

Conclusion générale

La cryptographie reste encore le moyen le plus sérieux d'assurer la sécurité des correspondances, étroitement liée à l'effort de guerre, elle n'a pas cessé de se développer depuis ses origines antiques.

Les Anciens avaient déjà perçu dans cette technique quelque peu ésotérique le meilleur moyen de garantir la confidentialité de leurs missives, ils l'ont développée d'une façon simple mais efficace, l'adaptant aux divers besoins, leurs innovations nous ont été transmises soit par le concepteur lui-même (César) soit par des historiens qui en admiraient l'ingéniosité.

Au cours de ce mémoire, nous avons étudié une problématique liée à la protection des images numérique afin de sécuriser leur transfert ou leur stockage. Nous avons expliqué différents techniques de chiffrement moderne.

Notre contribution de cette étude se focalise sur la sécurisation des images numérique en utilisant une approche basée sur le cryptosystème hybride, c'est-à-dire, on utilise un algorithme de chiffrement symétrique pour protéger l'image et on sécurise la clé par un cryptosystème à clé publique.

Cette contribution prend en compte la confidentialité de l'image numérique par la minimisation du temps de chiffrement avec les algorithmes symétriques, et évalue le niveau de sécurité par le chiffrement asymétrique. Après présentation des résultats expérimentaux, on a fait une étude comparative entre les cryptosystèmes implémentés.

Perspectives

Les précédentes de sécurisation utilisées ne sont pas totalement satisfaisantes pour diverses raisons :

La combinaison entre le cryptage et le tatouage numérique, il est possible de tatouer la clé de chiffrement (clé symétrique) dans une image.

Dans le cas particulier de certains types d'images, de grandes zones homogènes apparaissent, ces zones perturbent l'efficacité des algorithmes de chiffrement, pour résoudre ce problème, il faut compresser l'image avant son chiffrement.