2OS PM – Mardi 27 février 2024 Nom & prénom : .....

RSA – TE 812A

Problème	1	2	3	4	**Total**
Points	10	6	4	4	24
Points obtenus					

Problème 1 (10 points)

Le fichier Probleme1.txt contient deux nombres premiers p et q.

On choisit $e = 5$ qui satisfait la condition $\gcd(e, \varphi(n)) = 1$, où $n = p \cdot q$.

On dispose ainsi d'une clé publique (n, e).

a) Dans le fichier Probleme1.py, construire la clé privée (n, d). Afficher à la console la valeur de d.

b) Coder le message suivant (présent dans Probleme1.txt) à l'aide de la clé publique (n, e) et l'afficher à la console.

12121212121212121212121212121212121212121212121212121212121212

c) Décoder le message suivant (présent dans Probleme1.txt) à l'aide de la clé privée (n, d) et l'afficher à la console.

55228627266418678856463185798470045590747247627958594059706091003234585998374492561554612749266368533431697685315608739249228605414875645167357497080790434882130515969344843378451472060980182922101044371820824452560867955722656399610623242021367441438674089328134830572426581179521970937 5

Problème 2 (6 points)

Alice publie sa clé publique : $n = 10000082000145299$ et $e = 49$.

On intercepte le message provenant de Bob, $c = 5920555950326593$, destiné à Alice.

a) Déterminer la clé privée d'Alice (n, d).

b) Déchiffrer le message c destiné à Alice.

Dans le fichier Probleme2.py, créer un programme qui affiche à la console les solutions de ce problème.

Problème 3 (4 points)

Le nombre

$$n = 190444953133930421750380017 7$$

est le produit de deux nombres premiers p et q.

Connaissant

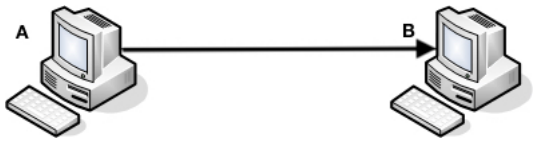
$$\varphi(n) = 190444953133921636650423 1536$$

déterminer p et q.

Dans le fichier Probleme3.py, créer un programme qui calcule puis qui affiche à la console p, q et le produit $p \cdot q$.

Problème 4 (4 points)

L'ordinateur A envoie des données chiffrées à l'ordinateur B.



Au début de l'envoi, l'ordinateur A envoie à l'ordinateur B un message signé puis chiffré, entete = 777777, connu de l'ordinateur B. L'ordinateur B reçoit ce message. Il le déchiffre. Si ce message est identique au message entete = 777777, alors l'authentification de A par B est assurée et la liaison est établie.

L'ordinateur B reçoit le message entete_envoye = 2894401431.

Est-ce que la liaison entre A et B est établie ?

Dans le fichier Probleme4.py, créer un programme qui justifie et qui affiche à la console votre réponse.

Table 1: Annuaire des clés **RSA**

	module de chiffrement	clé publique	clé privée
ordinateur A	$n_A = 4199382503$	$e_A = 251$	$d_A = 635743235$
ordinateur B	$n_B = 2987582503$	$e_B = 331$	$d_B = 2319577467$

NB : la clé privée de A n'est pas connue B et inversément.