* **Diapo 1 :**

Bonjour, je suis Romain Pasquier et aujourd’hui je vais vous présenter mon TIPE qui porte sur le cryptage et le décryptage d’images en couleurs.

* **Diapo 2 :**

Tout d’abord, dans la mesure ou les entreprises échangent régulièrement des données, on s’intéresse à sécuriser ces échanges en cryptant ces fichiers.

Et pour répondre au plus de besoins, on décide de s’intéresser aux images. Car ce format permet de recouvrir un plus large choix de fichier de travail. On peut scanner un texte ou encore prendre en photo un schéma …

* **Diapo 3 :**

Alors on décidera de traiter la question suivante dans notre étude : **Comment transmettre en toute sécurité le plus de types de documents à des entreprises alliées ?**

* **Diapo 4 :**

L’objectif sera donc de :

* **Diapo 5 :**

Pour répondre à la problématique on suivra ce plan d’étude :

* **Diapo 6 :**

Remarque : Grâce à la date et à l’heure, on se déplace dans la liste des 16 premiers caractères pour en extraire 4 coefficients. On pourra (voir annexe) effectuer par la suite plusieurs actions qui vont augmenter la difficulté pour décrypter par force brut.

* **Diapo 7 :**
* **Diapo 8 :**

Remarque : A et C doivent absolument être diffèrent du modulo (condition vérifié car le minimum dans le matrice n’est pas compris.

* **Diapo 11 :**

Remarque : On observe que la colonne blanche reste une colonne blanche.

* **Diapo 12 :**

Méthode 1 :

Résoudre une équation diophantienne. Pas adapté car une perte de temps considérable pour les calculs.

Méthode 2 :

On refait un cryptage seulement sur le tableau de l’image (pour récupérer les coefficients en x, y avec une perte de temps minimale) puis on colle en i, j les pixels en x, y de notre image

Remarque : On peut appliquer cette méthode 2 car on utilise une clef fixé pour le cryptage et décryptage d’image.

* **Diapo 17 :**

Ceci montre pourquoi on observe des motifs sur notre image cryptée.

Remarque : Il serait donc « facile » de trouver la combinaison des coefficients (a, b, c, d) si on procède sur une ligne (trouver a) et sur une colonne (trouver c) jusqu’à obtenir une forme d’image « cohérente ». Pour trouver b on travaillera sur une ligne fixée et sur une colonne fixé pour d.

* **Diapo 18 :**

En étant dans la peau d’un hacker j’ai décidé de créer un code « force » brut en partant du principe qu’on avait à trouver 4 coefficients et à parcourir **TOUTE** l’image dans la mesure où on connait le résultat.

Remarque : Si on procédait comme indiqué précédemment on mettrait quand même plus de temps à la décrypter qu’avec le code source mais moins qu’avec ce code brut (on rajoute simplement une complexité de 4 fois O(min(X,Y)\*min(X,Y)), O(X) et O(Y))

Respectivement pour créer toutes les combinaisons de (a, b) et de (c, d) puis pour parcourir toute une ligne puis toute une colonne).