Cryptolog

(Unité pédagogique de Cryptographie)

Préparé et réalisé par :
Ramy Chemak

I Cadre du projet

Dans le cadre de l'exposition scientifique internationale 2015 (ESI 2015), en tant que membre de la section informatique de l'association Jeunes-Science de Tunisie (AJST), je présente ce modeste logiciel de Cryptage\Décryptage en tant que projet scientifique réalisé par M. Ramy Chemak et afin de participer à l'ESI 2015 et exporter l'activité de l'AJST vers le public national et international. Ce projet vise à rapprocher la culture des projets aux jeunes adhérents, et les inspirer pour qu'ils puissent réaliser d'autres exploits encore meilleurs.

II Présentation générale du projet

Ce projet sous forme d'un logiciel de Cryptage\Décryptage est destiné au grand public. Il comprend plusieurs programmes exploitables, simples et faciles à utiliser. Il permet la réalisation de certaines formes de cryptage usuelles et souvent utilisées, tout en simplifiant le principe de la tâche pour l'utilisateur afin de vulgariser la culture de la sécurité informatique et forcer le barrage séparant les gens de toutes formes d'écriture chiffrée.

III Buts du projet

- Faciliter la compréhension des textes en formats assez compliqués ou la conversion des chaînes de caractères en ces formats.
- Faciliter le cryptage des textes par certaines méthodes de cryptage usuelles (César, affine, ...).
- Offrir une simple plateforme de cryptographie et de sténographie.
- Faciliter la compréhension de certains codes souvent utilisés (code RVB, code hexadécimal, caractères spéciaux, ...).
- Vulgariser la culture de la sécurité informatique.
- Simplifier le principe de chiffrage aux gens en leur expliquant les méthodes de cryptage.

IV Description du projet

1. Aspect générale

Le projet se présente sous la forme d'un logiciel comportant plusieurs modules (ou programmes) présentant les différents services qu'ils offrent.

L'utilisateur peut choisir le service dont il veut se bénéficier, et le logiciel lui répond à ses besoins tout en simplifiant la tâche pour l'utilisateur.

Le programme permet à l'utilisateur de comprendre l'algorithme de chaque système de cryptage.

2. Catégorisation des programmes

✓ ***Tableur de codes usuels:***

- Code couleur RVB
- Code couleur hexadécimales
- Code caractères spéciaux

✓ ***Convertisseur de langues:***

- Convertisseur codage binaire
- Convertisseur code Morse

✓ ***Cryptage\Décryptage:***

- Cryptage César
- Cryptage Affine
- Cryptage Vigenère
- Cryptage Hill
- Cryptage RSA
- Stéganographie

✓ ***Hashage:***

- Hashage SHA1
- Hashage SHA-224
- Hashage SHA-256
- Hashage SHA-384
- Hashage SHA-512
- Hashage MD5

3. Description des programmes

✓ ***Code couleur RVB:***

Ce programme affiche la couleur correspondante à un code RVB donné, et vice versa.

✓ ***Code couleur hexadécimale:***

Ce programme affiche la couleur correspondante à un code hexadécimal donné, et vice versa.

✓ ***Code caractères spéciaux:***
Ce programme liste les différents caractères spéciaux (lettres spéciaux, lettres grecques, devises, symboles scientifiques ...) et affiche leurs encodage HTML correspondant, et vice versa.

✓ ***Convertisseur codage binaire:***
Ce programme permet de déchiffrer un code binaire saisi par l'utilisateur et l'afficher sous forme de texte clair, et vice versa.

✓ ***Convertisseur code Morse:***
Ce programme permet de déchiffrer un code Morse sous forme binaire (0 pour un signal nul et 1 pour un signal actif) saisi par l'utilisateur et l'afficher sous forme de texte clair, et vice versa.

✓ ***Cryptage César:***
Ce programme permet de crypter\décrypter un texte\cryptogramme donné à l'aide d'une clé de chiffrement\déchiffrement donné par l'utilisateur par la méthode de cryptage César.

✓ ***Cryptage Affine:***
Ce programme permet de crypter\décrypter un texte\cryptogramme donné à l'aide d'une clé de chiffrement\déchiffrement donné par l'utilisateur par la méthode de cryptage Affine.

✓ ***Cryptage Vigenère:***
Ce programme permet de crypter\décrypter un texte\cryptogramme donné à l'aide d'une clé de chiffrement\déchiffrement donné par l'utilisateur par la méthode de cryptage Vigenère.

✓ ***Cryptage Hill:***
Ce programme permet de crypter\décrypter un texte\cryptogramme donné à l'aide d'une clé de chiffrement\déchiffrement donné par l'utilisateur par la méthode de Hill.

✓ ***Cryptage RSA:***
Ce programme permet de crypter\décrypter un texte\cryptogramme donné à l'aide d'une clé de chiffrement\déchiffrement donné par l'utilisateur par la méthode RSA.

✓ ***Stéganographie:***
Ce programme permet de crypter un texte donné dans une image non-cryptée donnée, ou décrypter une image cryptée donnée et afficher le texte qu'elle contient.

✓ ***Hashage:***
Ce programme permet de signer un texte saisi par l'utilisateur à l'aide d'un ou plusieurs des systèmes de hashage disponibles.