calcule enfin $m_2 \equiv s^{e_E} \pmod{n_E}$.

La clé publique du secrétariat (n_S, e_S) reste $(33, 3)$. La clé privée de l'enseignant (n_E, e_E) est $(21, 5)$.

1. En citant les théorèmes utilisés, montrez que $m_1 = m_2 = m$.
2. Vérifiez que la clé privée de l'enseignant est $d_E = 5$.
3. L'enseignant veut transmettre la note $m = 11$ au secrétariat. Quel couple (c, s) doit-il envoyer ?
4. Expliquez pourquoi ce nouveau protocole permet d'empêcher le tricheur d'usurper l'identité de l'enseignant.

4 Enigma (5pts)

On considère une machine Enigma simplifiée à une seule roue. L'anneau fixe est composé des lettres `A`, `B`, `C`, `D`, ... L'anneau mobile est aussi composé des lettres `a`, `b`, `c`, `d`, ...



Dans la configuration donnée par la figure, la lettre claire `A` est chiffrée `d`, et l'anneau mobile tourne d'un cran dans le sens trigonométrique (contraire à celui des aiguilles d'une montre). Ainsi, si on doit chiffrer à nouveau la lettre `A`, on obtient `e`.

1. Si en position initiale la lettre `a` de l'anneau mobile est en face de la lettre `A` de l'anneau fixe, quel est le chiffrement de `BABA` ?
2. Repartant de la position initiale où la lettre `a` de l'anneau mobile est en face de la lettre `A` de l'anneau fixe, quel mot a été chiffré en `fbeh` ?
3. Toujours en repartant de la position initiale `a` en face de `A` et avec la correspondance `A` et `a` valent '0', `B` et `b` valent '1', `C` et `c` valent '2' ..., on chiffre un message $(x_0, x_1, x_2, \ldots, x_i, \ldots)$ où $x_i \in \mathbb{Z}/26\mathbb{Z}$. Si f désigne la fonction de chiffrement, que vaut $f(x_i)$? (C'est une expression simple qui dépend de x_i et du rang i.) Donnez l'expression de la fonction de déchiffrement.
4. Maintenant la position initiale de l'anneau mobile est décalée de d lettres (par exemple si $d = 2$ le `A` fixe est en face du `c` mobile). Donnez la nouvelle expression pour $f(x_i)$.
5. Ne connaissant pas le décalage initial d, expliquez une méthode d'attaque de ce système de chiffrement.