16770 PELLETIER Grégoire

Cryptographie des cartes bancaires, fonctionnement et casse du chiffrement RSA

Je voulais m'intéresser au domaine financier ou bancaire, et je voulais trouver un sujet qui lie Informatique et Mathématiques. J'ai très vite choisit la cryptographie qui était en parfait accord avec le thème "enjeux sociétaux".
L'utilisation croissante des données, notamment sensibles et confidentielles, nécessite un progrès constant dans leurs protections et leurs chiffrements. L'intérêt qu'elle suscite et le progrès technique renforce la menace qui pèse sur ces données, et lutter contre cette menace est un enjeu majeur.

Positionnement thématique (ETAPE 1)

INFORMATIQUE (Informatique pratique), MATHEMATIQUES (Autres).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
cryptographie	*cryptography*
chiffrement RSA	*RSA*
force brute	*brute force*
arithmétique	*arithmetic*
factorisation	*factorization*

Bibliographie commentée

Les cartes bancaires permettent plus de la moitié des transactions effectuées en France, la fiabilité du chiffrement de ces échanges est donc absolument indispensable. Pour ce faire, nous disposons de plusieurs méthodes et algorithmes (la puce, le code confidentiel, le chiffrement RSA et l'authentification DES) [1]. Le chiffrement RSA est aujourd'hui un des algorithmes les plus répandus en cryptographie et est utilisé pour sécuriser nos cartes bancaires, cependant, les progrès en informatique et en algorithmique pourraient menacer cette méthode [1]. D'ailleurs, des attaques ont déjà réussi à casser ce chiffrement par le passé, comme lors de l'affaire Humpich [2]. La fiabilité du chiffrement RSA est basée entièrement sur l'hypothèse que l'entier utilisé pour la clé publique ne soit pas factorisable en temps acceptable lors de la transaction. Le chiffrement repose uniquement sur la factorisation de cet entier, factoriser l'entier de la clé publique c'est casser RSA [3]. Les algorithmes les plus performants, comme le "crible algébrique", permettent de factoriser des entiers proches de 1024 bits, qui ne sont donc plus considérés comme fiables [3]. L'algorithmique quantique représente la plus grande menace pour le chiffrement RSA puisque l'algorithme de Shor et un ordinateur quantique suffisamment puissant permettraient de casser facilement RSA, même pour des clés "très grandes" (complexité en log(N)^3). Les autres méthodes de protection des cartes bancaires peuvent aussi être vulnérables [5]. Il convient donc de modifier ce moyen de chiffrer nos données et de l'améliorer pour assurer la sécurité des transactions par cartes bancaires, en suivant les progrès techniques qui entraînent une diminution de la sécurité. Il est aussi nécessaire de multiplier les méthodes de protection des cartes bancaires [4]. A défaut, dans l'hypothèse de la

création d'un ordinateur quantique suffisamment fiable et grand (de l'ordre du million de Qubits), il conviendrait de remplacer RSA par d'autres chiffrements cryptographiques moins sensibles au progrès des ordinateurs quantiques.

Problématique retenue

Il s'agit d'étudier différentes failles du chiffrement RSA et les solutions éventuelles à apporter pour déterminer si le chiffrement RSA va suffisament évoluer pour rester un moyen efficace de protéger nos cartes bancaires dans le futur.

Objectifs du TIPE

Je me propose :

_d'expliquer comment le chiffrement RSA permet de sécuriser les cartes bancaires,

_d'étudier les limites de ce procédé,

_de réaliser des algorithmes permettant l'implémentation du chiffrement RSA et permettant de casser ce chiffrement (pour des "petits entiers", de l'ordre de 256 bits),

_d'explorer les solutions qui permettraient d'améliorer la fiabilité du chiffrement RSA.

Références bibliographiques (ETAPE 1)

[1] Jacques Patarin : La cryptographie des cartes bancaires : *https://www.pourlascience.fr/sr/article/la-cryptographie-des-cartes-bancaires-4766.php*

[2] Thomas Genet : Le protocole cryptographique de paiement par carte bancaire : *https://interstices.info/le-protocole-cryptographique-de-paiement-par-carte-bancaire/*

[3] Anca Nitulescu : Cryptosystème RSA : *https://www.di.ens.fr/~nitulesc/files/crypto3.pdf*

[4] Louis Guillou : Histoire de la carte à puce du point de vue d'un cryptologue : *http://jacques-andre.fr/chi/chi04/guillou.pdf*

[5] Steven J. Murdoch : EMV flaws and fixes: vulnerabilities in smart card payment systems : *https://murdoch.is/talks/leuven07emv.pdf*

DOT

[1] *avril-mai 2020 : décision de réaliser un TIPE sur la cryptographie, choix du chiffrement RSA, recherche de sources et d'une bibliographie concernant la sécurité des cartes bancaires et RSA.*

[2] *septembre 2020 : réalisation d'une première version du Beamer et recherches bibliographiques, concernant différentes attaques (Wiener, Hastad, chronométrage) et le théorème des restes chinois, qui ne seront pas retenues.*

[3] *novembre-décembre 2020 : implémentation des différents algorithmes en Python, utilisation du code ASCII, choix de la force brute pour casser RSA pour des entiers de forme générale.*

[4] *mai 2021 : dernières retouches du beamer et des algorithmes, rédaction du MCOT et du DOT, fin de la réalisation du TIPE.*