

Résumé

La Cryptographie est l'étude des méthodes et techniques permettant de transmettre des données de manière confidentielle. On distingue deux grands systèmes de cryptage:

- Les cryptosystèmes symétriques où la méthode de cryptage (décryptage) est connue par l'expéditeur et le destinataire.
- Les cryptosystèmes asymétriques (dit aussi à clefs publiques).

Après avoir présenté les outils algébriques nécessaires pour la construction de systèmes cryptographique on fait une étude sur les algorithmes de cryptage RSA et EL GAMAL ainsi que leurs complexités.

ملخص

قدمنا في هذه المذكرة دراسة حول خوارزميات التشفير العام وتعقيدها، والتي نذكر خلالها بعض مفاهيم وخصائص الحقول المحدودة، وأيضا نحدد نوعين من التشفير متماثل وغير متماثل كما نذكر بعض الأمثلة الخاصة بكل نوع. وفي الأخير، فإننا ندرس المفهوم العام للتشفير وبعض أنواعه، وندرس مدى تعقيد خوارزميتي التشفير الغير متماثل RSA و EL GAMAL.