TD4 — Chiffrement à clé publique

Ex1. Échauffement symétrique modulaire On se place dans le corps de Galois $\mathbb{F}_{19} = \mathbb{Z}/19\mathbb{Z}$ des entiers modulo 19 munis de l'addition et de la multiplication usuelles modulo 19. Les éléments de ce corps sont représentés par les entiers de 0 à 18. Pour chacun des algorithmes de chiffrement symétrique suivants, expliquer le fonctionnement de l'algorithme de déchiffrement.

(a) $\mathrm{Enc}_k(m) = m + k \pmod{19}$. Quelles sont les valeurs de k autorisées ? Que vaut l'opposé de 7 ? En déduire $\mathrm{Dec}_7(c)$.

(b) $\mathrm{Enc}_k(m) = km \pmod{19}$. Quelles sont les valeurs de k autorisées ? Que vaut l'inverse de 9 ? En déduire $\mathrm{Dec}_9(c)$.

(c) $\mathrm{Enc}_k(m) = k^m \pmod{19}$. Quelles sont les valeurs de k autorisées ? Que vaut le logarithme de 15 en base 3 ? Comment exprimer $\mathrm{Dec}_3(c)$?

Ex2. 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 $0 \leqslant x < \varphi(n)$ 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 ?

Ex3. Textbook RSA : chiffrement
Berthille a choisit les paramètres suivants pour constituer sa clé RSA : $p = 29$, $q = 157$, $e = 17$. Elle transmis 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. Attaque sur textbook RSA
Jude a intercepté les messages 194 et 403 que Berthille a envoyé à Dalilah et Ezechiel de clés publiques RSA respectives $(301, 4097)$ et $(107, 4097)$. Jude sait que Berthille a chiffré deux fois le même message m. Aidez-le à retrouver la valeur de m sans factoriser le nombre 4097.

Annexe

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	<	>						