*47332 KENZOUA Florian*

# Cryptographie : un jeu d'enfant ?

Le bon fonctionnement du transport des informations numérisées repose sur la sécurité des données. Après avoir découvert la diversité de méthodes de cryptographie et son importance, j'ai voulu étudier le fonctionnement, les performances et les failles d'algorithmes à ma portée.

À l'instar des jeux pour enfants comme le jeu du Code secret, crypter ou décrypter des messages prend parfois une dimension ludique. La cryptographie permet de se lancer un défi, créer un algorithme compétitif face aux attaques, le décryptage, quant à lui, relève alors du challenge.

## Positionnement thématique (ÉTAPE 1) :

- *INFORMATIQUE (Informatique Théorique)*
- *MATHEMATIQUES (Algèbre)*

## Mots-clés (ÉTAPE 1) :

| **Mots-clés (en français)** | **Mots-clés (en anglais)** |
|---|---|
| *Cryptographie* | *Cryptography* |
| *Chiffrement asymétrique* | *Asymmetric encryption* |
| *Complexité* | *Complexity* |
| *Vulnérabilités* | *Vulnerabilities* |
| *Nombres premiers* | *Prime numbers* |

## Bibliographie commentée

La cryptographie est la science qui permet le chiffrement de nos données. En cryptographie, il existe deux méthodes de chiffrement : le chiffrement symétrique ou asymétrique [1]. La première méthode consiste à utiliser une clé publique. La seconde repose sur l'utilisation d'une clé publique à laquelle on ajoute une clé privée. L'avantage de la méthode asymétrique est d'augmenter la sécurité du transfert de données car l'expéditeur et le récepteur sont les seules personnes à connaître la clé privée. Ils sont donc les seuls à pouvoir coder et décoder les messages envoyés.

Le protocole le plus utilisé aujourd'hui, est le chiffrement RSA [2]. Il a été créé en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman et publié en 1978. Le problème du logarithme discret évoqué par Christophe Delaunay [3] met en avant les différences de fiabilité et de

complexité entre les deux méthodes de chiffrement, afin d'expliquer pourquoi le RSA est un outil efficient en cryptographie. Il est utilisé, encore aujourd'hui, car c'est un programme asymétrique, offrant un haut degré de sécurité.

Comme beaucoup de protocoles, par exemple, celui de Diffie-Hellman ou encore le crypto système de Goldwasser-Micali, le chiffrement RSA repose sur la théorie des nombres premiers : plus les nombres premiers utilisés sont importants, plus la protection engendrée par le protocole est solide. En effet, pour espérer décrypter un message à l'aide de (e, n), la clé publique, où e est premier, il faut appliquer l'algorithme de factorisation de Richard Schroeppel sur n. La complexité est alors énorme. Il est d'ailleurs possible de retrouver des listes de ces nombres premiers [4]. Il existe une course aux grands nombres premiers, c'est un enjeu majeur de la cryptographie. Des tests de primalité permettent de déterminer de grands nombres premiers [5].

Enfin, il est possible de trouver des failles au chiffrement RSA comme des méthodes de recherche de racines modulaires d'un polynôme. Ces méthodes ont été développées notamment par Don Coppersmith [6] et Nicholas Howgrave-Graham [7].

## Problématique retenue

Notre travail a pour but de répondre à la question suivante : Grand classique de la cryptographie, pourquoi le chiffrement RSA est-il si répandu ?

## Objectifs du TIPE du candidat

Afin de mener à bien notre étude, nous utiliserons le langage python pour programmer les algorithmes, déterminer et comparer leur complexité temporelle.

1. Étudier l'intérêt du chiffrement RSA, par rapport à un chiffrement symétrique, le coder.

2. Proposer des programmes informatiques pour déterminer des grands nombres premiers.

3. Exploiter des failles potentielles du chiffrement RSA et prouver son efficacité face à celles-ci.

## Références bibliographiques (ÉTAPE 1)

**[1]** HOUDA FERRADI : Initiation à la cryptographie : théorie et pratique *: 2016, https://www.di.ens.fr/~ferradi/cours.pdf*

**[2]** JEAN BERSTEL : Algorithme RSA *: 1999, https://www-igm.univ-mlv.fr/%7Eberstel/Cours/Crypto/RSA99.pdf*

**[3]** CHRISTOPHE DELAUNAY : Le « Problème du logarithme discret » en cryptographie *: 2015, https://images.math.cnrs.fr/Le-probleme-du-logarithme-discret-en-cryptographie.html?id_forum=9780*

**[4]** NOMBRES PREMIERS : Liste des nombres premiers de 0 à 50000 *: https://www.nombres-premiers.fr/liste.html*

**[5]** LATIFA ELKHATI : Tests de primalité et cryptographie *: 2002, https://www.maths.univ-evry.fr/pages_perso/bayad/Enseignement/TER/testsdeprimaliteCrypto.pdf*

**[6]** DON COPPERSMITH : Journal of Cryptology *: 1997, pages 233-260, https://link.springer.com/article/10.1007/s001459900030*

**[7]** NICHOLAS HOWGRAVE-GRAHAM : Finding Small Roots of Univariate Modular Equations Revisited *: 1997, pages 131-132, https://link.springer.com/chapter/10.1007/BFb0024458*