2. La Cryptographie

Noureddine AZZOUZA Riadh MEGHATRIA

[1]Université Djilali BOUNAAMA Khemis Miliana, Algérie

Cours de Sécurité Informatique, M2GLSD

Plan

Introduction

1. La cryptographie est une science très ancienne. Les premières traces de chiffrement revient à environ 3000 ans avant notre ère
2. La cryptographie a été utilisée exclusivement à des fins militaires.

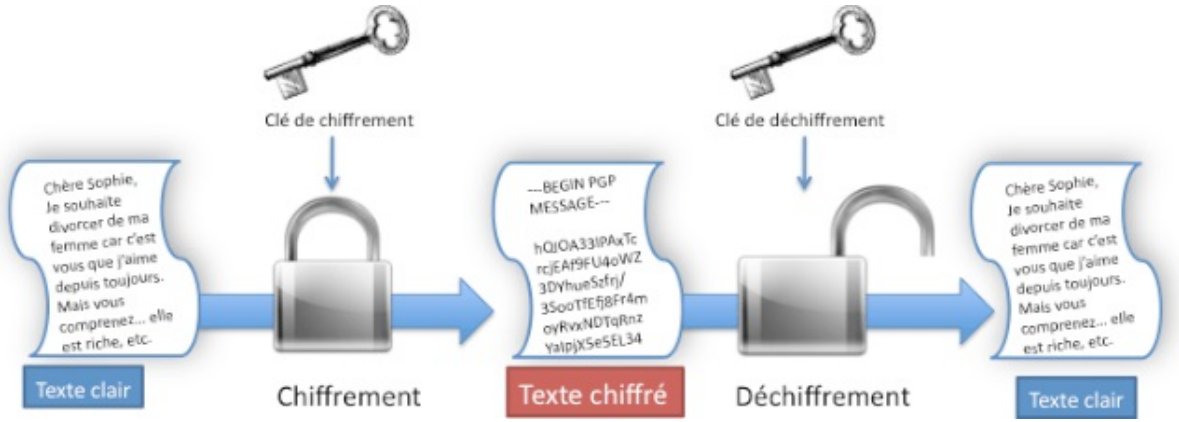
Deux manières d'envoyer des messages

- La CRYPTOGRAPHIE : rendre le message incompréhensible par l'ennemi
- La STEGANOGRAPHIE : cacher le message pour que l'ennemi ne le trouve pas.

Buts

Au Début :

- Assurer la confidentialité des communications



Aujourd'hui :

- Assurer la confidentialité, authenticité et l'intégrité des messages

Cryptographie

Définitions

1. Science visant à créer des méthodes pour sécuriser les données.
2. Exigé comme mécanisme fondamental afin d'assurer la confidentialité des informations

Origine

Mots grecs : Kruptos (caché) + Graphein (écrire)

Vocabulaire

1. Texte en clair
   - Le message à protéger (à chiffrer)
2. Texte chiffré
   - le résultat du chiffrement du texte en clair(cryptogramme)
3. Chiffrement
   - la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré
4. Déchiffrement
   - la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair
5. Clé
   - paramètre qui permet, à l'aide d'un algorithme de chiffrement, de chiffrer un message
6. Décrypter
   - Déchiffrement sans possession clé

Cryptosystème

Définition

1. algorithmes + clés

Principe d'un cryptosystème

Définitions

Cryptographie

branche regroupe l'ensemble des méthodes (algorithmes) qui permettent de chiffrer et de déchiffrer un texte en clair

Cryptanalyse

l'art de révéler les textes en clair sans connaître la clé utilisée (Raisonnement analytique et outils mathématiques)

Cryptologie

Cryptographie + cryptanalyse

Stéganographie

Art de dissimulation

Classification des Cryptosystèmes

Classification des Cryptosystèmes