

EXERCICES RSA

Exercice 1

On considère les valeurs $P = 53$, $Q = 11$ et $E = 3$.

- Calculez le module N .
- Calculez la fonction d'Euler $T = (P - 1)(Q - 1)$.
- Utilisez le lien suivant pour calculer la valeur D de la clé privée : <https://planetcalc.com/3311/>.
- Chiffrer JEVOUSAIME en s'aidant du lien : <https://www.wolframalpha.com>. On transformera auparavant le texte en nombre : 10 05 22 15 21 19 01 09 13 05
- Vérifier que vous retrouvez le texte d'origine en déchiffrant.

Exercice 2

Connaissant la clé publique ($N = 119$, $E = 5$) de ce cryptogramme RSA :

090 086 036 067 032 001 003 031 059 031

- Calculez P et Q .
- Calculez la clé secrète D en s'aidant du lien : <https://planetcalc.com/3311/>.
- Déchiffrez le cryptogramme en s'aidant du lien : <https://www.wolframalpha.com> et du tableau suivant :

1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M

14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Exercice 3

Bob choisit comme nombre premier $P = 17$ et $Q = 19$, comme exposant $E = 5$. Alice et lui se fixent un protocole RSA dans lequel les messages sont des nombres en base 10 que l'on code par bloc de 2 chiffres. Alice veut envoyer le message "462739".

- Donnez la clé publique de Bob.
- Donnez la clé secrète de Bob.
- Ecrivez le message chiffré que Alice envoie à Bob.
- Déchiffrez le message qu'a reçu Bob et vérifiez que c'est bien celui qu'a envoyé Alice.

Exercice 4

Bob utilise le protocole RSA et publie sa clé publique $N = 187$ et $E = 3$.

- Chiffrez le message $m = 15$ avec la clé publique de Bob.
- En utilisant le fait que $T = 160$, retrouvez la factorisation de N .
- Retrouvez la clé privée de Bob.