FACULTE DES SCIENCES INFORMATIQUES

EXAMEN DE LA DEUXIEME SESSION DE LA CRYPTOGRAPHIE ET THEORIE DES CODAGES.

NOMS :

QUESTION 1 (2 points). Expliquez le mécanisme de confidentialité et d'authentification avec le chiffrement asymétrique et symétrique combiné.

QUESTION 2 (3 points). Expliquez en détaille les chiffrements symétrique avec DES et Asymétrique avec RSA.

QUESTION 3 (5 points). On vous donne cette fonction D=(M*K-1)MOD Z_{26}, dans l'alphabet (a=0, b=2,……,z=25) avec comme clé k=3 déchiffrez le message suivant : m=''VMHHQ''.

QUESTION 4(4 points). On vous donne cette clé k=11 pour chiffrement symétrique, trouvez son inverse dans Z_{26}.

QUESTION 5(6 points). Décrypter le message «**XDRJXWJSDPVTBH**» en utilisant le chiffrement d'Affine avec k = (19,3) sachant la même clé a été utilisée pour le chiffrement.

Bonne application

Il faut beaucoup prier !