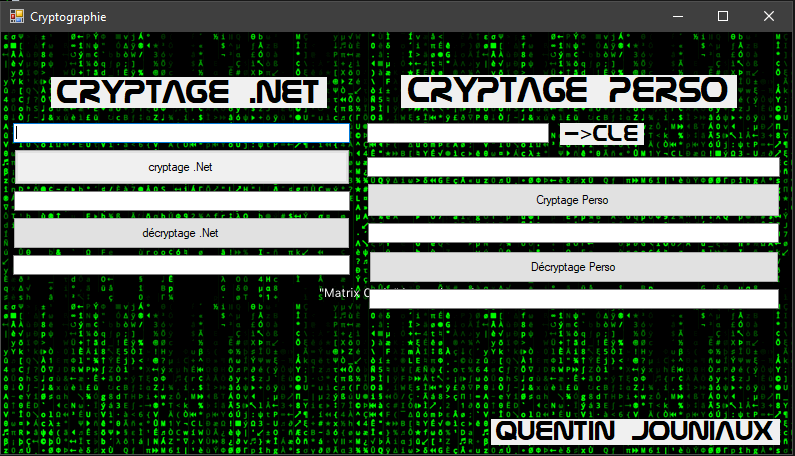
2021/2022

Quentin JOUNIAUX

2IS

Cryptographie

Système d’exploitation-Laboratoire



# Explication du l’interface

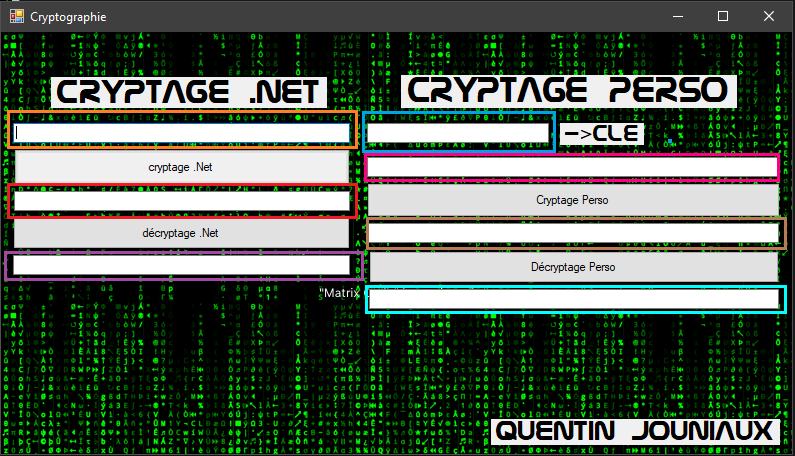


Figure 1 Interface

* Champ pour le texte en claire avant un cryptage en .Net
* Champ pour le texte crypter en .Net
* Champ pour le texte en claire après un cryptage en. Net
* Champ pour la clé de cryptage du cryptage personnel
* Champ pour le texte en claire avant un cryptage personnel
* Champ pour le texte crypter en personnel
* Champ pour le texte en claire après un cryptage personnel

# Cryptage .Net

## Explication

Pour le cryptage .Net j’ai choisi le cryptage RSA qui est un cryptage a clés asymétrique ou publique. La cryptographie à clé publique utilise deux clés pour le cryptage : une clé publique pour crypter les données et une clé privée pour les décrypter. On peut ainsi publier la clé publique tout en conservant la clé privée secrète. D’un point de vue informatique, il est impossible en un temps raisonnable de deviner la clé privée à partir de la clé publique. Un utilisateur qui possède une clé publique peut donc crypter des informations mais est dans l’impossibilité de les décrypter. Seule la personne disposant de la clé privée correspondante peut décrypter ces informations. Cette méthode présente un très gros avantage : elle permet d’échanger des messages de manière sécurisée sans aucun dispositif de sécurité. L’expéditeur et le destinataire n’ont plus besoin de partager des clés secrètes par une voie de transmission sécurisée car les communications impliquent uniquement l’utilisation de clés publiques. Aucune clé privée n’est transmise ou partagée.

|  |  |
| --- | --- |
| Avantages | Inconvénients |
| Très puissant et sûre | Beaucoup plus lent que les cryptages symétriques |
| Le chiffrement asymétrique prend en charge la signature numérique qui authentifie l’identité du destinataire => garantit que le message n’est pas altéré pendant son transit. | Le progrès des algorithmes impose des clés de taille élevée |
| Ne force pas l’utilisateur à communiquer des clés | Les 2 interlocuteurs doivent avoir les 2 clés pour pouvoir communiquer |
|  | En cas de perte de la clés privé = impossible de décrypter |

Le choix du type de cryptage dépendra de l’utilisation que l’on en fait. On utilisera un chiffrement symétrique quand on veut envoyer rapidement un message mais on utilisera un chiffrement asymétrique quand on veut être sûr de sa sécurité et qu’on ne veut pas prendre de risque.

## Code

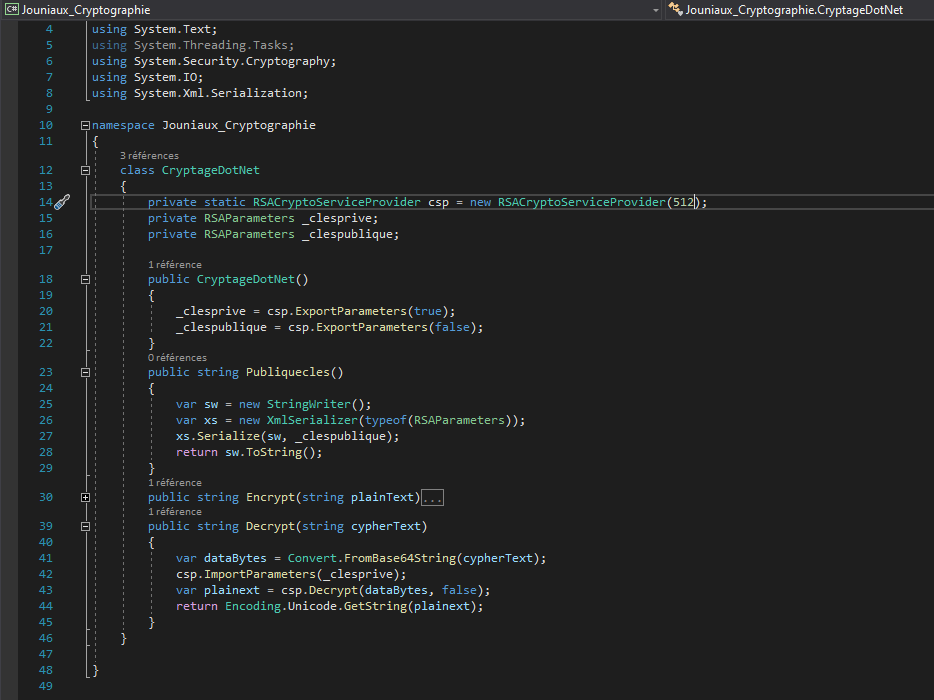


Figure 2 Code de la classe Cryptage .Net

# Cryptage personnel

## Explication

Pour mon cryptage personnel j’ai choisi un chiffrement par le chiffre de Vigenère amélioré. C’est un chiffrement dit polyalphabétique c’est-à-dire qu’une même lettre va être codé différemment en fonction de sa position dans le texte tout ça déterminer par une clé.

Le principe du chiffrement de Vigenère est en fait très simple. On utilise un tableau, qui peut être réécrit par cœur facilement. Ce tableau est bi-dimensionnel et comporte en X et en Y les lettres de l’alphabet (dans mon cas il comprend 65536 caractères donc un tableau de 65536x65536). En X, les lettres sont celles du texte en clair, en Y les lettres sont celles de la clé. Pour chiffrer, on commence par faire correspondre toutes les lettres du texte clair avec les lettres de la clé. Si la clé est inférieure en taille au texte en clair (ce qui est généralement le cas), on la répète autant de fois que nécessaire.

On voit que la clé est répétée autant de fois qu'il est nécessaire pour correspondre avec la taille du texte en clair. La taille de la clé est importante au niveau de la sécurité du chiffre, en effet on voit que plus la clé est courte, plus elle sera répétée. Le risque est donc pour l'attaquant de pouvoir repérer des répétitions dans le texte.

Une fois que nous avons étendu la clé à l'ensemble du texte à chiffrer, on peut chiffrer en utilisant le tableau.

Ce cryptage n’est plus considéré comme très sûre mais il a tout fois un attrait historique car il a longtemps été reconnu et utilisé.

## Code

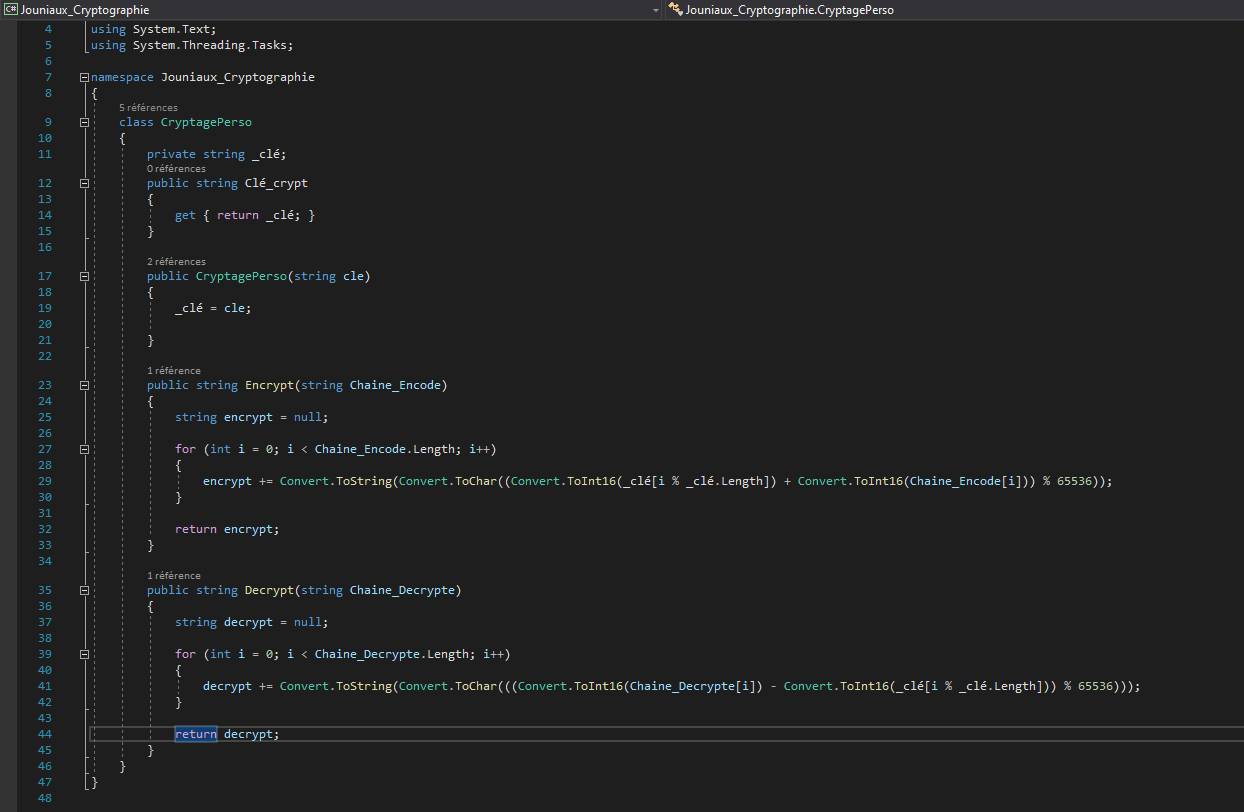


Figure 3 Code de la classe cryptage Perso

# Références

Anon., s.d. [En ligne]   
Available at: https://blog.mailfence.com/fr/difference-chiffrement-symetrique-asymetrique/  
[Accès le 11 12 2021].

Anon., s.d. [En ligne]   
Available at: https://codes-sources.commentcamarche.net/source/25294-cryptage-par-la-methode-de-vigenere  
[Accès le 12 12 2021].

Anon., s.d. [En ligne]   
Available at: https://www.youtube.com/watch?v=sYGS80-Joi8&t  
[Accès le 12 12 2021].

[Figure 1 Interface 1](#_Toc90319781)

[Figure 2 Code de la classe Cryptage .Net 2](#_Toc90319782)

[Figure 3 Code de la classe cryptage Perso 3](#_Toc90319783)