**Feuille d'exercices 3.**

**Exercice 1 (Calcul rapide des puissances)** Soit $a$ un entier positif.
1) Quel est le nombre minimal de multiplications nécessaires pour élever $a$ à la puissance $2^i$?
2) Le calcul de la puissance $a^n$ peut être accéléré comme suit:

- on décompose $n$ en base 2: $n = b_k b_{k-1}...b_0$.
- on effectue le produit des $a^{2i}$ correspondant aux $b_i$ valant $i$.

Donner le détail des calculs effectués par cette méthode pour calculer $3^{19}$.
3) Adapter ce qui précède aux calculs des puissances modulo $q$.

**Exercice 2 (Logarithme discret)** Soit $\alpha$ un élément primitif de $(\mathbb{Z}/p\mathbb{Z})^*$ s'écrit donc $a = \alpha^k$.
Le nombre $k$ est le logarithme discret de $a$ à base $\alpha$.
1) Classer tous les éléments de $(\mathbb{Z}/19\mathbb{Z})^*$ suivant leur ordre.
2) Trouver un élément primitif $\alpha$ de $(\mathbb{Z}/19\mathbb{Z})^*$ ainsi que les logarithmes discrets à base $\alpha$ de tous les éléments de $(\mathbb{Z}/19\mathbb{Z})^*$.

**Exercice 3 (Pas de bébé, pas de géant)** Soit $g$ une racine primitive du corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Le problème du logarithme discret consiste à exprimer un élément $\beta \in \mathbb{F}_p$ sous la forme $\beta = g^x$. Shanks a proposé un algorithme basé sur l'observation suivante: soit $m = \lceil \sqrt{p-1} \rceil$, la division euclidienne de $x$ par $m$ donne $x = mi + j$ avec $0 \leq i, j < m$ et on a:

$$\beta g^{-mi} = g^j \bmod p$$

1) Expliquer pourquoi on a $i < m$.
D'où, l'algorithme:

- 1: $m \leftarrow \lceil \sqrt{p-1} \rceil$
- 2: Calculer $g^j$ pour $0 \leq j < m$
- 3: Trier les couples $(j, g^j \bmod p)$ suivant leur deuxième coordonnée; soit $L_1$ la liste obtenue.
- 4: $g_1 \leftarrow g^{-m}$, $\gamma \leftarrow \beta$
- 5: Pour $i$ de 0 à $m-1$,
  - Tester si $\gamma \in L_1$,
  - Si oui, retourner $x = mi + j$,
  - $\gamma \leftarrow \gamma \times g_1$

On considère le groupe multiplicatif de $\mathbb{F}_{113}$. On prendra $g = 3$.
2) Expliquer intuitivement le fonctionnement de cet algorithme.
3) Donner la complexité de l'algorithme. Est-ce polynomial, exponentiel, sous-exponentiel?
4) Utiliser l'algorithme de Shanks pour calculer $log_3(111)$.

**Exercice 4 (Diffie-Hellman)**
1) Vérifier que $g = 2$ est un générateur du groupe multiplicatif $\mathbb{F}_{11}^*$.
2) Quel est le secret commun (clé commune) qu'établissent Alice et Bob en utilisant le protocole de Diffie-Hellman avec $p = 11$ et $g = 2$ si les nombres aléatoires qu'ils ont choisis sont $x_A = 7$ et $x_B = 8$?

**Exercice 5 (ElGamal dans $\mathbb{Z}/p\mathbb{Z}$)** Alice reçoit le cryptogramme ElGamal $(30, 7)$. Sa clé publique est $(p = 43, g = 3)$. Déterminer le message en clair correspondant.

**Exercice 6 (ElGamal, partiel 2007)**
On note 0,1,2 les éléments du corps $\mathbb{F}_3$. Le polynôme $Q = X^3 + 2X^2 + 1$ est irréductible sur $\mathbb{F}_3$, ce qui permet d'identifier le corps fini $\mathbb{F}_{27}$ au quotient $\mathbb{F}_3[X]/(Q)$ de l'anneau de polynômes par l'idéal engendré par $Q$. On note $x$ la classe de $X$ dans ce quotient. On rappelle que $\mathbb{F}_{27} \simeq \mathbb{F}_3[x]$: tout élément de $\mathbb{F}_{27}$ s'écrit de manière unique comme un polynôme de degré inférieur ou égal à 2 en $x$ et les multiplications dans ce corps se font modulo $Q$. Vous devez déchiffrer le message $(K, H)$ $(P, X)$ $(N, K)$ $(H, R)$ $(T, F)$ $(V, Y)$, où chaque couple de ce cryptogramme cache une lettre à trouver.

Le message en clair a été chiffré en utilisant un chiffrement d'ElGamal sur le corps fini $\mathbb{F}_{27}$, votre clé secrète de déchiffrement est l'entier $a = 11$, la clé publique de chiffrement est $(x + 2)$ et les 26 lettres de l'alphabet sont en correspondance avec les 26 éléments non nuls du corps, de la manière suivante:

| | | |
|---|---|---|
| $A = 1$ | $B = 2$ | $C = x$ |
| $D = x + 1$ | $E = x + 2$ | $F = 2x$ |
| $G = 2x + 1$ | $H = 2x + 2$ | $I = x^2$ |
| $J = x^2 + 1$ | $K = x^2 + 2$ | $L = x^2 + x$ |
| $M = x^2 + x + 1$ | $N = x^2 + x + 2$ | $O = x^2 + 2x$ |
| $P = x^2 + 2x + 1$ | $Q = x^2 + 2x + 2$ | $R = 2x^2$ |
| $S = 2x^2 + 1$ | $T = 2x^2 + 2$ | $U = 2x^2 + x$ |
| $V = 2x^2 + x + 1$ | $W = 2x^2 + x + 2$ | $X = 2x^2 + 2x$ |
| $Y = 2x^2 + 2x + 1$ | $Z = 2x^2 + 2x + 2$ | |

1) Vérifier rapidement que $x^{11} = x + 2$.
2) Exprimer $x^{12}$ et $x^{13}$ comme des polynômes de degré inférieur ou égal à 2 en $x$.
En déduire que $x$ engendre le groupe multiplicatif $\mathbb{F}_{27}^*$.
3) Expliquer pourquoi, pour trouver l'inverse de $(x^2 + 2)^{11}$, on peut calculer $(x^2 + 2)^{15}$.
4) Vérifier, à l'aide de calculs déjà effectués, que $(2x + 2)(x^2 + 2)^{15} = 2x + 1$.
5) Décrire le système de chiffrement d'El Gamal et le déchiffrement que vous devez appliquer, pour justifier que la première lettre du message en clair cherché est un $g$.
6) Sachant de plus que $x^{14} = 2x$, $x^{16} = 2x^2 + 1$, $x^{19} = x^2 + x$, $x^{21} = 2x^2 + 2x + 1$, déchiffrer les cinq lettres suivantes et donner le mot de six lettres que vous avez trouvé.
7) Donner une estimation du coût d'une addition, puis d'une multiplication, dans un corps fini $\mathbb{F}_q$, où $q = p^n$.

**Exercice 7 (ElGamal avec ordre composé)**
On considère le système de chiffrement ElGamal dans un groupe cyclique $\langle g \rangle$ d'ordre $2q$, où $q$ est un nombre premier. On va démontrer que la sécurité sémantique n'est pas vérifiée. On note $y = g^x$ la relation entre clé publique et clé secrète.
1) Quelle est la valeur de $g^q$?
2) Soit $(u, v) = (g^r, y^r m)$ le chiffrement d'un message $m$. Montrer comment le calcul de $u^2$ permet de connaître le bit de poids faible (la parité) de $r$.
3) En connaissant la parité de $r$ déduire une attaque à clair choisi contre la sécurité sémantique.

**Exercice 8** Soient $p$ et $q$ deux nombres premiers distincts tels que

$$p = 2 \bmod 3 \text{ et } q = 2 \bmod 3$$

1) Montrer que $2(p - 1)(q - 1) + 1$ est divisible par 3.
2) On pose $k = \phi(pq)$. Calculer l'inverse $d$ dans $\mathbb{Z}/k\mathbb{Z}$ de

$$e = \frac{2(p-1)(q-1)+1}{3}$$

3) Soit $p = 17$ et $q = 11$. On pose $n = pq$. Alice et Bob communiquent en utilisant l'algorithme RSA. La clé publique de Bob est $(107, n)$. Quelle est sa clé secrète?
Alice veut transmettre le message $M$ à Bob, Bob reçoit $C = 9$.
Quel était le message $M$ envoyé par Alice?

**Exercice 9 (Attaque de RSA par diffusion de messages sur un même exposant $e$ petit)**
Supposons que Alice souhaite envoyer le même message $m \in A$ à Bob (dont le module est $N_1 = 55$), Eve ($N_2 = 51$) et David ($N_3 = 46$) qui partagent tous les trois le même $e = 3$. Elle envoie donc:

$$\begin{cases} 25 &= m^3 \bmod N_1 \\ 44 &= m^3 \bmod N_2 \\ 42 &= m^3 \bmod N_3 \end{cases}$$

Résoudre le système de congruence:

$$\begin{cases} x &= 25 \bmod N_1 \\ x &= 44 \bmod N_2 \\ x &= 42 \bmod N_3 \end{cases}$$

En déduire le message $m$ initialement envoyé.

**Exercice 10 (Attaque sur RSA par module commun)**
Un phase coûteuse en calcul est la recherche des (bons) nombres premiers $p$ et $q$. Fort de cette remarque, vous décidez que tous les employés de votre entreprise partageront le même module $n = pq$, seul l'exposant de chiffrement $e$, et donc celui de déchiffrement $d$ sera spécifique à chacun d'entre eux.

Vous envoyez un message $M \in \mathbb{Z}/n\mathbb{Z}$ à deux de vos employés à l'aide de leur clé publique $e_1$ et $e_2$. Les messages chiffrés correspondants sont $C_1$ et $C_2$. On peut supposer que $e_1$ et $e_2$ sont premiers entre eux (il est très probable qu'ils le soient).

Edmond, l'espion, interceptant $C_1$ et $C_2$ et connaissant $n$, $e_1$ et $e_2$ peut faire les calculs suivants:

$$\begin{array}{rcl} b_1 & \leftarrow & e_1^{-1} \bmod e_2 \\ b_2 & \leftarrow & (b_1 e_1 - 1) e_2^{-1} \\ X & \leftarrow & C_1^{b_1} (C_2^{b_2})^{-1} \bmod n \end{array}$$

A quoi mènent les calculs d'Edmond? Quelle est leur complexité?

**Exercice 11 (RSA avec deux facteurs trop proches)**
Supposons que $n$ soit un entier produit de deux nombres premiers $p$ et $q$ proches (on peut toujours supposer que $p > q$). On pose $t = \frac{p+q}{2}$ et $s = \frac{p-q}{2}$. Montrer que:
1) $n = t^2 - s^2$,
2) $t$ est légèrement supérieur à la racine carrée de $n$,
3) $s$ est petit,
4) On peut utiliser ces informations pour factoriser $n$ (l'algorithme s'appelle algorithme de Fermat),
5) Comment appliquer cet algorithme pour factoriser 24960007, puis 3649574023?
6) Déterminer la complexité de l'algorithme en fonction de $s$ ou $p$, et $n$.
7) Déterminer le nombre d'itérations de l'algorithme lorsque $p$ diffère de $\sqrt{n}$ de moins de $(4n)^{1/4}$.

**Exercice 12 (Attaque $p-1$ sur RSA)**
Cette attaque est très performante lorsque $p$ (un des facteurs du module $N = pq$) possède une propriété particulière: soit $B$ un entier arbitraire (qu'on choisira petit); on dit qu'un nombre est $B$-lisse si tous ses diviseurs premiers sont inférieurs ou égaux à $B$.
1) Montrer que l'ensemble des nombres $B$-lisses est stable par multiplication.

L'attaque dite $p-1$ fonctionne si $p-1$ est $B$-lisse (pour un $B$ quelconque que l'on supposera connu). Elle se base sur le théorème de Fermat et le calcul de pgcd.
2) Rappeler comment s'écrit le petit théorème de Fermat dans $\mathbb{Z}/p\mathbb{Z}$.
3) En déduire que pour tout $a$ premier avec $p$, et tout entier $k$ multiple de $p-1$, on a $pgcd(a^k - 1, N) \neq 1$.
4) Expliquer comment construire simplement un (grand) multiple de $p-1$, en utilisant la $B$-lissité. (Rappel: la valeur de $p$ est inconnue)
5) Conclure.