Université Bordeaux 1 — **MHT203 – Cryptologie**
Mathématiques — Année 2012–2013

FEUILLE D'EXERCICES n° 8

RSA

Exercice 1 – On considère le système de chiffrement RSA avec la clé publique $(n, e) = (2773, 51)$.

1) Factoriser n. Quelle est la valeur de $\varphi(n)$?

2) Déterminer l'exposant de déchiffrement d.

3) Chiffrer le message $M = 1322$; déchiffrer le cryptogramme $C = 23$.

Exercice 2 –

1) Parmi les couples suivants $(3087, 323)$, $(3953, 475)$, $(3599, 435)$ lesquels sont des clés publiques possibles pour RSA ? Quelles sont les clés secrètes correspondantes ?

2) Quels sont les cryptogrammes du message $M = 234$?

Exercice 3 – Soit un cryptosytème RSA de clé publique $(e, n = pq)$. Vérifier que connaître l'un des trois nombres p, q et $\varphi(n)$ permet de calculer la clé privée.

Exercice 4 – Pour accélérer le déchiffrement RSA on utilise le théorème des restes chinois. Supposons que $d_K(y) = y^d$ et $n = pq$.

1) On définit $d_p = d\,[p-1]$, $d_q = d\,[q-1]$, $M_p = q^{-1}[p]$ et $M_q = p^{-1}[q]$; puis on effectue les opérations suivantes :

$$x_p \leftarrow y^{d_p}\,[p], \quad x_q \leftarrow y^{d_q}\,[q], \quad x \leftarrow M_p q x_p + M_q p x_q\,[n].$$

Montrer que $x = y^d \bmod n$.

2) Etant donné $p = 1511$, $q = 2003$ et $d = 1234577$. Calculer d_p, d_q, M_p et M_q ; puis déchiffrer le texte $y = 152702$.

Exercice 5 – Montrer que si l'on chiffre un message lettre par lettre le système RSA n'apporte aucune sécurité.

Exercice 6 – Soit $n = 16459$. En remarquant que $12534^2 \equiv 1 \bmod n$, factoriser n par un calcul de pgcd.

Exercice 7 – Alice utilise le système RSA avec le module $n = 391$ et l'exposant public $e = 3$.

1) Vérifier que le cryptogramme du message $m_1 = 246$ est $c_1 = 2$ et celui de $m_2 = 58$ est $c_2 = 3$.

2) En déduire le message m_3 correspondant au cryptogramme $c_3 = 6$, sans calculer l'exposant de déchiffrement.