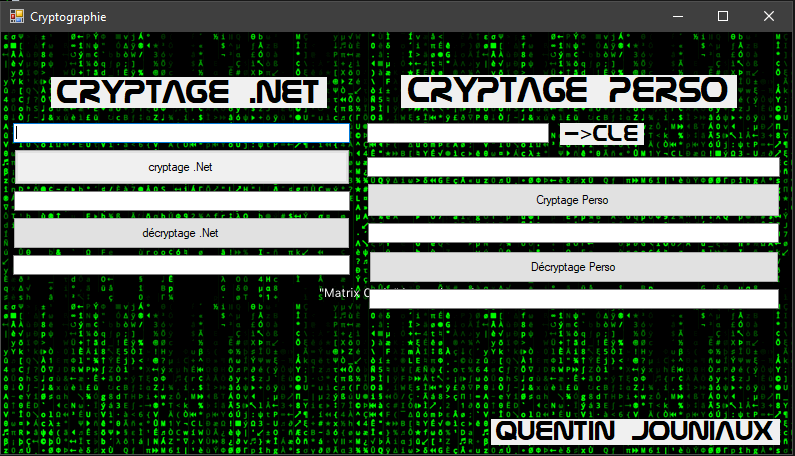
2021/2022

Quentin JOUNIAUX

2IS

Cryptographie

Système d’exploitation-Laboratoire



# Explication du l’interface

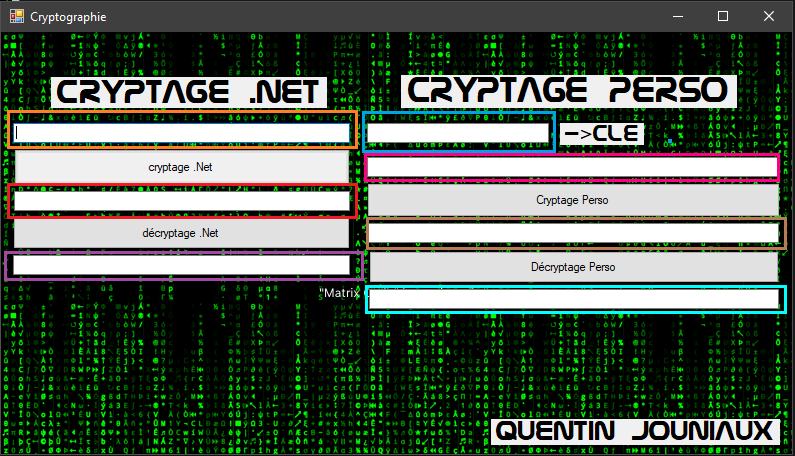


Figure 1 Interface

* 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

Pour le cryptage .Net j’ai choisi le cryptage RSA.

Le chiffrement RSA est asymétrique : il utilise une paire de clés (des nombres entiers) composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles. Les deux clés sont créées par une personne, souvent nommée par convention Alice, qui souhaite que lui soient envoyées des données confidentielles. Alice rend la clé publique accessible. Cette clé est utilisée par ses correspondants (Bob, etc.) pour chiffrer les données qui lui sont envoyées. La clé privée est quant à elle réservée à Alice, et lui permet de déchiffrer ces données. La clé privée peut aussi être utilisée par Alice pour signer une donnée qu'elle envoie, la clé publique permettant à n'importe lequel de ses correspondants de vérifier la signature.

Une condition indispensable est qu'il soit « calculatoirement impossible » de déchiffrer à l'aide de la seule clé publique, en particulier de reconstituer la clé privée à partir de la clé publique, c'est-à-dire que les moyens de calcul disponibles et les méthodes connues au moment de l'échange (et le temps que le secret doit être conservé) ne le permettent pas.