22273 SIMON Aloïs

La cryptanalyse du RSA

La cryptographie joue un rôle majeur dans les communications, répondant au besoin des civilisations depuis qu'elles existent : le maintien du secret. L'algorithme RSA est l'un des plus utilisés dans nos communications informatiques actuelles. C'est pourquoi j'ai décidé d'étudier celui-ci dans mon TIPE.
Les communications informatiques doivent se faire de manière sécurisée aujourd'hui, j'ai donc décidé d'étudier la façon dont sont transportées ces informations, ce qui s'inscrit dans le thème de cette année.

Positionnement thématique (phase 2)

INFORMATIQUE (Informatique Théorique), INFORMATIQUE (Informatique pratique), MATHEMATIQUES (Algèbre).

Mots-clés (phase 2)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Cryptanalyse	*Cryptanalysis*
RSA	*RSA*
Factorisation de Fermat	*Fermat's factorization method*
Attaque de Wiener	*Wiener's attack*
Sécurité	*Security*

Bibliographie commentée

La cryptographie joue un rôle majeur dans les communications. Au croisement des mathématiques et de l'informatique, elle est aujourd'hui une science à part entière, répondant au besoin du maintien du secret.

Parmi les modèles développés au cours du temps, celui du RSA, du nom de ses inventeurs (Ronald Rivest, Adi Shamir et Leonard Adleman), est réputé très sécurisé [1].

La force de cet algorithme repose principalement sur la théorie des grands nombres premiers et le fait que ce soit un chiffrement asymétrique [2]. Il faut pour réussir à appliquer l'algorithme RSA se donner deux grands nombres premiers qui serviront de base pour notre algorithme. Il est impossible d'appliquer un algorithme qui vérifie en un temps relativement court si ces nombres d'environ 500 chiffres sont premiers. On applique donc une méthode, le test de Miller-Rabin, qui vérifie si un nombre n'est pas premier ou si il est fortement probable qu'il le soit [3].

Ainsi, à partir de ces nombres on peut construire les clés de chiffrements et de déchiffrement du système RSA.

Toutefois, sous certains critères, ce chiffrement peut être vulnérable et l'on peut trouver la clé de déchiffrement.

Une méthode facile à mettre en place est celle de l'attaque par factorisation de Fermat [4]. Elle permet de trouver, grâce à la clé publique (clé de chiffrement), les nombres premiers à l'origine des clés du RSA et donc de retrouver la clé privée (clé de déchiffrement). Elle se base sur la factorisation en nombres premiers ce qui est en général difficile à faire rapidement dans certaines conditions.

Une méthode plus particulière mais assez efficace si les conditions sont respectées est "l'attaque de Wiener". Elle est quant à elle basée sur les fractions continues qui permettent de trouver la clé privé, encore une fois, sous certaines conditions, assez rapidement [5]. Due à Wiener qui montra en 2002 que sa méthode permettait d'obtenir la clé privé efficacement.

Ainsi, grâce à ces méthodes il est possible de déterminer des conditions sur les nombres premiers servant de base au RSA permettant de s'assurer d'une sécurité accrue et évitant les attaques précédentes.

Problématique retenue

Dans quelle mesure le système de cryptographie RSA est-il sécurisé ?

Objectifs du TIPE

Comprendre la cryptographie RSA
Voir les limites de l'efficacité de ce système
Déterminer des conditions renforçant la sécurité de ce système

Abstract

Cryptography plays a major role in communications. At the intersection of mathematics and computer science, it is today a science in its own right, responding to the need of civilizations since they exist: the maintenance of secrecy. I took a special interest in the RSA cryptography system. This process is based on the big prime numbers an it's why it's secured. Two methods can decipher the RSA under some condition: the Fermat and Wiener method.

Références bibliographiques (phase 2)

[1] Ronald L Rivest, Adi Shamir, Leonard Adleman : A method for obtaining digital signatures and public-key cryptosystems

[2] Gilles Zemor : Cours de cryptographie : *ISBN : 2842250206*

[3] Michael O Rabin : Probabilistic algorithm for testing primality

[4] Son Y. yan : Cryptanalytic Attacks on RSA

[5] Wiener's attack : *https://en.m.wikipedia.org/wiki/Wiener%27s_attack*

DOT

[1] *Recherche des étapes clés dans la méthode du RSA*

[2] *Recherche de méthodes pouvant déchiffrer le RSA*

[3] *Etude de l'attaque de Fermat*

[4] *Etude des fractions continues*

[5] *Etude de l'attaque de Wiener*

[6] *Ecriture du code informatique pour l'algorithme RSA et les méthodes de déchiffrage*