Attaques sur RSA

La cryptographie et la cryptanalyse - la science de la protection des messages et l'analyse de tels messages - m'intéresse particulièrement, et étudier ici l'algorithme RSA et quelques attaques possibles me semblait particulièrement instructif.

En ville, les flux de données prennent de plus en plus d'importance, des payements des transports en commun, au caméras de surveillance. Mais toutes ces données, qui doivent être échangées entre plusieurs instances, sont sensibles ; il faut donc les protéger, et c'est là qu'intervient la cryptographie.

Positionnement thématique (ÉTAPE 1) :

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

Mots-clés (ÉTAPE 1) :

Mots-clés (en français)	**Mots-clés (en anglais)**
RSA	*RSA*
Cryptographie asymétrique	*Asymmetric cryptography*
Cryptanalyse	*Cryptanalysis*
Attaque de Wiener	*Wiener's attack*
Attaque de Håstad	*Håstad's attack*

Bibliographie commentée

L'avènement de l'informatique a facilité les communications, et l'usage de la cryptographie a fortement augmenté depuis.

On distingue deux types de systèmes cryptographiques : les algorithmes symétriques, et asymétriques. Les algorithmes symétriques utilisent la même clé pour chiffrer et pour déchiffrer les messages. Le principal défaut de cette méthode réside dans la difficulté d'échanger les clés : il faut pour cela disposer d'un canal sécurisé, comme par exemple se l'échanger en personne. Mais cela n'est pas forcément possible, comme dans le cas d'échanges par internet par exemple.
Suite à ce problème, de nouveaux algorithmes, utilisant un autre principe, voient le jour dans les années 1970. Ces systèmes cryptographiques utilisent des couples de clés : clé publique, clé privée. La clé publique sert à chiffrer les messages, et est librement accessible. La clé privée, quant à elle, permet de déchiffrer les messages chiffrés avec la clé publique correspondante, et est gardée secrète.
Ainsi on peut envoyer des messages chiffrés sans avoir besoin d'échanger au préalable une clé

avec le destinataire : il suffit d'aller chercher sa clé publique dans un annuaire.
Le principal défaut de ce type d'algorithme est qu'ils sont beaucoup plus lents que que leurs pairs symétriques, pour un même niveau de sécurité, comme le montre **[6]** : l'initialisation de AES CBC 256, l'algorithme symétrique le plus couramment utilisé, prend 0.619µs, tandis qu'une opération de RSA 2048 prend 0.16ms, soit environ 260 fois plus longtemps. On peut néanmoins les combiner pour tirer parti des avantages de chacun, en échangent une clé pour un algorithme symétrique par un algorithme à clé asymétrique, et en continuant l'échange avec l'algorithme symétrique.

Aujourd'hui, une grande partie des applications cryptographiques utilisent un schéma asymétrique, dont l'algorithme le plus répandu est RSA **[1]**, utilisé pour sécuriser une grande variété de systèmes, des communications internet (via le protocole TLS **[7]** de HTTPS) aux cartes bancaires.
C'est la raison pour laquelle je me pencherai uniquement sur cet algorithme.

La sécurité de RSA repose sur la difficulté de factoriser des grand entiers semi-premiers. Il est néanmoins possible, sous certaines conditions, de contourner la sécurité de RSA et de récupérer le contenu d'un message chiffré sans disposer de la clé privée, voire même de récupérer la clé privée **[2] [3] [4]**.

Problématique retenue

Pourquoi l'algorithme RSA est-il utilisé alors qu'il existe des attaques sur cet algorithme ?

Objectifs du TIPE du candidat

1. Implémentation de l'algorithme RSA, de façon naïve, et avec un schéma de remplissage

2. Etude et implémentation d'attaques sur RSA

3. Montrer que l'implémentation de RSA doit être faite avec précaution

Références bibliographiques (ÉTAPE 1)

[1] R.L RIVEST, A. SHAMIR, L. ADLEMAN : A Method for Obtaining Digital Signatures and Public-Key Cryptosystem *: Communications of the ACM, v. 21, n. 2, (1978), pp. 120-126*

[2] D. BONEH : Twenty years of attacks on the RSA cryptosystem *: Notices of the American Mathematical Society (AMS), 46, no. 2, (1999), 203-213*

[3] MICHAEL J. WIENER : Cryptanalysis of Short RSA Secret Exponents *: IEEE Transactions on Information Theory 36 (1990), 553–558*

[4] M. JASON HINEK : (Very) Large RSA Private Exponent Vulnerabilities *: CACR Technical Report CACR 2004-01, Centre for Applied Cryptographic Research, University of Waterloo, 2004*

[5] WIKIPEDIA : Optimal asymmetric encryption padding *: https://en.wikipedia.org/wiki /Optimal_ asymmetric_ encryption_ padding, consulté le 22/04/2022*

[6] CRYPTO++ : Speed comparison of popular crypto algorithms *: https://www.cryptopp.com /benchmarks.html, consulté le 25/01/2023*

[7] RFC : The Transport Layer Security (TLS) Protocol *: https://www.rfc-editor.org/rfc /rfc524, consulté le 25/01/2023*

DOT

[1] *: Avril 2022 : Implémentation de RSA et de OAEP ;*

[2] *: Fin juin - août 2022 : Implémentation et démonstration de l'attaque de Wiener (qui a demandé l'implémentation des fractions continues) ;*

[3] *: Octobre - Novembre 2022 : Implémentation et preuve de l'attaque de Hastad, et détermination du nombre minimum d'équations nécessaires ;*

[4] *: Janvier 2023 : Suite à la lecture de [4], implémentation d'une attaque sur les grands messages ;*

[5] *: Début mars 2023 : Essais pour adapter l'attaque précédente à l'attaque de Hastad. Cela se révèlera insatisfaisant à cause de l'encodage ;*

[6] *: Fin mars 2023 : Extension de l'attaque de Wiener à de grands exposants privés ;*

[7] *: Mai 2023 : Ajout de l'attaque multiplicative.*