

TD5 — Chiffrement à clé publique

Comme au contrôle terminal, il est recommandé de se munir d'une calculatrice pour traiter certains de ces exercices.

Ex1. Protocole de Diffie-Hellman On se place dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ des entiers modulo n inversibles pour la multiplication modulo n . Son cardinal est noté $\varphi(n)$, l'indicatrice d'Euler de n . On fixe un générateur $g \in (\mathbb{Z}/n\mathbb{Z})^*$, c'est-à-dire un élément tel que tout $y \in (\mathbb{Z}/n\mathbb{Z})^*$ peut s'exprimer comme une puissance $0 \leq x < \varphi(n)$ de g , c'est-à-dire vérifiant $g^x = y \pmod{n}$. Alice et Bob échangent suivant le protocole DH avec $n = 199$ et $g = 97$.

- (a) Donner une condition nécessaire et suffisante pour qu'un entier k soit inversible modulo n . Comment calcule-t-on son inverse ?
- (b) Rappeler le principe du protocole DH.
- (c) Alice choisit $a = 71$. Calculer la valeur qu'elle envoie à Bob. Sachant qu'elle reçoit 76, quel est le secret partagé ?
- (d) Bob choisit $b = 129$. Vérifier à partir de la valeur reçue d'Alice que le secret partagé obtenu est bien le même.
- (e) On souhaite utiliser le protocole DH pour générer une clé pour chiffrer un message avec AES-256-GCM. Quelles précautions faut-il prendre dans le choix de g et n ?

Ex2. Chiffrement de ElGamal On considère maintenant le schéma de chiffrement ElGamal dans le même groupe que précédemment, $n = 199$ et $g = 97$.

- (a) Alice choisit la clé secrète $s = 42$. Calculer sa clé publique.
- (b) Bob a utilisé la clé publique d'Alice pour chiffrer le message $(71, 156)$. Déchiffrer le message.
- (c) Comparer la taille d'un message chiffré avec celle d'un message en clair pour le chiffrement de ElGamal.

Ex3. Textbook RSA : chiffrement

Berthille a choisit les paramètres suivants pour constituer sa clé RSA : $p = 29$, $q = 157$, $e = 17$. Elle transmits sa clé publique à Aldebert qui lui a envoyé le message $[263, 1100]$ obtenu en codant les lettres du message initial sur 6 bits en utilisant le codage fourni en annexe puis en chiffrant 12 bits par 12 bits avec la clé RSA.

- (a) calculer les clés publique et privée de Berthille ;
- (b) déchiffrer le message transmis par Aldebert ;
- (c) chiffrer la réponse 4U avec la clé publique de Berthille.
- (d) que faut-il penser de cette manière de chiffrer des messages ? de la taille de la clé ?

Ex4. Textbook RSA : signature

Berthille a conservé sa clé RSA de l'exercice précédent. Elle décide de déclarer sa flamme à Clothaire en lui envoyant le message $\langle 3$ et de signer son message grâce à sa clé RSA.

- (a) calculer la signature transmise par Berthille avec son message ;
- (b) vérifier la signature comme le ferait Clothaire en recevant le message signé ;
- (c) que faut-il penser de cette manière de signer des messages ? comment l'améliorer ?

Annexe — aide au calcul

Suites de carrés successifs modulo 199 (*i.e.* $u_{n+1} = (u_n^2 \pmod{199})$) :

- 71, 66, 177, 86, 33, 94, 80, 32, 29...
- 76, 5, 25, 28, 187, 144, 40, 8, 64, 116...
- 95, 70, 124, 53, 23, 131, 47, 20, 2, 4, 16...
- 97, 56, 151, 115, 91, 122, 158, 89, 160, 128, 66...

Quelques produits modulo 199 : $5 \times 76 = 181$, $8 \times 156 = 54$, $20 \times 95 = 109$, $25 \times 181 = 147$,
 $40 \times 147 = 109$, $56 \times 97 = 59$, $56 \times 115 = 72$, $59 \times 151 = 153$, $66 \times 86 = 104$, $72 \times 122 = 28$,
 $89 \times 97 = 76$, $94 \times 104 = 25$, $153 \times 158 = 95$.

Suites de carrés successifs modulo 4097 (*i.e.* $u_{n+1} = (u_n^2 \pmod{4097})$) :

- 61, 3721, 2078, 3943, 3231, 205, 1055, 2738, 3231, ...
- 194, 763, 395, 339, 205, 1055, 2738, 3231, 205, ...

Suites de carrés successifs modulo 4553 (*i.e.* $u_{n+1} = (u_n^2 \pmod{4553})$) :

- 263, 874, 3525, 488, 1388, 625, 3620, 866, 3264, 4229, 257, 2307, 4345, 2287, 3525, ...
- 286, 4395, 2199, 315, 3612, 2199, ...
- 1100, 3455, 3612, 2199, 315, 3612, 2199, 315, 3612, ...
- 1766, 4504, 2401, 703, 2485, 1357, 2037, 1586, 2140, 3835, 1035, 1270, 1138, 1992, 2401, ...
- 3971, 1802, 915, 4026, 4549, 16, 256, 1794, 4018, 3939, 3650, 422, 517, 3215, 915, ...

Quelques produits :

$$205 \times 2884 = 19 \times 64 + 36 \pmod{4097}$$

$$263 \times 3264 = 38 \times 64 + 36 \pmod{4553}$$

$$1100 \times 3612 = 46 \times 64 + 40 \pmod{4553}$$

$$61 \times 2078 = 3848 \pmod{4097}$$

$$205 \times 1473 = 2884 \pmod{4097}$$

$$286 \times 3612 = 4054 \pmod{4553}$$

$$1766 \times 2485 = 3971 \pmod{4553}$$

$$3848 \times 3943 = 1473 \pmod{4097}$$

$$3971 \times 4018 = 1766 \pmod{4553}$$

Un codage des caractères sur 6 bits (ainsi le caractère U est codé 30) :

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	A	B	C	D	E	F	G	H	I	J
2	K	L	M	N	O	P	Q	R	S	T
3	U	V	W	X	Y	Z	a	b	c	d
4	e	f	g	h	i	j	k	l	m	n
5	o	p	q	r	s	t	u	v	w	x
6	y	z	<	>						