

# TD Théorie de l'information

## Diffie-Hellman

**Exo 1** Ecrire un algorithme non-récurif qui, pour trois entiers  $g$ ,  $x$  et  $n$  saisis par l'utilisateur, calcule  $g^x \pmod n$ . Modifier l'algorithme pour qu'il utilise la représentation en base deux de  $x$ .

**Exo 2** Pour  $p$  un nombre premier  $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \dots, p-1\}$  est un groupe avec la multiplication. Pour  $\mathbb{F}_7^* = \{1, 2, 3, 4, 5, 6\}$

1. Donner la table de multiplication,
2. Résoudre les équations :  $2 \cdot x = 2$ ;  $5 \cdot x = 2$ ;  $6 \cdot x = 1$
3. Calculer  $g^x \pmod 7$  pour  $g, x \in \{1, 2, 3, 4, 5, 6\}$ .
4. Quelles sont les générateurs de  $\mathbb{F}_7^*$  ?
5. Calculer  $\log_5 2$ ,  $\log_5 3$ ,  $\log_3 6$ .
6. L'indicateur d'Euler  $\varphi$  est la fonction qui à  $n$  associe le nombre d'entiers strictement positifs inférieurs ou égaux à  $n$  et premiers avec  $n$ . Par exemple,  $\varphi(8) = 4$ . Vérifier pour  $\mathbb{F}_7^*$  que : le nombre de générateurs de  $\mathbb{F}_p^*$  est  $\varphi(p-1)$ ;
7. Alice et Bob veulent appliquer le protocole de Diffie-Hellman. Ils choisissent en commun  $p = 7$  et  $g = 5$ . Choisir des clés secrètes  $a$  (pour Alice) et  $b$  (pour Bob) et appliquer le protocole avec ces deux valeurs.

### Exo 3

1. 2 est un générateur de  $\mathbb{F}_{11}^*$  ?
2. 3 est un générateur de  $\mathbb{F}_{11}^*$  ?
3. combien de générateurs possède  $\mathbb{F}_{11}^*$  ?
4. en  $\mathbb{F}_{11}^*$  calculer  $\log_2 10$  (solution de l'équation  $2^x = 10$ ) et  $\log_8 2$  (solution de l'équation  $8^x = 2$ ).
5. L'algorithme suivant teste si  $a$  est un générateur de  $\mathbb{F}_p^*$ .

```
teste générateur
entrées : un entier premier p, un entier a
sortie : OUI, si a est un générateur de  $\mathbb{F}_p^*$ , NON sinon
pour tout q, premier et divisant p-1 faire
    si  $a^{\frac{p-1}{q}} = 1 \pmod p$ 
        alors renvoyer NON
    fin si
fin pour
renvoyer OUI
end procedure.
```

Appliquer ce teste pour répondre aux points 1. et 2.

### Exo 4

1. Montrer que 5 est un générateur de  $\mathbb{F}_{17}^*$ .
2. Montrer que 4 n'est pas un générateur de  $\mathbb{F}_{17}^*$ . En déduire la valeur de  $4^n \pmod{17}$  pour tout entier  $n$ .
3. Alice et Bob veulent appliquer le protocole de Diffie-Hellman. Ils choisissent en commun  $g = 5$  et  $p = 17$ . Choisir des clés secrètes  $a$  (pour Alice) et  $b$  (pour Bob) et appliquer le protocole avec ces deux valeurs.

## RSA

**Exo 5** Soit  $p = 3$  et  $q = 5$  deux nombres premiers et  $n = p \cdot q = 15$ .

1. Pour chaque  $e$ ,  $1 < e < (p - 1) \cdot (q - 1) = 8$ , premier avec  $(p - 1) \cdot (q - 1) = 8$  trouver un  $d$  tel que  $e \cdot d = 1 \pmod{(p - 1) \cdot (q - 1)}$ .
2. Pour chaque couple  $(e, d)$  trouver au point 1. et  $x \in \{2, 3, 4, 5\}$  vérifier que  $x^{e \cdot d} = x \pmod{n}$ .
3. Décrire le protocole RSA avec
  - (a) les données privées d'Alice :  $p = 3$ ,  $q = 5$ ,
  - (b) la clé publique :  $(n, e) = (15, 3)$

**Exo 6** Décrire le protocole RSA avec les données privées d'Alice :  $p = 3$  et  $q = 7$ .

## Protocole de partage de clé secrète de Shamir

**Exo 7** Soit  $P : \mathbb{R} \rightarrow \mathbb{R}$  le polynôme de degré minimale qui passe par les points de contrôle  $(-1, 1)$ ,  $(1, 3)$  et  $(-2, 3)$ .

- Calculer  $P(0)$ ,
- Donner le polynôme  $P$ .

**Exo 8** Résoudre les équations suivantes en  $\mathbb{Z}/5\mathbb{Z}$  :  $4x = 2$ ,  $2x + 3 = 1$ ,  $3x + 1 = 2x + 4$ .

**Exo 9** Soit  $Q : \mathbb{Z}/11\mathbb{Z} \rightarrow \mathbb{Z}/11\mathbb{Z}$ ,  $Q(x) = 2x + 3$ . Donner le secret et cinq parts du secret :

$$p_1 = Q(1), p_2 = Q(2), p_3 = Q(3), p_4 = Q(4), p_5 = Q(5).$$

**Exo 10** Une famille de quatre personnes décide de garder leur fortune dans un coffre fort électronique; chaque personne a son propre code (part du secret). Le coffre s'ouvre si trois de ces quatre codes sont saisis. Les codes sont :

$$p_1 : 3; p_2 : 1; p_3 : 1; p_4 : 3.$$

Soit  $R : \mathbb{Z}/5\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z}$  le polynôme correspondant à ce protocole.

- Donner  $R(0)$  (le secret),
- Donner  $R$ ,
- Tracer la graphique de la fonction  $R$ .

**Exo 11** Proposer un code détecteur et correcteur d'erreurs basé sur le polynôme de l'exo. 4.