Protection des Données

Élèves: Achraf THABET, Agustin ZORZANO

FISE A2

Installation

1. Exécutez: make
2. Exécutez ./Programme

Il est nécessaire d'avoir GMP installé avec le support de c et c ++.

Paramètres

Le programme permet une série de paramètres. Les flags à utiliser sont listés ci-dessous.

- **-columns**: Il vous permet de définir le nombre de colonnes dans la matrice. Ce doit être une valeur supérieure à 1.
- **-rows**: Il vous permet de définir le nombre de lignes dans la matrice. Ce doit être une valeur supérieure à 1.
- **-column_1**: Il vous permet de définir la colonne 1 de la matrice qui sera utilisée pour l'encodage. Ce doit être une valeur supérieure ou égal à 0.
- **-column_2**: Il vous permet de définir la colonne 2 de la matrice qui sera utilisée pour l'encodage. Ce doit être une valeur supérieure ou égal à 0.
- **-tattoo**: Il vous permet de définir le tatouage à appliquer lors de l'encodage. Ce doit être un nombre binaire avec un maximum taille de 128 bits
- **-ks**: Il vous permet de définir la clé qui sera utilisée pour générer r2. Ce doit être un nombre positif
- **-process**: Il vous permet de spécifier le type de processus que vous souhaitez exécuter (encodage, décodage ou les deux). La valeur doit être "e", "d" ou "ed".
- **-file**: Il vous permet d'utiliser une matrice qui est enregistrée dans un fichier csv. Le fichier doit être séparé par ",". Si vous décodez, c'est obligatoire. Si vous décodez et que vous utilisez le fichier généré avec le processus d'encodage, alors vous devez utiliser "encoded_with_tattoo.csv".
- **-EP**: Il vous permet d'indiquer la valeur EP. Il ne sera utilisé que s'il s'agit d'un processus de décodage. Si vous décodez, c'est obligatoire.
- **-p**: Il vous permet d'indiquer la valeur p. Si vous décodez, c'est obligatoire.
- **-q**: Il vous permet d'indiquer la valeur q. Si vous décodez, c'est obligatoire.

Exemple

./Programme -columns 4 -rows 5 -tattoo 01101101

Cela exécutera le programme en créant une matrice de 5 lignes et 4 colonnes (les valeurs seront aléatoires) et le tatouage utilisé sera 01101101.

Output

Le programme générera une sortie par le terminal (standard output) et également dans des fichiers. Le terminal affichera:

- La matrice d'origine à encoder
- Les valeurs de p, q et les colonnes d'encodage utilisées
- L'EP obtenu et la partie du tatouage utilisée lors de l'encodage
- Les matrices obtenues et le tatouage obtenu lors du décodage selon les deux méthodes

Plusieurs fichiers seront créés dans lesquels on pourra visualiser les matrices. Certains seront au format csv et d'autres au format txt (avec un affichage "plus convivial"):

- La matrice d'origine (csv et txt)
- Les matrices décodées par les deux méthodes (csv et txt)
- Quelques matrices intermédiaires (csv)

Clarifications

- Vous pouvez exécuter “sh compare.sh” pour vérifier si les matrices décodées sont les mêmes que l'original. Le fichier est un script bash qui exécute deux commandes diff comparant le fichier "original.csv" avec les fichiers “decoded_3_3_1.csv” et “decoded_3_3_2.csv”

- Nous n'avons pas pu effectuer tous les tests donc il pourrait y avoir certains bugs/erreurs pour certains cas (par exemple avec les données passées en paramètres lors de l'exécution du programme). Cependant, nous pensons qu'il ne devrait y avoir aucun problème à utiliser les valeurs par défaut (./Programme)