

Introduction générale

Depuis que l'homme a été créé, il vit parmi ses semblables et communique avec eux et donc ressent parfois le besoin de dissimuler des informations secrètes en les rendant illisibles car le maintien du secret est une nécessité qui offre parfois la sécurité et donc la cryptographie a toujours été parmi nous.

La cryptographie est la « science du secret », regroupe deux branches : d'une part, la cryptographie, qui permet de coder des messages, et d'autre part, la cryptanalyse, qui permet de les décoder.

La cryptographie informatique professionnelle est un phénomène récent, rendu indispensable du fait que les informations sont accessibles pratiquement à tous par des réseaux publics.

La cryptographie moderne est orientée vers la manipulation des chiffres et utilise avec abondance des résultats de l'arithmétique, établit souvent il y a longtemps et dont l'utilité pratique n'avait pas été prouvée.

L'informatique par la puissance de calcul qu'elle offre est un outil essentiel de la cryptographie moderne.

Nous sommes intéressés dans notre projet de fin d'étude par la cryptographie des textes arabes on utilise l'algorithme à clé secrète DES et l'algorithme à clé publique RSA.

Notre mémoire est structurée comme suite :

Chapitre 1 : regroupe les généralités de la cryptographie.

Chapitre 2 : présente un historique de la cryptographie arabe.

Chapitre 3 : est consacré à la présentation des principales méthodes de cryptage comme RSA et DES.

Chapitre 4 : le dernier chapitre concerne la partie développement de l'application du notre projet, qui détaille l'implémentation de l'algorithme DES et RSA pour le cryptage des textes arabe.