Etablissement Inter – Etats d'Enseignement Supérieur
CENTRE D'EXCELLENCE TECHNOLOGIQUE PAUL BIYA
BP 13 719 Yaoundé (Cameroun) Tél.(237) 22 72 99 57/(237) 22 72 99 58
Site web: www.ialcameroun.com E-mail: contact@ialcameroun.com

EXAMEN DE FIN DE SEMESTRE

Session de Juin 2020

Epreuve de Rattrapage de Cryptographie

Niveau : II **Année académique : 2019/2020** **Filière : GL et SR** **Durée : 01h**

Exercice 1:

On considère le chiffrement RSA suivant : En supposant que l'entité X change sa clé RSA tous les 25 jours et l'entité Y tous les 31 jours. Sachant que X change sa clé aujourd'hui et que Y a changé sa clé y a trois jours, déterminer quand sera la prochaine fois que X et changeront leur clé le même jour.

Exercice 2:

Pour transmettre un message on utilise le système de chiffrement suivant :

- 1ere étape : à chaque lettre du message en clair on associe son numero d'ordre dans l'alphabet. On obtient ainsi une suite de nombres. (A=1, B =2, C=3,..)
- 2eme étape : on considère la suite d'entiers naturels(Xi) définie par :

$$\begin{cases} xi = 1 \\ pour\ tout\ entier\ i\ non\ nul: x_{i+1} \end{cases} = (5xi + 2) mod 33$$

- 3eme étapes on ajoute terme à terme les suites obtenues dans la 1ere et 2eme étape : on a alors le message chiffré.

1. Déchiffrez le message suivant :

   5,12,6,23,31,18,28,9,35,18 ;15,27 ,16,27,21,22,16,24,32,34,10,21.

2. Comparez cette technique de chiffrement avec la technique du masque jetable.

Exercice 3:

M. Tankou envoie ses notes au secrétariat de L'IAI par mail. La clé publique de M .Tankou est (3,55); celle du secrétariat est (3,33).

1. Vérifier que la clé privée de M. Tankou (supposée connue de lui seul) est 27; et que celle du secrétariat est 7.

2. Pour assurer la confidentialité de ses messages, M. Tankou chiffre les notes avec la clé RSA du secrétariat. Quel message chiffré correspond à la note 12 ?

3. Pour assurer l'authenticité des messages contenant les notes, M. Tankou signe ses messages pour le secrétariat après les avoir chiffrés. Le secrétariat reçoit le message 23. Quelle est la note correspondante ?