1. La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données.
- La cryptanalyse est l'étude des informations cryptées, afin d'en découvrir le secret.
- La cryptologie englobe la cryptographie et la cryptanalyse

Exercice 1

1.

2. M= LES FINS NE JUSTIFIENT PAS LES MOYENS

Exercice 2

1. pour le professeur : $\varphi(55)=40$ $27*3=81=1 \bmod 40$
pour la secretaire :$\varphi(33)=20$ et $7*3=21=1 \bmod 20$
2. le professeur envoit $m=12^2 \bmod 33=12[33]$;=> $m=12 \bmod 33$
3. la note $(23^3 \bmod 55)^7 \bmod 33=(12^7 \bmod 33) =12$

Exercice 3

Soit un système de chiffrement où : p = 131, q = 151.

1. p et q sont premiers entre eux alors la condition du système RSA est satisfaite.
2. Calcule de e et d.
   n = pxq =131*151=19781
   $\varphi(n)=(p-1)(q-1)=130*150=19500$
   e=11143
   ed-1est exactement divisible par $\varphi(n)$ => d=7
   (11143*7-1=19500* 4)
3. Quel entier positif inferieur à $p \cdot q = 19781$ sera le message en clair si le message codé reçu est 141 :
   c =141 $m = c^d \bmod n$
   => $m=141^7 \bmod 19781=1032$
   m=1032

Exercice 4

II-On veut garder la confidentialité d'un document en chiffrant son contenu par le code de Vigenère.

1- Le chiffrement de Vigenere fait partie de quelle famille de code ?

La famille des codes de substitution

2- Chiffrer avec le chiffre de Vigenère le texte suivant M= **BONNE CHANCE** tel que la taille du bloc est m = 4, $n_1 = 5$, $n_2 = 14$, $n_3 = 7$, $n_4 = 25$

C=GCUM JQOZ SQL

- Pour le même texte en clair on obtient le texte chiffré suivant **FWLOIKFB RKC**.

3- Quels sont les clés utilisées telle que m=4 ?

$n_1 = 4$, $n_2 = 8$, $n_3 = 24$, $n_4 = 1$

Exercice 5

La signature est valide si
– $C = S^e \bmod n$.
Dans ce cas
– $S^e \bmod n = 182^{13} \bmod 221 = 65$, ce qui est valide