

# Cryptographie et Sécurité - TD3

[guillaume.postic@universite-paris-saclay.fr](mailto:guillaume.postic@universite-paris-saclay.fr)

## Exercice 1 : chiffrement RSA

On rappelle le principe du chiffrement RSA vu en cours.

Étant donné la clé publique  $k_{pub} = (n, e)$  et le texte  $x$  en clair, ( $x < n$ ), le chiffré est obtenu avec  $y = E_{k_{pub}}(x) \equiv x^e \pmod n$ .

Étant donné la clé privée  $k_{pr} = d$  et le chiffré  $y$ , le texte clair est obtenu avec  $x = D_{k_{pr}}(y) \equiv y^d \pmod n$ .

On rappelle que  $n = pq$ , avec  $p$  et  $q$  deux nombres premiers tq  $\varphi(n) = (p-1)(q-1)$ ,  $e \in \{1, 2, \dots, \varphi(n) - 1\}$  tel que  $\text{pgcd}(e, \varphi(n)) = 1$  et on a  $de \equiv 1 \pmod{\varphi(n)}$ .

1. On considère l'exemple suivant :  $p = 11$ ,  $q = 17$  et  $e = 27$ . À quoi sont égaux la clé publique  $k_{pub}$  et la clé privée  $k_{pr}$  ?
2. Alice veut chiffrer le message  $x = 10$ . Quel est le chiffré  $y = E_{k_{pub}}(x)$  qu'elle envoie à Bob ?
3. À la réception de  $y$ , Bob va le déchiffrer. Vérifier que l'on a  $D_{k_{pr}}(y) = 10$  et que Bob récupère bien le message envoyé par Alice.

## Exercice 2 : Diffie-Hellman

1. Trouvez la valeur du secret partagé par Alice et Bob, à partir des paramètres suivants : module  $p = 23$  ; générateur  $g = 5$  ; clé privée d'Alice  $a = 6$  ; clé privée de Bob  $b = 15$ .
2. Bob reçoit de la part d'Alice un message  $C = 18$  chiffré avec l'algorithme ElGamal. Quelle est la valeur du message clair  $M$  que Bob déchiffre ?

## Exercice 3 : courbes elliptiques

On considère la courbe elliptique suivante :  $y^2 \equiv x^3 + 3x + 3 \pmod 5$

1. Déterminez tous les points faisant partie de cette courbe.
2. Quels sont les éléments générateurs ? Formulez votre réponse sous la forme :  $(x_g, y_g) \rightarrow (x_{2g}, y_{2g}) \rightarrow \dots \rightarrow O$

## Exercice 4 : théorème des restes chinois

Trouvez la valeur de  $x$  qui résout le système de congruence suivant :

$$x \equiv 3 \pmod 5$$

$$x \equiv 1 \pmod 7$$

$$x \equiv 6 \pmod 8$$