ENSIBS
2022/2023

Mathématiques pour la cryptographie
S6- CyberLog

Contrôle : vendredi 17 février

Durée : 1h et 20 minutes.

Les réponses devront toujours être justifiées. Les documents, les ordinateurs et les autres appareils électroniques sont interdits

---

Exercice 1.

(1) À quoi sert le protocole de Diffie-Hellman ?

(2) Expliquer à l'aide d'un schéma ce protocole.

(3) Que se passe-t-il si le canal de communication est compromis et qu'un observateur malveillant (Eve) écoute les communications ? Comment est-ce que Eve pourrait trouver le résultat partagé par Alice et Bob ?

(4) Pouvez-vous généraliser ce protocole d'échange pour trois personnes ?

(5) Comment définir et calculer l'ordre d'une courbe elliptique sur un corps fini sur SageMath ?

Exercice 2. Considérons la courbe elliptique E sur le corps $\mathbb{F}_7$ d'équation

$$E : y^2 = x^3 + 2x + 4.$$

(1) Déterminer tous les points de cette courbe. Quel est l'ordre du groupe $E(\mathbb{F}_7)$?

(2) Pour chaque point $P \in E(\mathbb{F}_7)$, déterminer son symétrique.

Alice et Bob utilisent le protocole d'échange de clé de Diffie-Hellman sur la courbe $E(\mathbb{F}_7)$ et le générateur $P = (0, 2)$. Alice choisit $a = 4$ comme clé secrète et Bob choisit $b = 3$.

(3) Calculer les messages aP et bP de l'échange de clés et de leur clé commune.

Exercice 3. Pour qu'Alice puisse envoyer un message secret M à Bob en utilisant le système du chiffrement El Gamal, ils peuvent procéder comme suit :

— Bob commence par générer sa clé publique en choisissant un nombre premier p et un élément g du groupe $(\mathbb{F}_p^*, \times)$.

— Bob choisit ensuite un nombre b secret et calcule $B = g^b \pmod p$.

— Bob publie sa clé publique (p, g, B).

— Pour envoyer le message M, Alice choisit un nombre a secret et envoie $(c_1, c_2) = (g^a, MB^a)$ modulo p à Bob.

— À la réception de (c_1, c_2), Bob calcule $c_2(c_1^b)^{-1}$ et obtient M.

(1) Expliquer pourquoi cela fonctionne.

Supposons que la clé publique de Bob est $(p, g, B) = (47, 5, 3)$ et que $c_1 = 17$.

(2) Trouver les clés secrètes a et b.

(3) Calculer c_1^b, puis déterminer son inverse dans $(\mathbb{F}_{47}^*, \times)$.

Pour chiffrer un mot, Alice le transforme en séquences de nombre à l'aide de la table ci-après, puis elle chiffre chaque nombre associé.

Lettre à coder	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Nombre associé	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Lettre à coder	O	P	Q	R	S	T	U	V	W	X	Y	Z
Nombre associé	34	35	36	37	38	39	40	41	42	43	44	45

(4) Alice envoie à Bob la séquence

$$(17, 18),\ (17, 29),\ (17, 41),\ (17, 29),\ (17, 9),\ (17, 31).$$

Quel est le message en clair d'Alice ?