Université Paris 12
Licences d'Informatique et de Mathématiques
2007-08

TD de Mathématiques Discrètes
TD 6 - Arithmétique - Système RSA

Mars 2008

Exercice 1 : RSA, chiffrement, déchiffrement

On considère le système cryptographique RSA avec la clef publique (n, e), avec $e = 51$ et $n = 47 * 59 = 2773$.

1. Quelle est la valeur de $\varphi(n)$?
2. Quelle est la clef secrète qui permet de décoder les messages ?
3. Quel est le cryptogramme du message $M = 1322$?
4. On déchiffre $C = 357$. Quelle est la valeur du message ?

Exercice 2 : Quelles clefs pour RSA ?

1. Parmi les couples $(3087, 323), (3243, 475), (3953, 625), (3599, 435)$, lesquels sont des clés publiques possibles pour RSA ? Justifier.
2. Quelles sont les clefs secrètes correspondantes ?
3. Quels sont les cryptogrammes du message 234 ?
4. Donner un exemple de clé publique qui permette de chiffrer des blocs de 12 bits avec RSA.

Exercice 3 :

Soient p et q deux premiers impairs et soit $n = p \cdot q$. Montrez qu'au lieu d'effectuer la procédure RSA avec $\varphi(n)$, on peut également utiliser $\varphi(n)/2$. C'est-à-dire, si $e, d \in \mathbb{N}$ avec $ed \equiv 1 \mod (\varphi(n)/2)$ alors $x^{ed} \equiv x \mod n$ pour tout $0 \leq x < n$.

Exercice 4 :

Alice encrypte le message m en appliquant la procédure RSA. Pour cela elle utilise la clé publique de Bob qui est (899, 11). Le texte résultant est 468. Déterminez le message m.

Exercice 5 :

Supposons que Alice et Bob (les deux utilisent la procédure RSA) ont le même $n = p \cdot q$. Supposons en plus que e_A et e_B sont premiers entre eux.

Montrez que :
Si Eve intercepte les textes cryptés d'un message m qui a été envoyé par Charles à Alice et Bob, $c_A = m^{e_A} \mod n$, $c_B = m^{e_B} \mod n$,
alors Eve peut déterminer m.