Université Lyon I

MIF30
Partiel de Cryptographie et Sécurité

7 mars 2005. Durée: 2H.
Notes de cours/TD autorisées.
Calculatrice interdite, rédaction du détail des calculs exigée.

Exercice I

Pour $x \in \mathbb{Z}$, résoudre,

1.
$$x^2 \equiv 1 \pmod{15}$$

2.
$$x^2 \equiv 11 \pmod{991}$$

Exercice II

1. Calculer l'inverse de 3 modulo 55
2. Calculer
$$18^{13} \pmod{55}$$
3. En déduire la valeur de
$$3^{27} \pmod{55}$$

Exercice III

Pour $x \in \mathbb{Z}$, résoudre le système de congruences:

$$\begin{cases} x^2 \equiv -1 \pmod{13} \\ 4x \equiv 1 \pmod{15} \end{cases}$$

Exercice IV

Chiffrement de Merkle-Hellman

1. Alice choisit le sac à dos facile

$$s = (s_i)_{i\in[1,4]} = (4, 5, 10, 21),$$

$N = 50$, et $d = 13$.

2. Calculer le sac à dos déguisé $ds = (ds_i \bmod N)_{i\in[1,4]}$. La clef publique d'Alice est le couple (N, ds).

3. Bob veut envoyer à Alice le message $M = (1, 0, 0, 1)$. Calculer le message crypté envoyé par Bob.

4. Alice a reçu de Martin le message crypté $MC = 18$. Quels calculs fait Alice pour retrouver le message clair envoyé par Martin?

Exercice V

Méthode RSA.

On considère dans la suite la clef publique (n=253, e=63) utilisée pour crypter le message

$$M = ZZZ$$

en codant Z par l'entier 26.

On pose

$$N = 26^{63} \pmod{253}$$

On admettra les résultats suivants

$$75^2 \equiv 59 \pmod{253}$$

$$124^2 \equiv 196 \pmod{253}$$

$$75 * 59 \equiv 124 \pmod{253}$$

$$n^7 \equiv 1 \pmod{23} \leftrightarrow n \equiv 1 \pmod{23}$$

1. Calculer la clef privée associée d associée.

2. Montrer que

$$N^7 = 26 \pmod{253}$$

3. Calculer

$$75^7 \pmod{253}$$

4. Montrer l'équivalence

$$n^7 = 1 \pmod{253} \leftrightarrow n = 1 \pmod{253}$$

5. En déduire la valeur de N et donner le cryptage du message $M = ZZZ$