

Filière : TSSR2/TSDI2	Formateur : M. IGHIOUR
Module : Notions de sécurité des réseaux informatiques	
Date : 29/11/2023	Durée : 1h30
NE : Contrôle 1	

Exercice 1 :

- 1) Quel est le principe de chiffrement de Caesar ? (2pts)
- 2) Ecrire puis expliquer les éléments qui font partie à la formule de chiffrement du VERNAM. (2pts)
- 3) Qu'est-ce qu'une attaque ?

Exercice 2 :

Calculer les valeurs demandées : (4pts/élément)

- a) E_{ROT3} (« JE SUIS LA ») - Ceasar
- b) D_{ROT4} (« BRTNTAYIKLW ») - Ceasar
- c) D_{TOTO} (« mpfjn gtn ubch »)- Vigenere
- d) E_{OTOT} (« MSPORT ») – Vigenere
- e) E_{10101} (« 10110111 ») – Vernam
- f) E_{10101} («144 ») – Vernam
- g) D_{1010} (« 98 ») – Vernam

NB :

E (Encryption) : fonction de chiffrement

D (Decryption) : fonction de déchiffrement