Université de Lille — FACULTÉ DES SCIENCES ET TECHNOLOGIES

L1 - SESI - 2017–2018

Mathématiques Informatique
Arithmétique et Cryptographie

DS2 – 17 mai 2018
Durée 2h

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

Les documents et appareils électroniques (calculatrices, téléphones, ordinateurs portables, etc...) ne sont pas autorisés.

Notez le numéro de votre groupe sur la copie.

Exercice 1 (3 points)

Dans cet exercice, l'alphabet utilisé est l'alphabet latin usuel (`ABC...XYZ`).

Décrypter le message suivant obtenu par un chiffrement de Vigenère à l'aide d'une clé de longueur 3, (p, q, r) où p, q, r sont trois nombres premiers consécutifs (les caractères espaces ne sont pas chiffrés) :

```
QP FLCF SL FJTRUNR LE P LDG TL WVTR
```

Exercice 2 (4 points)

On souhaite résoudre le système de congruence :

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

où m, n sont deux nombres premiers entre eux, a, b sont des entiers fixés et x est l'inconnue entière.

1. 1. Donner la définition de « u est inversible modulo n ».
   2. Donner une condition nécessaire et suffisante afin que l'inverse de u modulo n existe.
   3. *Exemple.* Trouver (à la main) l'inverse de 9 modulo 16. Puis l'inverse de 16 modulo 9.
2. 1. Soit $\tilde{m}$ un inverse de m modulo n et soit $x_1 = \tilde{m}m$. Montrer que x_1 est solution du système :

$$\begin{cases} x \equiv 1 \pmod{n} \\ x \equiv 0 \pmod{m} \end{cases}$$

   2. Trouver comment obtenir une solution x_2 du système :

$$\begin{cases} x \equiv 0 \pmod{n} \\ x \equiv 1 \pmod{m} \end{cases}$$

   3. En déduire que $x = ax_1 + bx_2$ est solution du système initial.
   4. *Exemple.* Trouver une solution $0 \leq x < 9 \times 16$ au système suivant :

$$\begin{cases} x \equiv 2 \pmod{9} \\ x \equiv 3 \pmod{16} \end{cases}$$

Exercice 3 (4 points)

On fixe des entiers naturels a, b, n. On choisit un entier x_0. Et pour tout entier $k > 0$, on définit la suite d'entiers suivante par la relation de récurrence [1] :

$$x_{k+1} = ax_k + b \pmod{n}.$$

Dans la suite tous les calculs sont effectués modulo n.

1. *Exemple.* Pour $a = 2$, $b = 3$, $n = 50$, et $x_0 = 10$, calculer les termes x_1, x_2, x_3, x_4.
2. On repart avec a et b quelconques, mais on connaît n. Supposons que l'on connaisse aussi trois termes consécutifs x_k, x_{k+1} et x_{k+2} et qu'en plus $x_{k+1} - x_k$ soit inversible modulo n.
   — Exprimer x_{k+2} en fonction de a, b, x_{k+1}.
   — Exprimer x_{k+1} en fonction de a, b, x_k.
   — En déduire $x_{k+2} - x_{k+1}$.
   — Exprimer a en fonction de x_k, x_{k+1}, x_{k+2} et l'inverse de $x_{k+1} - x_k$.
   — En déduire b (en fonction de a, x_k, x_{k+1}).
3. Trouver une solution de l'équation $53x + 100y = 1$, (donner les détails des calculs). En déduire l'inverse de 53 modulo 100.
4. Pour $x_k = 15$ et $x_{k+1} = 68$, $x_{k+2} = 51$ et $n = 100$, trouver les valeurs de a et b.

Exercice 4 (5 points)

Voici les données pour définir les clés d'un chiffrement par le système RSA :

$$p = 7, \qquad q = 13, \qquad e = 5, \qquad d = 29$$

1. Faire un schéma de principe du chiffrement à clé publique (et de RSA en particulier).
2. Quelle est la clé publique ? Vérifier que la clé publique est valide.
3. Quelle est la clé privée ? Vérifier que la clé privée convient.
4. Quelle est la fonction de chiffrement ? Chiffrer le message $x = 4$.
5. Quelle est la fonction de déchiffrement ? Déchiffrer le message $y = 2$.

Exercice 5 (4 points)

Pour obtenir le résultat d'une opération modulo n, il faut souvent effectuer une division euclidienne par n. Nous allons voir que pour certains n, on peut s'en passer, ce qui facilite les calculs.

1. **Cas $n = 10^k$, $k \in \mathbb{N}$.**
   Montrer que si on connaît l'écriture décimale d'un entier u alors il facile de trouver le reste de la division de u par n. (On pourra noter u_0 le chiffre des unités, u_1 celui des dizaines,...)
   Exemple. Avec $u = 9876543210$ et $n = 10^4$, trouver le reste de la division de u par n.
2. **Cas $n = 10^k - 1$, avec $k = 4$ ($n = 10^4 - 1 = 9999$).**
   1. Soit u un entier ayant 4 chiffres en écriture décimale. On l'écrit sous la forme

      $$u = 100a + b \qquad \text{avec } 0 \leq a, b < 100.$$

      Trouver une façon simple de calculer le reste de $100u$ modulo $n = 9999$.
      Exemple. Avec $u = 1789$, on a $a = 17$, $b = 89$. Combien vaut $100u$ modulo 9999 ?
   2. Soient u et v deux entiers ayant 4 chiffres : $u = 100a + b$, $v = 100c + d$, avec $0 \leq a, b, c, d < 100$.
      Trouver une façon de calculer $u \times v$ modulo $n = 9999$, sans division euclidienne, sous forme d'une somme de quatre nombres inférieurs à $n = 9999$.

1. De nombreux générateurs de nombres pseudo-aléatoires sont construits sur la base de ce type de suite de nombres.