Haute école d'ingénierie et d'architecture Fribourg. Mathématiques spécifiques 2. 21 juin 2017

Nom, Prénom: [redacted]

6,5 pts

Note: 5,1

Travail écrit

Matériel autorisé: Formulaire, calculatrice, résumé manuscrit d'une page recto-verso.
Durée: 60 minutes.

Dans tous les exercices, il est demandé d'écrire les détails des calculs. Une solution non développée sera considérée comme fausse.

Question 1 : 2 points

1. Quels sont les quatre derniers chiffres de 13^{8007}?
2. Calculer l'index de coïncidence χ de $X =$`cabad` si on considère que l'alphabet avec lequel on travaille ne contient que les lettres $\{a, b, c, d, e\}$.

2

Question 2 : 3 points
Chiffrer et déchiffer le message $m = 110101$ à l'aide du chiffre de Merkle-Hellman en utilisant la suite supercroissante $[1, 3, 5, 10]$. Les calculs se feront modulo 23 et on multipliera le message par 11. On donnera, en particulier, la clé privée ainsi que la clé publique.

3

Question 3 : 3 points
Bob utilise le protocole RSA et publie sa clé publique $n = 187$ et $e = 3$.

1. Encoder le message $m = 15$ avec la clé publique de Bob.
2. Retrouver la factorisation de n, puis la clé privée de Bob.
3. Déchiffrer le message (faire les détails des calculs)

1,5

1) a) $13^{8007} \mod 10\,000$

$\text{pgcd}(13, 10\,0000) = 1$ ✓

$\varphi(10\,000) = \varphi(m \cdot 10^4) = \varphi(5^4 \cdot 2^4) = \varphi(5^4) \cdot \varphi(2^4)$

$= 2^3 \cdot (2-1) \cdot 5^3 \cdot (5-1) = 8 \cdot 125 \cdot 4 = 4000$ ✓

$13^{8007} = 13^{4000} \cdot 13^{4000} \cdot 13^{7}$ ✓

$13^{8007} \mod 10\,000 \Rightarrow 13^{7} \mod 10\,000 \Rightarrow 62\,748\,517$

4 derniers chiffres = 8517 ✓

b) $X(X, X') = \frac{1}{25} + \frac{4}{25} + \frac{1}{25} + \frac{1}{25} = \frac{7}{25} = 0,28$ ✓

2) Clé privée $(1, 3, 5, 10)$ $m = 23$ $p = 11$

$\text{pgcd}(23, 11) = 1$

clé publique : $1 \cdot 11 \mod 23 = 11$
$3 \cdot 11 \mod 23 = 10$
$5 \cdot 11 \mod 23 = 9$
$10 \cdot 11 \mod 23 = 18$

$\Rightarrow (11, 10, 9, 18)$ ✓

On doit envoyer 1101 0100 (j'ajoute 2 0 pour adapter à la longueur

Cryptage : $1 \cdot 11 + 10 + 18 = 39$
$= 10$ ✓

Message clair : (1101 0100) en binaire
Message crypté : (39 10) en décimal ✓

Déchiffrer : ~~Méthode inverse de~~

Résoudre $x \cdot p \bmod m = 1$

$11x \bmod 23 = 1$

	r	. a	. b		q
1	23	1	0		2
2	11	0	1	$1_4 - 2 \cdot 1_2$	
3	1	1	-2	$1_2 - 11 \cdot 1_3$	11
4	0	-11	23		

PGDC $(23, 11) = 1$ ✓

~~PGDC~~ $x = 21$ ✓

$39 \cdot 21 \bmod 23 = 14 = 1101$ ~~erreur~~

$10 \cdot 21 \bmod 23 = 3 = 0010$ ✓

3) $m = 15 \quad n = 187 \quad e = 3$

$\varphi(187) = \varphi(17 \cdot 11) = \varphi(17) \cdot \varphi(11) = 16 \cdot 10 = 160$

r	. a	. b		q
160	1	0		-
3	0	1		53
1	1	-53	$r_1 - 53 \cdot r_2$	3
0	-3	159	$r_2 - 3r_3$	

$\Rightarrow d = a^{-3} + \varphi(n) = 157$

chiffrer : $c = a^k \bmod n \Rightarrow 15^3 \bmod 187$

$3 = 011$

A	B
15	15
38	9
135	93
86	93

↑ message crypter

clé privé = (p, q, d), $p = 17$ et $q = 11$

$= (17, 11, 157)$

Péchithur: $c^d \equiv m \mod n$

$m = 93$

$n = 187$

$d = 157$

$93^{157} \equiv m \mod 187$

Non. Calculs ? X