11/11/2018

**Elaborer un algorithme de transmission sécurisée d’informations**



Votre carrière commence ici.

89 quai des Chartrons, 33300 Bordeaux

LY Steven ; ILUNGA KILUMBU A MUTEB Amos

Ynov

# Abstract

To establish a secure transmission protocol, we used cryptographic methods as well as steganography. These methods have been used since ancient times, as we know from Jules Caesar's famous code of simply shifting the letters of the alphabet by a fixed amount. In the same way the writing with the lemon juice makes it possible to hide the message and to make it appear only in presence of flame. Therefore, these secure transmissions are mainly useful and used in wartime and require a huge investment to be able to encrypt or decrypt. The goal is for one to transmit the message without anyone else than the recipient can understand it and while for the other way he must do everything to understand the coded message. We can speak here of a war of information. Today, at a time when technology is at the peak of its time and huge amounts of data are circulating around the world, it is our duty to develop an algorithm for the secure transmission of the most reliable information possible. As a result, we used the RSA algorithm to code our message and then camouflaged it using the LSB: Least Significant Bit method, thus making the message the most difficult to decipher.

# Introduction

Les messages codés ont toujours joué un rôle important dans les communications en temps de guerre. Le fait de devoir connaître la clé pour résoudre le message chiffré empêchait toute trace de fuite d’information par d’éventuels espions et seuls les véritables destinataires pouvaient connaître la réelle signification des messages codés. De nombreuses personnes se sont penchées sur ces méthodes de chiffrage quel que soit l’époque. En effet, on note des procédés marquants et inimaginables comme le fait de faire avaler à leurs messagers des boulettes de cire contenant le message et de les envoyer au destinataire. Cependant les messages peuvent être décryptées par d’autres potentielles personnes douées pour comprendre les différentes méthodes de chiffrage. On parle aujourd’hui d’hacker, des personnes qui peuvent chercher à accéder aux données confidentiel et importantes. Ainsi il est de notre devoir de mettre en place un protocole de sécurisation des données à envoyer et aussi de récupération afin de les transmettre aux partenaires de Ynov. On va pour ce faire explorer le domaine de la cryptographie ainsi que la stéganographie.

# Chapitre I. LA CRYPTOGRAPHIE

## 1.Définition

La cryptographie est un terme qui désigne l’ensemble des techniques qui permet de chiffrer des messages d’une part incompréhensible nécessitant généralement une clé de déchiffrement pour pouvoir le lire comme l’auteur du message aurait voulu le transmettre. Les hommes dansants de Conan Doyle écrivain britannique et célèbre auteur du détective Sherlock Holmes confronte notre héros à des messages chiffrés par des dessins d’hommes qui est un véritable exemple de la cryptographie.

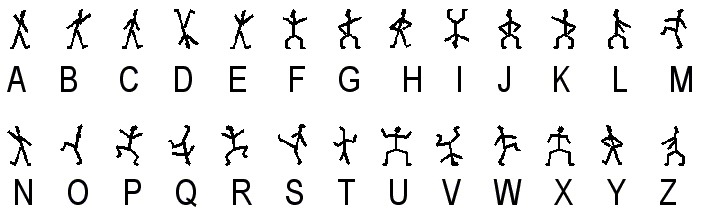


Figure 1 Les hommes dansants

Ainsi la cryptographie peut être adopté avec des symboles en forme de bonhommes appelés stickmen qui représentent chacune une lettre de l’alphabet. Il est clair que sans le code de la Figure 1 Les hommes dansants, la plupart des personnes ne verront que de simples dessins d’enfants alors qu’il ne résulte en fait qu’un véritable message caché. La cryptographie peut fonctionner avec des symboles mais nous allons nous intéresser à des notions mathématiques pour notre système informatique au sein de l’entreprise Ynov.

## 2.Méthode de cryptographie

### 2.1. Source de la méthode

Dans le jeu vidéo Zero Escape Virtue’s Last Reward, nos personnages sont confrontés à un message codé qui convient parfaitement à la cryptographie :

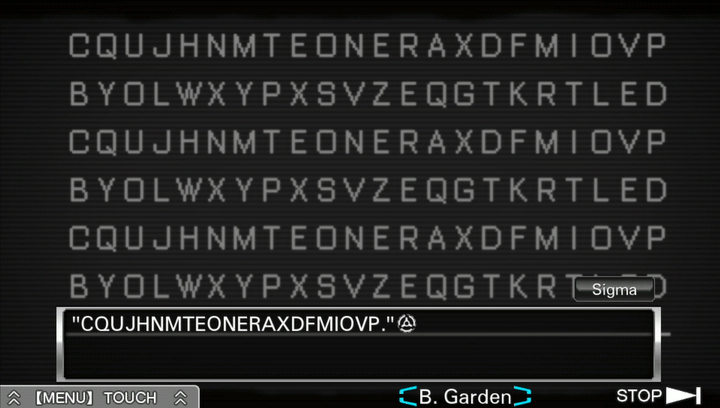


Figure 2 Code du jeu VLR

Pour résoudre ce code le personnage principal doit trouver la clé qui est :  
***78153 61098 83809 42419 90551***

On effectue ensuite la factorisation entière en nombres premiers de la clé et on obtient la clé secrète : ***198449351*** *puissances* ***3.*** Enfin il ne reste plus qu’à déchiffrer le message en décalant par la droite et en inscrivant la lettre par le chiffre correspondant : ***COMPLETED***

Il est extrêmement difficile de trouver la factorisation entière en nombres premiers de la clé de ce fait elle a été calculée par un personnage extraordinairement doué en mathématique. La complexité de ce code est particulièrement intéressante et nous allons ainsi l’étudier comme base de notre code au sein de l’entreprise Ynov.

### 2.2. L’algorithme RSA

Le système RSA est créé en 1977 par 3 mathématiciens qui ont chacun donnés leurs initiales dans leur œuvre : Ron **R**ivest, Adi **S**hamir et Len **A**dleman. Ce système est aujourd’hui un système universel qui est employé partout dans le monde que ce soit par internet ou les entreprises, c’est donc un système parfait pour le nôtre.

L’algorithme RSA est basé sur un résultat d’arithmétique avec les nombres premiers qui sont mis en avant. Les nombres premiers ne sont divisible que par eux-mêmes et par un. De ce fait il en existe une infinité {2,3,5…*198449351…*}

On dit que **p** est un diviseur du nombre entier **n** s’il existe un nombre entier **q** tel que   
Deux nombres entiers p et q sont dits premiers entre eux si le plus grand entier divisant à la fois **p** et **q** est 1. D’après le théorème de Bezout :   
*les entiers a et b sont premiers entre eux (si et) seulement si l'équation admet des solutions.*  
Donc il existe deux nombres entiers relatifs (l’un positif, l’autre négatif) **m** et **n** tels que

**Théorème.** Soient p et q deux nombres premiers, et posons   
Soit e est un entier premier avec, alors il existe un entier d > 0 et un entier m tels que .

On note le nombre a élevé à la puissance k, c’est-à-dire le nombre a multiplié par lui-même k-1 fois.

Pour tout entier a < n premier avec n, le reste de la division de par n est égal à a.

### 2.3. Notre message codé

A l’aide du théorème RSA nous allons élaborer notre code :

On choisit les deux nombres premiers **p** et **q** tel que p=11 et q=23

On calcule alors donc

On choisit e un entier premier avec donc   
On prend **e=7**  
. On recherche ensuite la clé secrète d en posant **m=2**

Notre clé secrète est donc **d=63**

La particularité de ce code c’est qu’il peut être chiffré par n’importe qui, mais déchiffrer par seulement ceux qui possède la clé secrète.

On établit un tableau avec des valeurs pour chacun des nombres.

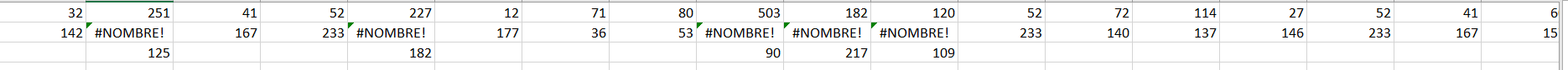
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A = 01 | B = 02 | C = 03 | D = 04 | E = 05 | F = 06 | G = 07 | H = 08 | I = 09 | J = 10 |
| K = 11 | L = 12 | M = 13 | N = 14 | O = 15 | P = 16 | Q = 17 | R = 18 | S = 19 | T = 20 |
| U = 21 | V = 22 | W = 23 | X = 24 | Y = 25 | Z = 26 | = 27 | , = 28 | . = 29 | : = 30 |
| ! = 31 | « = 32 | » = 33 |  |  |  |  |  |  |  |

Tableau 1 Tableau des valeurs

On veut coder le message : **« YNOV A RECRUTE UN EXPERT ! »**

On a ainsi le code : 32 25 14 15 22 27 01 27 18 05 03 18 21 20 05 27 21 14 27 05 24 16 05 18 20 27 31 33

On regroupe ce nombre en tranches de chiffres **strictement inférieurs à** **n = 253**:  
32 251 41 52 227 012 71 80 503 182 120 052 72 114 27 052 41 60 51 82 027 31 33

Ensuite on élève ces groupes de nombres par **e=7** puis on divise par **n=253** en gardant le reste tout en rajoutant des 0 à gauche pour avoir des nombres à **3 chiffres** :

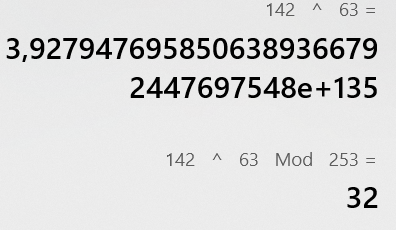
On privilégie les calculs avec l’ordinateur et des logiciels tel que Excel mais on remarque que les nombres sont tellement grand que le logiciel ne peut pas calculer, ce qui est un bon point pour la sécurité du code. On fait les calculs que Excel n’a pas réussi à calculer à la main avec la calculatrice.

On obtient en chiffrer :  
142 125 167 233 182 177 036 053 090 217 109 233 140 137 146 233 167 157 017 124 146 081 198

Notre code à déchiffrer est donc :

142125167233182177036053090217109233140137146233167157017124146081198  
Un chiffre très long et incompréhensible si on essaie de le déchiffrer, la seule solution pour réussir à le lire est d’utiliser la clé secrète que l’on possède d=63.

On regroupe ce nombre en groupe de 3 chiffres puis on élève chaque groupe par la clé secrète qui est 63.

  
Avec Excel tous les nombres obtenus contiennent des erreurs dû à un nombre trop grand, en effet les nombres vont jusqu’à e+135 ce qui est juste immense. On devra ainsi calculer à la calculatrice un par un tous les nombres à déchiffrer et retrouver le message de base. Ce qui prouve que c’est un ensemble bijectif.

Ainsi au sein de l’entreprise Ynov on donnera aux personnes importantes et fiable la clé secrète d=63 puis on pourra laisser public Tableau 1 Tableau des valeurs et e=7 pour laisser les personnes chiffrés leurs messages.

## 3.Bilan de la cryptographie

La cryptographie apporte de nombreux avantages pour faire passer des messages tout en laissant aux autres personnes un simple message incompréhensible. De ce fait sans connaître la clé pour déchiffrer les messages il est impossible de connaître le véritable message. Mais il n’est pas impossible de chercher de nous-même la clé par nos propres moyens. Figure 1 Les hommes dansants peut être trouver en analysant les messages codés et en faisant un lien entre eux, ce qu’a pu réussir le détective Sherlock Holmes. Figure 2 Code du jeu VLR a pu être déchiffrer grâce à une mathématicienne en trouvant la factorisation entière en nombres premiers de la clé. Et notre code que l’on a créé peut lui aussi être trouver en factorisant le nombre n ou élevant les groupes de nombres un par un et de vérifier si le message est compréhensible. La personne devra faire ce processus jusqu’à notre clé qui est 63, ce qui est très long à faire, de plus il faudrait un logiciel plus performant que Excel pour pouvoir élever le nombre et calculer le reste. On envisage ainsi de changer la clé avec des nombres plus grands pour pouvoir rendre le code pratiquement impossible à hacker.

# Chapitre II. LA STEGANOGRAPHIE INFORMATIQUE

## 1.Définition

La stéganographie est l’art de camoufler un message dans un objet qui paraît juste normal. Cette méthode existe depuis de nombreuses années allant même jusqu’à l’Antiquité. En effet, l’homme a comme particularité de communiquer avec ses semblables mais parfois il ne veut pas que cela se sache par les autres. Il a donc usé de nombreux stratagèmes pour dissimuler le message qu’il veut transmettre à son destinataire. Les rois dans l’Antiquité faisaient raser les cheveux de leurs esclaves pour y inscrire sur leurs crânes le message qu’ils voulaient transmettre et attendre que les cheveux repoussent pour les envoyer comme message humain. De même on pouvait écrire avec le jus de citron pour y inscrire dans une lettre banale l’heure de la date d’évasion sans que personne puisse se douter de quelque chose puisque le message n’apparaissait qu’avec la chaleur des flammes.

Le monde de l’informatique a connu un essor fulgurant avec d’immense données qui s’échangent partout dans le monde. De ce fait la stéganographie est redevenue un sujet à la mode avec de nombreuses innovations pour camoufler ces échangent aux yeux des autres. Il est donc devenu courant de glisser dans quelques bits discrets d’une image, des textes et des programmes sans que personne sans aperçoivent. Il existe de nombreux moyens de camoufler les informations des plus simples aux plus compliqués.

Pour la stéganographie moderne où dorénavant tout est informatisé, il existe une méthode qui permet la **dissimulation des informations** dans les fichiers multimédias, particulièrement les images. Cette méthode va nous permettre d’échanger avec notre correspondant via internet, des réseaux sociaux, des périphériques de stockage ou tout autre media des messages « secrets » qui passeront inaperçu pour les autres. Nous allons donc nous intéresser aux notions de pixel d'une image qui est représenté par 3 nombres compris entre 0 et 255 : R représente l'intensité du rouge, G celle du vert, B celle du bleu. Ces nombres s'écrivent comme suite de 8 bits (écriture en base 2 avec 8 chiffres).

## 2.Méthode de la stéganographie

Dans notre cas, la méthode de la stéganographie interviendra au niveau du message crypté obtenu dans la première partie de notre travail, c’est à dire **142 125 167 233 182 177 036 053 090 217 109 233 140 137 146 233 167 157 017 124 146 081 198,** et donc nous allons trouver la correspondance de chaque nombre précédant en binaire dans le Tableau 1 Tableau des valeurs mais il faut avant cela le déchiffrer avec la méthode de la cryptographie communiquée dans le chapitre 1.

**142** : 8E : 1000 1110; **125**: 7D : 0111 1101; **167**: A7 : 1010 1101; **233**: E9 : 1110 1001  
**182** : B6 : 1011 0110; **177**: B1 : 1011 0001;  **036**: 24 : 0010 0100; **053**: 35 : 0011 0101  
**090** : 5A : 0101 1010;  **217**: D9 : 1101 1001; **109**: 6D : 0110 1101; **233**: E9 : 1110 1001  
**140** : 8C : 1000 1001; **137**: 89 : 1000 1100; **146**: 92 : 1001 0010; **233**: E9 : 1110 1001  
**167** : A7 : 1010 0111; **157**: 9D : 1001 1001; **017**: 11 : 0001 0001; **124**: 7C : 0111 1100  
**146** : 92 : 1001 0010; **081**: 51 : 0101 0001; **198**: C6 : 1100 0110

Dans la seconde partie, nous allons prendre un tableau noir-blanc ci-dessous où nous allons mettre notre message sans que cela ne soit remarquable. Chaque cellule sur l’image est codée sur 1 octet. Pour les cellules en couleur blanches nous avons une suite de 8 bits codé sur 1 ce qui correspond à une valeur de 255 en décimal : blanc =**11111111** ; et pour les cellules en noir elles sont toutes codés à 0, ce qui correspond aussi à 0 en décimal ; noir=**00000000.** Ci-dessous le tableau en noir et blanc correspondant à notre image :

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

Tableau 2 image noir-blanc

Dans la dernière partie de notre travail, comme cela a été expliqué dans l’introduction de la méthode de la stéganographie, nous allons changer les deux derniers bits de chaque cellule par les valeurs binaires trouvé après la correspondance des nombres. Cela étant déjà fait dans la 2ème partie de la sténographie. L’image aura été modifié sur les dernier bits mais l’œil humain ne verra aucune différence avec la modification des deux derniers bits et sera toujours vu comme l’image Tableau 2 image noir-blanc.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 111111**10** | 000000**00** | 111111**11** | 111111**10** | 111111**01** | 111111**11** | 111111**11** | 111111**01** | 111111**10** | 000000**10** | 111111**01** |
| 000000**11** | 111111**11** | 111111**10** | 111111**10** | 111111**01** | 000000**10** | 111111**11** | 111111**01** | 000000**10** | 111111**10** | 000000**11** |
| 111111**00** | 000000**01** | 111111**00** | 000000**10** | 111111**01** | 111111**00** | 000000**00** | 111111**11** | 111111**01** | 111111**01** | 111111**01** |
| 111111**01** | 111111**10** | 111111**10** | 000000**11** | 111111**01** | 111111**10** | 111111**01** | 000000**01** | 111111**10** | 111111**11** | 111111**01** |
| 111111**11** | 111111**10** | 000000**10** | 111111**01** | 111111**10** | 111111**00** | 111111**11** | 111111**00** | 000000**10** | 111111**00** | 111111**10** |
| 111111**01** | 111111**10** | 111111**01** | 000000**00** | 111111**10** | 111111**11** | 111111**10** | 000000**10** | 111111**01** | 111111**10** | 111111**10** |
| 111111**01** | 111111**11** | 111111**10** | 111111**01** | 000000**10** | 111111**01** | 000000**00** | 111111**01** | 111111**00** | 000000**01** | 111111**01** |
| 000000**11** | 111111**11** | 000000**00** | 111111**10** | 111111**01** | 000000**00** | 111111**10** | 111111**01** | 111111**01** | 111111**00** | 000000**01** |
| 111111**11** | 000000**00** | 111111**01** | 111111**10** | 111111**11** | 111111**11** | 111111**11** | 111111**11** | 111111**11** | 000000**00** | 111111**11** |

Tableau 3 : message codé

Pour retrouver le message, la personne devra prendre les deux derniers bits de chaque cellule et les regroupés par groupe de 8 bits afin de retrouver la correspondance décimale et ensuite il faudra qu’il ait la clé pour déchiffrer le message caché par la méthode de la cryptographie vu dans la première partie. Un exemple : pour la première cellule nous avons le nombre codé suivant : 111111**10**, pour la seconde nous avons 000000**00**, la troisième 111111**11**, et la quatrième 111111**10**. En associant les deux derniers bits de chaque cellule, nous avons le code binaire : **10001110** qui correspond à 142 en valeur décimale.

3. Bilan de la stéganographie

La méthode utilisée repose ici sur l’usage de bits de poids faible (**Least Significant Bit, LSB**) d’une image. Cette méthode consiste à modifier le bit de poids faible des pixels codant l’image qui n’influe pas énormément dans la valeur du pixel, il est en effet quasiment insignifiant. On code la couleur d’une image numérique à l’aide d’un triplet d’octets qui représente une suite de pixels, par exemple pour une couleur **RGB (Red Green Blue)** sur 24 bits, chaque octet indique en binaire l’intensité de la couleur correspondante : rouge, vert ou bleu. Cependant, dans notre cas nous aurons des pixels en noir et blanc (image noir-blanc) afin que cela nous permet pour chaque pixel d’obtenir une valeur d**’octet.** Il est impossible, à l'œil, de distinguer l'image qui cache le message, et l'image initiale. Si on devait présenter l’image comportant le message et l’image initial, on ne verrait aucune différence.

La stéganographie est exploitable dans de nombreux domaines et est semblable à de la magie qui cache quelque chose qui est en fait toujours présent depuis le début. La méthode LSB comporte de nombreux avantages pour rendre la photo la plus normal possible. Personne ne pourrait se douter de la présence quelconque de modification des derniers bits sur les pixels. Cependant il est très simple de vérifier les pixels des images et découvrir le message caché. Il est envisageable dans le futur d’utiliser une autre méthode au sein de l’entreprise Ynov.

## CONCLUSION

Nous avons dans ce rapport établit un système de transmission sécurisé combinant la cryptographie et la stéganographie. Ainsi nous avons utilisé l’algorithme RSA pour définir notre message codé et la clé pour le déchiffrer puis nous avons dissimulé ce message dans une image avec la technique du Least Significant Bit qui consiste à changer les deux bits de poids faible dans chaque pixel de l’image en noir et blanc. L’utilisation de cette méthode de la cryptographie associée à la stéganographie a pour effet d’améliorer considérablement la sécurité de la phase de communication, d’avoir une uniformité de l’information tant chez l’expéditeur que chez le destinateur direct du message au travers d'une clé et de la méthode de déchiffrement. Enfin cela permet de rendre totalement inaperçu l’information codé dans l’image.

## BIBLIOGRAPHIE

* Figure 1 Les hommes dansants: <http://matoumatheux.ac-rennes.fr/tous/crypto/dansant.htm>  
  Auteur : Arthur Conan Doyle ; Œuvre : *The Adventure of the Dancing Men,1903*
* Figure 2 Code du jeu VLR : <https://lparchive.org/Zero-Escape-Virtues-Last-Reward/Update%20119/>  
  Virtue's Last Reward ; plateformes : 3DS, PS4, PS Vita ; sortie en 2012
* Nombres premiers et cryptologie: l’Algorithme RSA: <https://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/>Auteur: Jonathan Touboul , 2007
* Table ASCII:  
  <https://fr.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange>source: Wikipédia
* Numération : <http://sitelyceejdarc.org/autodoc/cours/003%20T%20STI2D/Technologie%20transversale/steganographie/index.html?Imagenumrique.html>   
  Auteur: P.HOARAU, 2013