**Cryptographique Visuelle**

**Pascal Lafourcade et Cédric Lauradoux**

**La cryptographie permet de chiffrer des messages afin de pouvoir établir des communications sécurisées. L’objectif est que les messages échangés ne soient connus que par les personnes connaissant la clé secrète. L’objectif de cette activité est de faire découvrir la cryptographie visuelle.**

Une séance. Groupes de deux élèves.

**Objectif :**Découvrir la cryptographie visuelle et se poser la question de sa sécurité.

**Compétences travaillées :**

• Comprendre le mécanisme de chiffrement cryptographique visuelle ;

 • Déchiffrer un message chiffré avec la clé secrète ;

• Générer une clé secrète et chiffrer un message ;

Communiquer des informations sensibles en toute sécurité est l’objectif de la cryptographie. Il existe deux types de cryptographie : la cryptographie symétrique et la cryptographie asymétrique. Cette activité vise à faire découvrir une primitive de chiffrement symétrique : la cryptographie visuelle qui a été inventée en 1994 par Moni Naor et Adi Shamir dans leur article [1]. Cette technique de chiffrer simplement des images.

**Première Partie : Découverte de la cryptographie visuelle**

Les deux images ci-dessous sont proposées aux élèves. L’objectif est qu’il découvre par eux-mêmes le fonctionnement de la cryptographie visuelle. Ces images sont constituées de pixels noirs et blancs et sont a priori deux images aléatoires. Ils doivent manipuler ces images pour faire apparaître une image secrète.

**Solution**

Les élèves doivent observer ces images et s’apercevoir qu’elles ont de nombreux pixels similaires. Il est possible de noter les différences, cela peut se faire soit en coloriant les différences entre les deux images soit en les superposant. Ceci fait ainsi apparaître l’image du message secret.

Une personne qui n’a qu'une seule des deux images ne peut pas découvrir le message secret, ni même obtenir aucune information à son propos.

**Fonctionnement de l’algorithme de chiffrement**

Partant d'une image, il faut générer deux images qui semblent aléatoires, et qui révèlent l’image originelle quand elles sont superposées. L’idée de Noar et Shamir est de transformer chaque pixel de l’image de départ en quatre pixels. Ainsi, les deux images obtenues |(la clé et l’image chiffrée) seront quatre fois plus grandes, en nombre de pixels, que l'image d'origine.

Par exemple l'image de départ pour l'énigme était la suivante.

Un pixel blanc sur l'image en clair produit deux images, de taille deux pixels par deux pixels.

Pour chaque pixel blanc, une règle parmi les 6 suivantes est choisie aléatoirement. Ainsi en superposant les deux images, un pixel blanc correspond à un bloc de quatre pixels à moitié blanc.

Pour les pixels noirs, il faut choisir deux images complémentaires de manière aléatoire, afin d'obtenir un carré de quatre pixels tous noirs lors de la superposition. En faisant attention que la création des carrés de quatre pixels de chaque image comporte autant de pixels noirs que de pixels blancs. Ceci est la clé de cette construction.

**Comment être sûr que la sécurité** est garantie ?

Les règles ont pour objectif de produire deux images chiffrées qui contiennent chacune autant de pixels noirs que de pixels blancs, disposés d'une manière qui semble aléatoire sur chaque image séparément. Ainsi, une image seule ne permet de retrouver aucune information sur l'image secrète. En effet un adversaire n'est pas capable de savoir si la superposition permet d'obtenir un bloc à 50 % blanc ou un bloc noir, car les règles de génération des images sont choisies aléatoirement.

 **Deuxième Partie : Générer une clé secrète et chiffrer un message**

Dans la seconde partie de cette activité, les élèves vont créer à partir d’une image de leur choix : une clé secrète et une image chiffrée. Pour cela, ils se mettent par deux et chacun commence par dessiner une image en pixel art en noir et blanc. Par exemple d’image ci-dessous de taille 3x3 qui représente le symbole +.

BNB NNN BNB

Ensuite, ils vont générer ensemble une clé secrète partagé de taille 6x6 en choisissant aléatoirement des blocs de 4 pixels parmi les 6 possibilités suivantes :

NB NB BN BN NN BB BN NB BN NB BB NN

Par exemple une clé possible partagée entre deux élève est :

NN BB BN BB NN NB BN NB BN NB BN BN BN NB NB BN NB BN

Ensuite, chacun va avec un calque colorier le complémentaire pour obtenir le message chiffré afin d’avoir des pixels tout noir sur le + et des pixels gris sur le reste, comme suit :

NN NN BN BB BB NB NB BN NB BN NB NB BN BN NB BN BN BN

Une fois chaque élève de chaque binôme a fini de crée le message chiffré, ils se les échangent. Ainsi chacun est capable de superposer la clé pour découvrir le message secret reçu.

En continuant notre exemple, la superposition de la clé et du message chiffré laisse apparaître l’image originale suivante :

NN NN BN BB NN NB NN NN NN NN NN NN BN NN NB BN NN BN

En nettoyant les pixels gris l’image de départ apparaît nettement.

**Variantes :**

Une variante intéressante de cryptographie visuelle implique l'utilisation d'images leurres : les images chiffrées ne sont pas aléatoires, mais elles correspondent à des images. Il y a dans ce cas trois images de départ : deux images leurres et une image secrète, de même dimension. Sur chacune des deux images chiffrées, le dessin de l'une des images leurres est reconnaissable et en les superposant, c'est l'image secrète qui apparaît.

Pour cela, l'idée générale est qu'un pixel blanc de l'image secrète correspond à un bloc de quatre pixels à 75 % noirs sur les images superposées tandis qu'un pixel noir de l'image secrète correspond à un bloc de quatre pixels complètement noirs. Un pixel blanc d'une image leurre correspond à un bloc de quatre pixels à 50% noirs sur l'image chiffrée produite, tandis qu'un pixel noir d'une image leurre correspond à un bloc de quatre pixels à 75% noirs sur l'image chiffrée produite. Pour chaque pixel de l'image secrète, il y a huit cas à considérer, selon la valeur de ce pixel et celle des pixels correspondants sur les images leurres.

Une autre variante de la cryptographie visuelle permet de produire n images chiffrées, de telle sorte que la superposition d'au moins p images parmi les n images montre l'image secrète. Toutefois, les images générées sont alors très grandes, et la perte de contraste est elle aussi très grande.

**Conclusion**

Cette activité permet de comprendre le principe de chiffrement symétrique où il faut avoir une clé secrète partagée entre les deux personnes souhaitant communiquer. Elle permet aussi de présenter la cryptographie visuelle. Afin de créer facilement des images un générateur est disponible en ligne [2] pour vos activités.

**Adaptation**

* Au cycle 2 cette activité est possible sur des petites images de taille 3x3.
* Au collège, il es possible de faire des images plus grosses.
* Pour des lycéens, il est envisageable de coder ces algorithmes de chiffrement, déchiffrement et génération des clés en Python.

**RÉFÉRENCES**

[1] Moni Naor and Adi Shamir. Visual cryptography. In Advances in Cryptology EUROCRYPT’94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May9-12, 1994, Proceedings, volume 950 of Lecture Notes in Computer Science, pages 1–12. Springer, 1994.

[2] Site de génération