ENSA
ÉCOLE NATIONALE DES SCIENCES APPLIQUÉES
KHOURIBGA

Université Sultan Moulay Slimane

ENSA KHOURIBGA ÉCOLE NATIONALE DES SCIENCES APPLIQUÉES

- Projet en cryptographie –

Programmation de certains cryptosystèmes

DESCRIPTION

Le but de ce projet est de décrire le fonctionnement d'un cryptosystème moderne ainsi que la programmation de trois chiffrements étudiés en classe.

TRAVAIL DEMANDE:

- *Présentation de 20 à 30 minutes (sur Power-point ou autre outil informatique)*
  Présenter un cryptosystème moderne (voir ci-dessous la répartition des sujets par groupe) :
  - *Principe du fonctionnement*
  - *Un exemple illustratif*
  - *Cryptanalyse*
  - *Optionnel : Une note bonus est dédiée à chaque groupe qui réussit à programmer le cryptosystème.*

- *Rapport :*
  - *Cryptosystème moderne(voir la liste d'affectation)*
  - *L'algorithme et le programme de chacun des trois cryptosystèmes (écrits dans un langage informatique de votre choix): Code de Vigénère, chiffrement de Hill, masque jetable.*
  - *Une version imprimée à rendre le jour de la présentation*
  - *Une version électronique à envoyer au plus tard un jour avant la présentation à l'adresse suivante :* ***projet.ensak@gmail.com***

Date de remise des rapports : ..... - Date des exposés : .....

Groupe	*Etudiants*	*Sujet*
1		*Code Rabin*
2		*Code Goldwasser-Micali*
3		*Code Merkle-Hellman*
4		*Code El Gamal*
5		*Code Menezes-Vanstone*
6		*RSA* avec la multiplication de Montgomery