UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Feuille n°8 : Chiffrements

Exercice 1

	Alice				*Bob*	
Secret	*Public*	*Calcul*		*Calcul*	*Public*	*Secret*
	p, g				p, g	
a						b
		$g^a[modp]$	$\rightarrow$		$\cdots$	
	$\cdots$		$\leftarrow$	$g^b[modp]$		
	$(g^b)^a[modp]$		$=$		$(g^a)^b[modp]$	

1 Alice et Bob choisissent un nombre premier $p = 23$ et une base $g = 3$. Alice choisit un nombre secret $a = 6$. Elle envoie à Bob la valeur $g^a[modp]$. Calculer cette valeur.
2 Bob choisit à son tour un nombre secret $b = 15$. Bob envoie à Alice la valeur $g^b[modp]$. Calculer cette valeur.
3 Calculer la clé secrète comme Alice.
4 Calculer la clé secrète comme Bob.

Exercice 2

1 Alice et Bob choisissent un polynôme $P = X^3 + 2X + 1$ de $\mathbb{F}_3[X]$ et considère l''anneau quotient $k = \mathbb{F}_3[X]/ < P >$. Est-ce un corps ? Quel est son cardinal q ?
2 Montrer que le polynôme P divise $X(X-1)^4+1$ dans $\mathbb{F}_3[X]$. Montrer que $\alpha^{13} = \alpha(\alpha-1)^4$. Calculer la valeur de α^{13} et montrer que α est un générateur de $k^\times$.
3 Alice choisit un nombre secret $a = 6$. Elle envoie à Bob la valeur α^a. Calculer cette valeur.
4 Bob choisit à son tour un nombre secret $b = 15$. Bob envoie à Alice la valeur α^b. Calculer cette valeur.
5 Calculer la clé secrète comme Alice.
6 Calculer la clé secrète comme Bob.

Exercice 3

Alice et Bob choisissent un polynôme $P = X^3 + 2X + 1$ de $\mathbb{F}_3[X]$ et considère l''anneau quotient $k = \mathbb{F}_3[X]/ < P >$. On admet que α est un générateur de $k^\times$.
1 Alice choisit un nombre secret $a = 9$. Bernard choisit b et envoie $\alpha^b = 2 + \alpha + 2\alpha^2$. Quelle est la clé secrète commune c ?
2 Ils décident de chiffrer tout message m par le message $M := cm$. Alice souhaite envoyer $m = 2 + \alpha^2$. Quel message chiffré envoie-t-elle ?
3 Alice reçoit le message chiffré 2α ? Quel était le message de Bernard ?

Exercice 4

Alice et Bernard décident d'utiliser l'algorithme d'El Gamal. Il utilise le corps $\mathbb{F}_{19}$ avec l'élément $G = 3$.

1 Déterminer l'ordre de 3 dans $\mathbb{F}_{19}^{\times}$.

2 Bernard choisit sa clé privée $c = 4$. Déterminer sa clé publique $C = G^c$.

3 Alice choisit une clé temporaire privée $d = 5$. Quelle est sa clé publique D ? Elle souhaite envoyer le message $m = 17$. Elle le chiffre en utilisant la clé publique C de Bernard par $(M_1, M_2) = (D, mC^d)$. Expliciter ce message chiffré.

4 Comment Bernard retrouve-t-il le message m ?

5 Dans un second envoi, Bernard reçoit $(8, 3)$. Quel est le message m envoyé cette fois par Alice ? Quelle clé privée a-t-elle utilisé cette fois ?

Exercice 5

Alice et Bernard décident d'utiliser l'algorithme d'El Gamal, choisissent le polynôme $P = X^4 + X + 1$ de $\mathbb{F}_2[X]$ et considère l''anneau quotient $k = \mathbb{F}_2[X]/ < P >$. On admet que α est un générateur de $k^{\times}$. La clé publique de Bernard est $C = 1 + \alpha^2$.

1 Alice veut envoyer le message $m = 1 + \alpha$ avec sa clé privée $d = 3$. Quel est son message chiffré ?

2 Quelle est la clé secrète de Bernard ?

3 On intercepte le message chiffré $(\alpha^3, \alpha + \alpha^2 + \alpha^3)$. Quel est le message initial ?