Sécurité Informatique

1CS

Contrôle Final

Partie Exercices

Exercice1 *(2 points)*

Calculez 7^{-1} mod 1440.

Donnez une solution dans l'intervalle [0,1339] = {x Є Z; 0 ≤ x ≤ 1339} puis une autre solution dans l'intervalle [−1397, 42] = {x Є Z; −1397 ≤ x ≤ 42 }.

Exercice 2 *(2 points)*

On désire concevoir un mot de passe composé de 12 caractères et on dispose de toutes les lettres de la langue française minuscules et majuscules, tous les chiffres arabes ainsi que 12 caractères spéciaux.

- Calculer la force équivalente à une clé AES de ce mot de passe.
- Calibrer cette force en (Faible, Moyenne ou Forte) et donner la taille minimum pour avoir une force équivalente à une clé AES de 128 bits.

Exercice 3 *(2 points)*

Soit le diagramme de Fiestel suivant, on désire l'utiliser pour chiffrer ω Є $\{0, 1\}^6$ puis déchiffrer le résultat pour enfin retrouver ω. Soit ω = 110101, les fonctions f_1 et f_2 sont données avec le schéma, Remplissez les cases vides du diagramme par les valeurs correspondantes.

$f_1 : \{0,1\}^3 \to \{0,1\}^3$
000 → 101
001 → 100
010 → 111
100 → 000
011 → 001
101 → 101
110 → 010
111 → 110

$f_2 : \{0,1\}^3 \to \{0,1\}^3$
000 → 010
001 → 001
010 → 110
100 → 111
011 → 110
101 → 011
110 → 001
111 → 100