Cryptographie asymétrique et problèmes difficiles

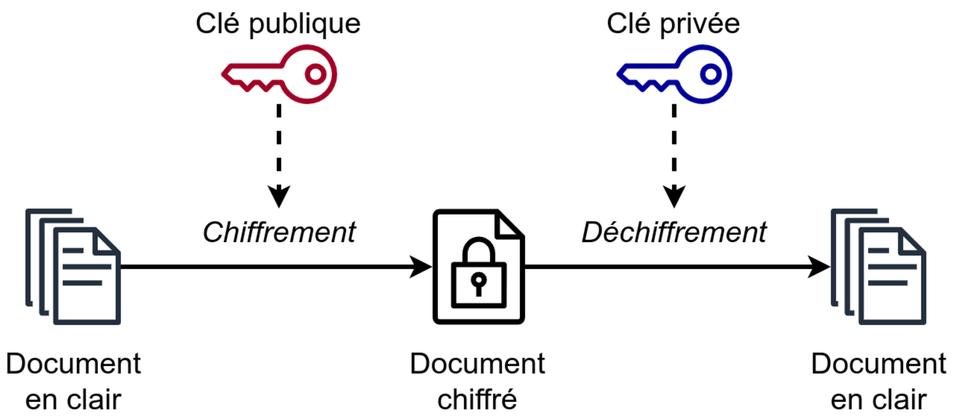
UNIVERSITÉ LIBRE DE BRUXELLES – FACULTÉ DES SCIENCES
DÉPARTEMENT DE L'INFORMATIQUE
Zia Gulzar - Marc Chevallier – Rasamimanana Ando - Zariouh El Kaidi Soufiane

Problème posé

Protection de données

Dans un contexte moderne où toutes nos informations personnelles sont transférées via internet, comment veiller à ce que nos données ne tombent pas dans de mauvaises mains ?

À travers l'histoire, avant l'avènement d'un monde ultraconnecté, de nombreuses solutions ont été proposées pour permettre des canaux de communication sécurisés. Du code de César basé sur un chiffrement par substitution monoalphabétique, où chaque lettre est remplacée par une autre lettre située un peu plus loin dans l'alphabet, aux solutions plus modernes, le problème reste le même. Comment empêcher qu'une personne non autorisée décode notre message ? La solution consiste à utiliser un encryptage dont le décryptage est trop difficile pour la capacité de calcul accessible aujourd'hui. Les algorithmes publiés par les équipes de chercheurs tels que Rivest–Shamir–Adleman (RSA) ou encore Merkle-Hellman tentent de le faire en utilisant un système de clés asymétrique. C'est-à-dire que la clé pour encrypter un message ne permet pas de le décrypter.



Description du projet

Objectif

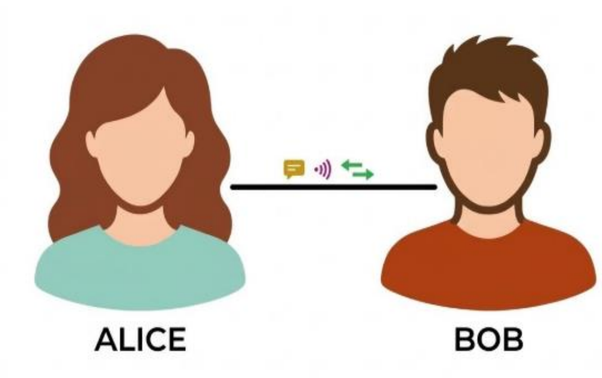
Ce projet est consacré à l'étude de deux systèmes de cryptographie : RSA et Merkle-Hellman.

Asymétrique

Ce système utilise une clé publique pour chiffrer et une privée pour déchiffrer. Il s'appuie sur des "fonctions à sens unique" : des opérations faciles à calculer, mais impossibles à inverser sans la clé privée (la "brèche secrète").

Merkle-Hellman

Le cryptosystème de Merkle-Hellman s'appuie sur le problème algorithmique du "sac à dos" (comment optimiser le contenu d'un espace limité). Bien que ce problème soit généralement très complexe à résoudre, la variante mathématique utilisée pour ce système s'est avérée vulnérable. Conséquence : il a été définitivement cassé par Adi Shamir en 1984.



RSA

Un autre concept, encore plus fondamental, repose sur la multiplication des nombres entiers. S'il est quasi instantané de multiplier d'immenses nombres entre eux, l'opération inverse — la factorisation — demande une puissance de calcul démesurée et devient impossible en pratique dès que les nombres comportent quelques centaines de chiffres. C'est précisément sur la difficulté de ce problème mathématique que l'algorithme RSA fonde toute sa sécurité.

Expérience

L'expérience menée dans le cadre de ce projet repose sur l'implémentation des algorithmes RSA et Merkle-Hellman. Nous avons d'abord modélisé une discussion chiffrée standard entre deux utilisateurs (Alice et Bob). Ensuite, pour enrichir notre analyse comparative, nous avons simulé un scénario d'interception où un tiers tente de récupérer le message, permettant ainsi d'illustrer les enjeux de sécurité propres à chaque cryptosystème.

Chiffrement

Le chiffrement transforme un message clair en un format illisible afin de sécuriser sa transmission. Les algorithmes cryptographiques opérant sur des nombres, la norme ASCII est d'abord utilisée pour convertir chaque caractère du message initial en valeur numérique.

ASCII Alphabet: Binary & Decimal Codes

Letter	Binary	Decimal	Letter	Binary	Decimal
A	1000001	65	N	1001110	78
B	1000010	66	O	1001111	79
C	1000011	67	P	1010000	80
D	1000100	68	Q	1010001	81
E	1000101	69	R	1010010	82
F	1000110	70	S	1010011	83
G	1000111	71	S	1010100	84
H	1001000	72	U	1010101	85
I	1001001	73	V	1010110	86
J	1001010	74	W	1010111	87
K	1001011	75	X	1011000	88
L	1001100	76	Y	1011001	89
M	1001101	77	Z	1011010	90

La cryptographie, c'est l'art de cacher des messages.
C'est comme un tour de magie pour transformer un message pour que seules certaines personnes puissent le comprendre.
Sans cela, on ne pourrait pas garder nos secrets sur internet.

UNIVERSITÉ LIBRE DE BRUXELLES – FACULTÉ DES SCIENCES

L'esprit en éveil : 25 ans de culture scientifique

PRINTEMPS DES SCIENCES 23-29 MARS 2026

Cryptographie asymétrique et problèmes difficiles

ULB UNIVERSITÉ LIBRE DE BRUXELLES

UNIVERSITÉ LIBRE DE BRUXELLES – FACULTÉ DES SCIENCES

DÉPARTEMENT DE L'INFORMATIQUE

Zia Gulzar - Marc Chevallier – Rasamimanana Ando - Zariouh El Kaidi Soufiane

RSA

PUB = (e, n) = (65537, 11704425078778514677850251313900047714959439 5...)

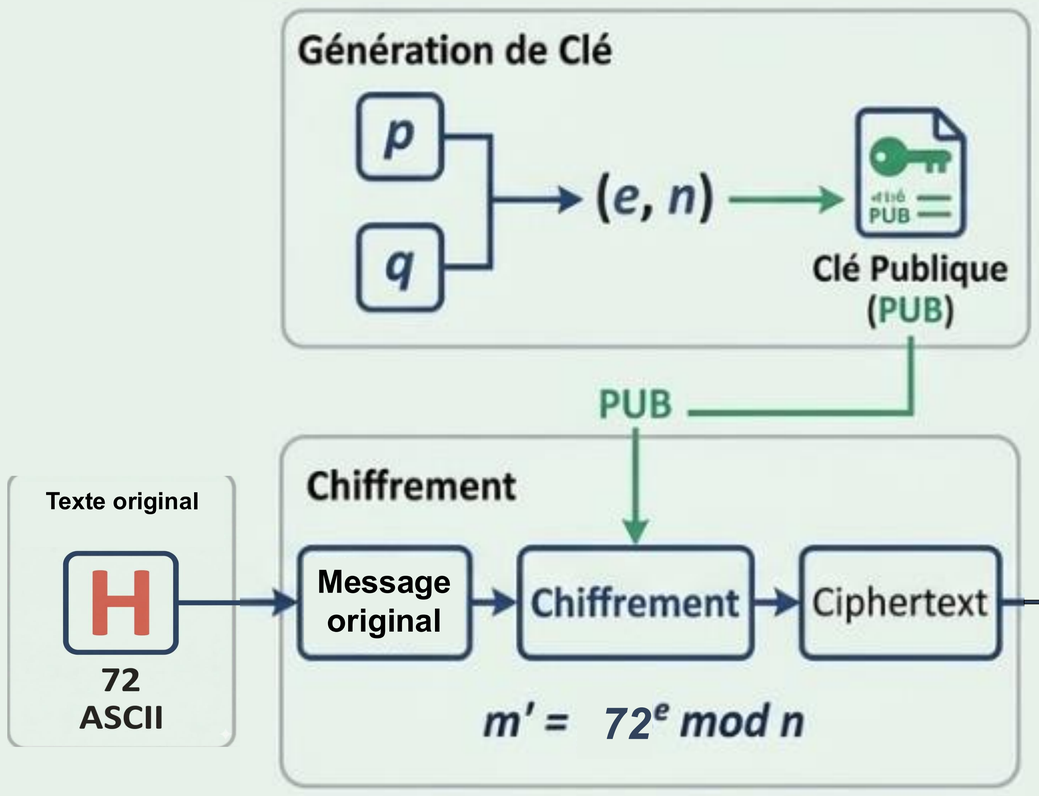
Texte : H

Format ASCII : 72

Formule : $m' = 72^e \bmod n$

Encodage :

69745678730473430220545406286400368
15644968814820191755672812350693248
94966253534301772515118664127775193
63111746134020784677590465316546295
10273209830766495123347260348182737
92676614649548858474927984422320646
50749934413089001429022807265018840
80270548950550679895378440348462397
97192215838666713717383384 88



Merkle-Hellman

PUB = [13209, 7995, 5889, 4049, 16052, 9571, 8857, 10169]

Texte : H

Format ASCII : 72

Binaire : 0 1 0 0 1 0 0 0

Formule :

0 × 13209 = 0
1 × 7995 = 7995
0 × 5889 = 0
0 × 4049 = 0
1 × 16052=16052
....

Encodage : 7995 + 16052 = 24047

UNIVERSITÉ LIBRE DE BRUXELLES – FACULTÉ DES SCIENCES