Université Kasdi Merbah Ouargla
Département d'informatique et technologie de l'information

Niveau : Licence 3 Durée : 01h :30min
Module : Sécurité Informatique
Resp du cours : Dr. Boukhamla AKRAM **29/05/2022**

Examen de Rattrapage 2ème semestre

Exercice 1 (10pts):

1. Déchiffrer en appliquant le chiffrement par transposition le texte suivant XEETAGANRTPEEMDARA sachant que la clé utilisée est MAI.

2. Déchiffrez le texte chiffré suivant « DXGGVCPTBG MAHSCUCXVSYP» sachant qu'il a été chiffré avec la clef « LICENCE».

3. Pour le même texte en clair on obtient le texte chiffré suivant «TGEXWBCIOS JEFJFNRTDEVV». Quelle est la clef ?.

Exercice 2 (10 pts):

Alice et Bob utilisent le protocole d'échange de clés Diffie-Hellman pour convenir d'une clé pour un chiffrement par décalage. Supposons que le mod public soit n=22 et la base publique est 5.

- Alice choisit 8 comme numéro secret. Quel numéro envoie-t-elle à Bob ?

- Bob choisit 12 comme numéro secret. Quel nombre envoie-t-il à Alice ?

- Comment Alice calcule-t-elle la clé (K1) et qu'obtient-elle ?

- Comment Bob calcule-t-il la clé (K2) et qu'obtient-il ?

Alice envoie également le message chiffré **WJIIZ NJGPODJI** (la clé est le décalage utilisé pour chiffrer ce message).
- Quel est le message d'Alice à Bob ?

Bon courage