TD Arithmétique

LSI 1

1 Cryptographie RSA

1.1 Description du protocole

On suppose qu'Alice veut envoyer un message secret $m = 12$ à Bob.

1. (a) Bob choisit deux nombres premiers, par exemple $p_1 = 7$ et $p_2 = 5$.
   (b) Bob calcule $n = p_1 p_2$ et $\phi(n)$ (avec quelle formule ?).
   (c) Bob choisit un nombre $e = 17$ premier avec $\phi(n)$.
   (d) Bob calcule un nombre d tel que $ed \equiv 1 \mod \phi(n)$.
2. Bob envoie e et n à Alice (c'est la clé publique).
3. Pour envoyer son message $m = 12$ (qui est un nombre entier modulo n) à Bob, Alice calcule le message crypté $c \equiv m^e \mod n$ et envoie c à Bob.
4. Bob reçoit c et calcule $m \equiv c^d \mod n$.

1.2 Vérification du protocole

1. Expliquer comment Bob peut calculer d après avoir choisi e.
2. Montrer que deux nombres sont égaux modulo n si et seulement si ils sont égaux modulo p_1 et p_2.
3. Montrer que pour tout $x \in \{0, 1, \dots n-1\{$ et pour tout $alpha \equiv 1 \mod (p_1 - 1)$, $x^\alpha \equiv x \mod p_1$
4. En déduire que pour tout $x \in \{0, 1, \dots n-1\{$, $x^{ed} \equiv x[n]$.
5. Montrer que Bob décrypte effectivement le message d'Alice.

1.3 Application

Dans toute la suite, on pourra utiliser les résultats numériques suivants :
- $319 = 11 \times 29$; $10^{11} \equiv 263 \mod 319$; $263^2 = 216 \times 319 + 265$;
- $133^3 \equiv 12 \mod 319$; $133^{25} \equiv 133 \mod 319$;
- $11^2 \equiv 121 \mod 280$; $11^4 \equiv 81 \mod 280$; $11^8 \equiv 121 \mod 280$; $11^{16} \equiv 81 \mod 280$
- $95 = 64 + 31$; $81 \times 11 \equiv 51 \mod 280$;$81 \times 121 \equiv 1 \mod 280$

Exercice 1. On considère la clef publique RSA $(11, 319)$, c'est à dire pour $n = 319$ et $e = 11$.

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

Exercice 2. Un professeur envoie ses notes au secrétariat de l'École par mail. La clef publique du professeur est $(3, 55)$, celle du secrétariat $(3, 33)$.

1. Déterminer la clef privée du professeur (supposée connue de lui seul) celle du secrétariat.
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 ?