جامعة مولاي إسماعيل
UNIVERSITÉ MOULAY ISMAÏL

مدرسة العلوم والتقنيات

Mini-projet

Module : Cryptographie et Sécurité informatique
Filière : Cycle d'Ingénieurs en Génie Informatique (CIGI-GL)

Instructions :

- Présentez un rapport bref mais complet de votre travail (6 pages max.)
- Remise : le code source sur CDROM.
- Date limite : 04 Decembre 2024.

Pondération : Ce projet compte pour 50% de la note finale.

A. Partie 1

L'émergence de l'internet des objets a permis le déploiement de certains services sur internet comme la vidéo conférence. Ce développement a conduit à une forte croissance du volume de flux vidéo échangés sur le réseau mondial. Cette expansion a posé un problème crucial en matière de sécurité, d'où la nécessité d'instaurer des mesures de protection adaptées. L'objectif principal de ce projet est de réaliser un crypto système hybride qui combine le crypto système basé sur les courbes elliptiques (ECC) et un algorithme de cryptage AES fondé sur la méthode de chiffrement par blocs (Block Cipher). Le projet consiste, dans un premier temps, à appliquer le processus de chiffrement AES pour protéger les images et puis, dans un second temps, de crypter la clé par le mécanisme ECC. La Figure 1 montre les étapes de décomposition de la vidéo et de Chiffrement.

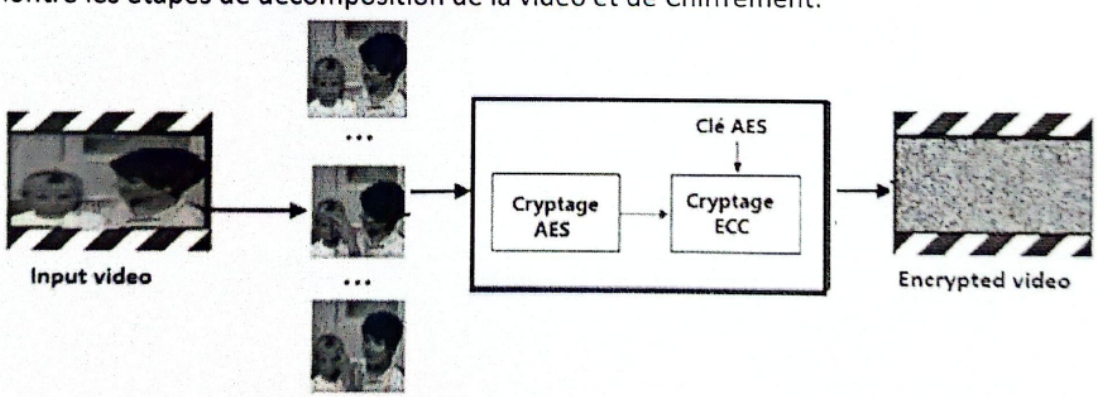

Figure 1. Processus de cryptage de la vidéo

La figure 2 illustre les images prises à différents moments de la vidéo.

Figure 2. Différent sous-images extraites

Travail à réaliser

Il vous est demandé de réaliser une application de compression et de cryptage des vidéos en utilisant l'outil informatique «**python**» :

1. Réaliser une application dotée d'une interface graphique.
2. Chargement de **la vidéo médicale**.
3. Donner les résultats de simulation (5 images médicales).
4. Décrire l'analyse de sécurité en utilisant les paramètres (PSNR, MSE et SSIM), et l'analyse de l'histogramme, de l'entropie et de corrélation.

Partie 2.

Cette partie vise à analyser la sécurité d'un protocole d'authentification basé sur les courbes elliptiques en utilisant l'outil AVISPA (Automated Validation of Internet Security Protocols and Applications). Par exemple le protocole d'authentification suivant :

Reader DB {Reader (P, s, P_S), Tag (P_t)}	Insecure channel	Tag DB {(P, t, P_t), Reader (P_S)}
Generates $r_1 \in Z_n^*$ Computes $R_1 = r_1.P$	$R1 = r1.P$ →	Generates $r_2 \in Z_n^*$ Computes $R_2 = r_2.P$ $M_1 = t.R_1 + r_2.P_S$
Checks the quantity : $M_1 \overset{?}{=} r_1.P_T + s.R_2$ If Yes, the server successfully authenticates the tag. Else, the process stop.	← $\{R_2, M_1\}$	
Calculates : $x = s \oplus r_1$ $M_2 = x.P_T + s.R_2$	M_2 →	Calculate : $x' = t \oplus r_2$ $M_2' = x'.P_S + t.R_2$ The tag checks if M_2' is equal to M_2 If Yes, the tag successfully authenticate the reader. Else, the tag stops the protocol process.

Travail à réaliser

1. Décrire le rôle de chaque entité « Reader et Tag »

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Rôle du Tag %%%%%%%%%%%%%%%%%%%
role tag(S,T:    agent,
                 Ps,Pt:    public_key,
                 SND,RCV:  channel(dy))
                        ...
```

2. Donner *l'analyse de sécurité* de ce protocole (authentification mutuelle, confidentialité, intégrité de données, Anonymat, ...)
3. Donner *l'analyse de performance* de ce protocole sous AVISPA.
   a. Calculer le cout de communication
   b. Calculer le cout de stockage
   c. Mener une étude comparative aux autres protocoles basés sur ECC.

Bon Courage