# Chapitre 1 : Intro

## Vocabulaire

* Chiffrer / déchiffrer :
  + C'est, via un algorithme, rendre un message intelligible et inversement.
* Décrypter :
  + Essayer de lire un message chiffré sans en connaitre la clé.
* Cryptologie : Science des secrets
  + Cryptographie : Dissimuler un secret
    - Rendre l'information incompréhensible pour celui qui n'a pas la(es) clé(s) de chiffrement
    - e.g. : Stéganographie
      * Consiste à dissimuler l'info dans un support (sans pour autant la chiffrer)
  + Cryptanalyse : Briser le secret
    - Analyser un texte pour le décrypter
* Translation :

|  |  |
| --- | --- |
| Cryptographie | Cryptography |
| Chiffrement | Encryption |
| Déchiffrer / Décrypter | Decryption |
| Algo. de chiffrement | Cipher |
| Message dans la forme originale | Plaintext |
| Message chiffré | Ciphertext |

# Chapitre 2 : Historique

A faire plus tard

# Chapitre 3 : Les algorithmes

## 3.1 Introduction

* Principe de Kerchoffs
  + La/les clés sont plus importantes que la manière de chiffrer
  + Les algos sont publiés et on considère un algo fiable s'il n'est pas possible de le craquer en un temps record.
* NIST : National Institute of Standards and Technology
  + Sécurité dans la ou les clés, longueur minimale conseillé
* Les types d'algorithmes :
  + A clé secrète
  + A clé privée
  + Hybride

## 3.2 : Algorithme à clé secrète

* Clé de déchiffrement calculée à partir de la clé de chiffrement
* Algo. symétrique : clé identiques
* 2 Catégories
  + Chiffrement continu (bit par bit)
  + Chiffrement par bloc
* Partage de la clé entre 2 interlocuteurs
  + Pose des soucis de sécurité, car la même clé est utilisée pour déchiffrer

## 3.3 : Algorithme à clé publique

* Utilise deux clés différentes pour le chiffrement et le déchiffrement
* Il y a donc une clé publique
* C'est facile à calculer, impossible à inverser.
  + On parle de fonctions mathématiques. Si on a toutes les opérandes, le calcul est simple. Mais trouver les opérandes à partir du résultat est une tâche compliquée et trop longue. C'est un excellent argument en faveur de la sécurité.
* Le temps de calcul de la clé doit être plus long que le temps de vie de l'information
* Le déchiffrement n'est pas bêtement l'inverse du chiffrement
* Moins de clé à gérer

## 3.3 : Infos sur les clés

* La taille de la clé est primordiale
  + Clé codée sur *n* bits = 2n possibilités. C'est exponentiel.
  + Donc plus elle est longue, plus il y a de possibilités, plus le temps pour décrypter sera long
* Le système DES (1977)
  + Clé codée sur 56 bits.
* Il faut protéger cette clé :
  + Comment la protéger ?
  + Qui peut y accéder ?

## 3.4 : La signature numérique

* Confidentialité
  + Le message doit être incompréhensible pour les autres
* Intégrité
  + Le message n'a pas été falsifié ni modifié (Si modification, signature non valide)
* Authentification
  + On est certain de l'identité des personnes en contact
* Non répudiation
  + On ne peut nier que le message a été envoyé / reçu
* Concept :
  + Technique mathématique de l'authenticité et de l'intégrité d'un message, d'un logiciel, d'un document électronique.
* Contenu :
  + Information sur l'entité de l'envoyeur
  + Signature de l'entité
  + Signature de l'autorité de certification

# Chapitre 4 : DES

# Chapitre 5 : AES

# Chapitre 6 : RSA

* Basé sur la factorisation des grands nombres
* Fonction avec trappe :
  + Facile à calculer, extrêmement compliqué à inverser
* Taille de la clé conseillé en 2018 : 2048 bits

## 6.1 : Protocole :

Bob choisi 2 nombres premiers : ***p*** & ***q***

Il calcul :

* ***n*** = ***p*** \* ***q***

et

* ***phi(n)*** = (***p***-1)\*(***q***-1)