Université **Badji-Mokhtar** **10/02/2022**
Département **Informatique**
Master 1 **ILC**

Corrigé de l'EXAMEN
Protection et Sécurité des Systèmes Informatiques

Durée: 1 H 00, documents non autorisés

Exercice 1. (8 point)

On considère les substitutions qu'on peut qualifier de **tri-cycle** :
on découpe l'alphabet numérisé [0,25] en trois intervalles I1=[0, 10] et I2= [11,20]. I3= [21,25].
Sur l'intervalle I1 on effectue un décalage cyclique de k1=2 et sur I2 de K2=3 et sur I3 de K3=4.

1. Ecrire les trois équations de cette substitution, Pour une lettre de rang k.
2.

Equation 1 : C(k) = (k+2) mod 11 **Si k appartient à [0..10]**

Equation 2 : C(k) = (k+3) mod 10+11 **Si k appartient à [11..20]**

Equation 3 : C(k) = (k+4) mod 5 + 21 **Si k appartient à [21..25]**

3. Donner le chiffré du mot **OMICRON**

C(OMICRON)= SQKEL SR

Exercice 2 (6 points)

Pour assurer la confidentialité, un professeur chiffre les notes, en utilisant la RSA (clé publique du secrétariat e = 3; n= 187; la clé publique du professeur est e=13 n=55).

1. Quel est le chiffré de la **note= 14** ?

Professeur chiffre les notes avec la clé publique du secrétariat :

$C(14)= 14^3 \bmod 187 = 126$

2. Si le professeur décide de signer les messages envoyés, donner le chiffre de la **note = 14.**

Le professeur doit signer le chiffré de la note par sa clé privée.
Cherchons la clé privée **(d,55):**
n=55, p=5,q=11

Z=40
ed=1 mod Z
13d=1mod40
d=37

C(14) apres signature est egale à:
126^{37} mod 55 =36
C(14)signé= 36

Exercice 3 (6 points)

On suppose que f1(a)=a **Or** 1001, f2(a)= a **XOR** 1010 pour toute chaine **a** de 4bits. En utilisant le chiffrement de Feistel:

1. Calculer C de m=11011011.
   Première itération-→ 1011 0110

   C(11011011)= 0111 0110
2. Expliquer le principe de diffusion, comment est- il mis en œuvre dans SDES?

   La diffusion est le fait que chaque bit du texte en clair ait une influence sur une grande partie du texte chiffré.
   La diffusion est mise en œuvre via un ensemble de permutations linéaires.

   Les permutations de SDES implémentant la diffusion sont
   - **IP** (bloc de 8) bits**:** Permutation initiale
   - **E/P:** Permutation expansive qui transforme un bloc de 4 bits en un bloc de 8 bit**,**
   - **P4**(bloc de 4bits**)**
   - **IP^{-1}** (bloc de 8 bits)**:** permutation finale ou inverse