HAI927I
Projet Image

Compte Rendu n°1
Sujet n°3 - Musée Sécurisé Virtuel

COUNILLE Alexandra
&
LIN-WEE-KUAN Malika

FACULTÉ DES SCIENCES
MONTPELLIER

UNIVERSITÉ
DE MONTPELLIER

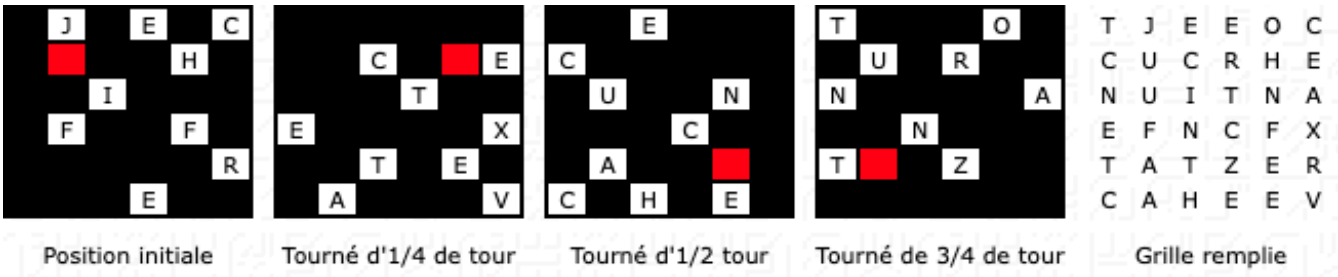
Lien du git :

https://github.com/FlooneClife/musee-securise-virtuel

Décrire un état de l'art des méthodes de chiffrement d'images par permutation.

1) Méthode 1 - Grille tournante :

Cette méthode utilise une grille, recouverte par un cache que l'on fait tourner.
Exemple : une grille 6x6 et un cache avec 9 trous.
Message = "JE CHIFFRE CE TEXTE AVEC UN CACHE TOURNANT Z".
On pose le cache sur la grille vide, puis on remplit les cases avec les 9 premières lettres du message (la case rouge sert de repère pour voir comment le cache tourne).
On tourne ensuite le cache d'un quart de tour, on écrit les 9 lettres suivantes du message etc...



On obtient une grille remplie de lettres dans un ordre incompréhensible.

2) Méthode 2 - Échange d'indice des symboles :
Cette méthode permet d'échanger par groupe l'ordre des symboles à partir d'une clé.
Exemple : Clé = (2,4,1,3)
--> La 1ère lettre est échangée avec la 2ème ;
--> La 2ème lettre est échangée avec la 4ème ;
--> La 3ème lettre est échangée avec la 1ère ;
--> La 4ème lettre est échangée avec la 3ème.
Ce procédé est répété pour chaque groupe de taille 4 jusqu'à la fin du message.

3) Méthode 3 - Permutation de colonne (transposition rectangulaire) :
Le message est représenté sous la forme d'un tableau d'une largeur et d'une hauteur définie par la taille de la clé et du message. Le principe est de chiffrer le message en ré-écrivant les colonnes dans l'ordre indiqué par la clé. Les cases vides du tableau sont remplies si nécessaire.

Exemple : Clé = (2,4,1,3), Message = JExSUISxUNxMESSAGE

2	**4**	**1**	**3**
J	E	x	S
U	I	S	x
U	N	x	M
E	S	S	A
G	E	.	.

Ordonner les colonnes par ordre croissant chiffrera le message, qui deviendra :
XSXSJ UUEGS XMAEI NSE

- Sources:
  - Chiffrements:
    - https://fr.wikipedia.org/wiki/Chiffrement_par_transposition
    - https://www.apprendre-en-ligne.net/crypto/transpo/index.html
    - https://www.apprendre-en-ligne.net/crypto/transpo/tournant.html
    - https://www.dcode.fr/chiffre-transposition
    - Cours de M^{me} Puteaux (https://github.com/PaulinePuteaux/HAI918I-SecMul)
  - Réalité augmentée:
    - https://www.usenix.org/system/files/conference/soups2015/soups15-paper-andrabi.pdf (crypto et de VR)
    - https://www.sciencedirect.com/science/article/pii/S1877050915022012 (la détection de contours et tracking en AR)
    - https://www.3demotion.net/realite-augmentee-centree/
    - https://oatao.univ-toulouse.fr/7356/1/douze.pdf
    - https://hal.inria.fr/tel-02403014v2/document
    - Cours de M. Strauss (https://www.lirmm.fr/~strauss/)