Sécurité Informatique
3 SI & ISIL **TD 1 : Le chiffrement RSA**

1 Codage et décodage RSA.

On considère la clef publique RSA (11, 319), c'est-à-dire pour $n = 319$ et $e = 11$.
Note : on pourra utiliser les résultats suivants :

- $319 = 11 \times 29$; $10^{11} = 263 \pmod{319}$; $263^2 = 216 \times 319 + 265$;
- $133^3 = 12 \pmod{319}$; $133^{25} = 133 \pmod{319}$;
- $11^2 = 121 \pmod{280}$; $11^4 = 81 \pmod{280}$; $11^8 = 121 \pmod{280}$; $11^{16} = 81 \pmod{280}$;
- $95 = 64 + 31$; $81.11 = 51 \pmod{280}$; $81.121 = 1 \pmod{280}$.

1. Quel est le message correspondant au codage avec cette clé du message $M = 100$?
2. Calculer d la clé privée correspondant à la clé publique e.
3. Décoder le message $M' = 133$.
4. Le message codé 625 peut-il résulter d'un codage avec la clé publique ? Même question avec la clé privée.

2 Cryptographie RSA et authentification

Un professeur envoie ses notes au secrétariat de l'École par mail. La clef publique du professeur est (3,55); celle du secrétariat est (3,33).

1. Vérifier que la clef privée du professeur (supposée connue de lui seul) est 27; et que celle du secrétariat est 7.

2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef RSA du secrétariat. Quel message chiffré correspond à la note 12 ?

3. Pour assurer l'authenticité des messages contenant les notes, le professeur signe ses messages pour le secrétariat aprés les avoir chiffrés. Le secrétariat reçoit le message 23. Quelle est la note correspondante ?