LIFPROJET - 2018

CHIFFREMENT FONDÉ SUR L'IDENTITÉ (IBE)

Mourad ALLAM – 11509098
Gabriel SEQUEIRA – 11508289
Nicolas EUVRARD-BLANC - 11508330

Spoutnik Corp.

Sommaire

I. Le chiffrement de nos jours

Dans un premier temps, il est bon de rappeler ce qu'est réellement le chiffrement : il s'agit d'une méthode qui permet de transmettre un message d'une personne A à une personne B sans que quiconque puisse lire hormis les deux concernés.

Historiquement, les premières traces écrites du chiffrement remontent à plus de 3000 ans avant J.C., représentés par des hiéroglyphes. A la moitié du 20ème siècle apparaît l'informatique, on se trouve alors dans une situation délicate : la puissance de calcul évolue rapidement, au point que les algorithmes de chiffrement sont vite déchiffrables numériquement.

En 1977, le chiffrement RSA révolutionne la cryptographie au point qu'aujourd'hui, il reste indétrônable. Son principe repose sur deux clés, une publique et une privée. La clé publique est accessible par tous et permet de chiffrer le message pour une personne, la clé privée, elle, permet de déchiffrer le message. Cette technique repose donc sur la confidentialité de la clé privée. Il existe, bien sûr, d'autres algorithmes tels que les IBE, AES, mais il subsiste le problème de l'évolution rapide de la puissance de calcul.

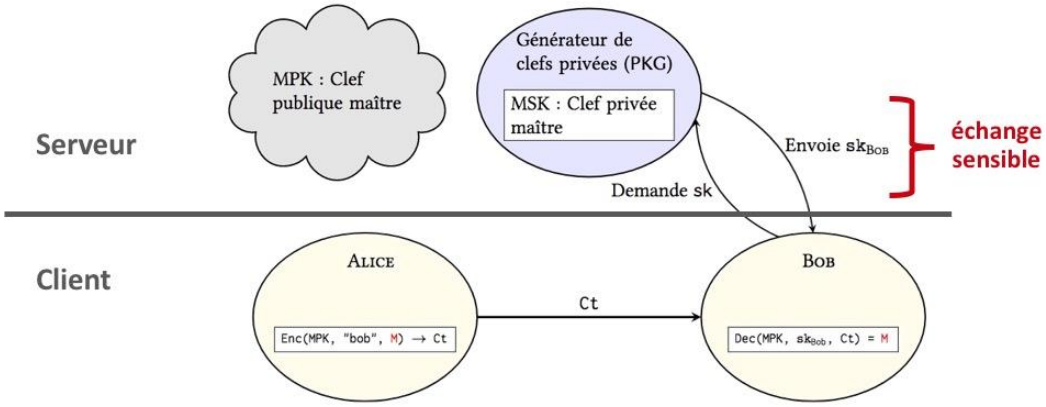
Afin de prévenir cette croissance, nous avons décidé de développer un chiffrement hybride basé sur l'IBE de Cocks et AES. Cette solution reposant sur des fonctions à sens unique (NDLR : l'image est facile à trouver mais pas l'antécédent) à partir de nombres entiers de très grande taille et respectant des préconditions, nous pensons donc qu'elle constitue un très bon moyen de contrer la puissance de calcul. De plus, le chiffrement hybride permet d'atténuer la notion de clé puisque tout passe par l'adresse mail et est invisible aux yeux des utilisateurs, nous ne sommes donc plus obligés de connaître la clé publique de la personne à qui on écrit.

L'IBE de Cocks est un algorithme assez complexe que nous allons développer dans la prochaine partie.

II. Spoutnik et IBE

a. Architecture

Le chiffrement basé sur l'identité (IBE « ID Based Encryption ») fonctionne sur un modèle de type client/serveur.



D'un côté nous avons le serveur qui est composé de la MPK (Master Public Key) ainsi que du PKG (Private Key Generator). Ce dernier possède une MSK (Master Secret Key).

Le partie cliente est simplement composée de sa clé privée (ou SKID) ainsi que d'un système pour calculer la clé publique de la personne à qui on souhaite envoyer un message.

Il existe plusieurs implémentations disponibles pour mettre en place l'IBE. Comme l'IBE de Boneh-Franklin ou celui de Gentry-Peikert-Vaikuntanathan. Nous voulions partir sur ce dernier mais nous n'arrivions pas à le prononcer à l'oral. Nous avons donc opté pour l'IBE de Cocks avec lequel nous n'avons pas ce problème.

La MPK est une clé qui peut être diffusée sans restriction. Alors que la MSK doit être bien protégée. Si celle-ci se trouve dans la nature, alors tout le système est mis en péril.

Première connexion d'un client souhaitant utiliser IBE :

- Le client se connecte sur le serveur (PKG)
- Le client s'authentifie via son adresse e-mail et demande sa SKID
- Le serveur génère la SKID du client en utilisant la MSK
- Le serveur renvoi la SKID au client

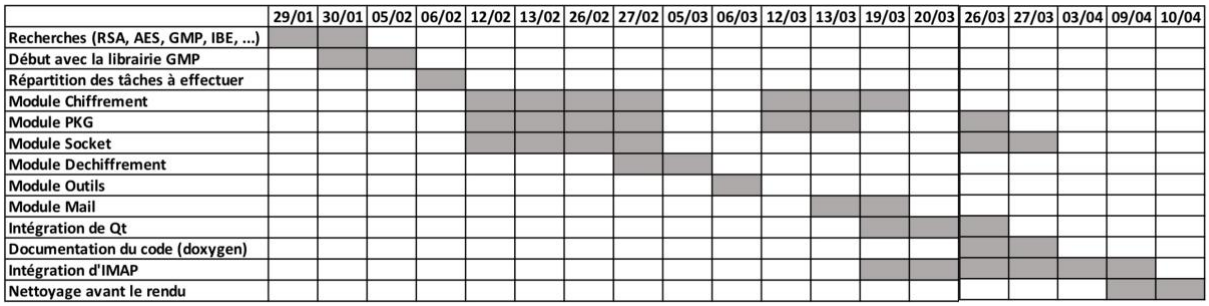
Le dernier échange entre le serveur et le client qui consiste à l'envoi de la clé secrète de celui-ci est sensible. En effet, si un attaquant réussi à se mettre au milieu de l'échange (MITM) et que celui-ci est en mesure de comprendre l'échange. Alors la clé privée sera connue de celui-ci. Ce qui met en péril le chiffrement.

Client qui souhaite envoyer un message en utilisant IBE :

- Utilise un chiffrement symétrique pour chiffrer ce qu'il envoi (AES, …)
- Chiffre le mot de passe AES en utilisant IBE
    - Connaître la MPK
    - Trouver clé publique du destinataire à partir de son adresse email
    - Donner ces 2 informations + le mot de passe AES à chiffrer à la fonction de chiffrement
- Envoyer le contenu chiffré avec AES + le mot de passe AES chiffré avec IBE en en-tête du message

L'exemple précèdent utilise un mode de chiffrement hybride. C'est à dire que l'on encapsule un chiffrement de type AES par un chiffrement de type IBE. On ne peut pas chiffrer le contenu entier en IBE car cela est beaucoup plus long à chiffrer et à déchiffrer. Aussi les algorithmes de chiffrement symétrique sont plus rapides que les algorithmes de chiffrement asymétrique.

b. Chronologie (Gantt)

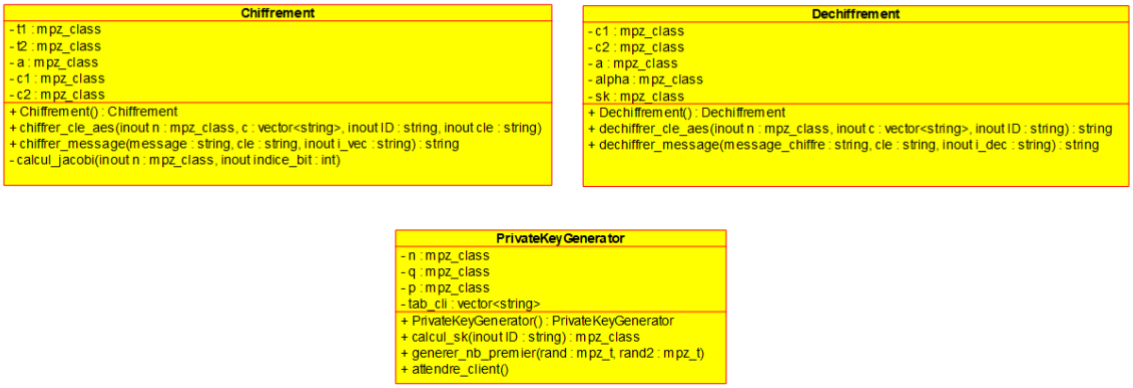


3 phases :

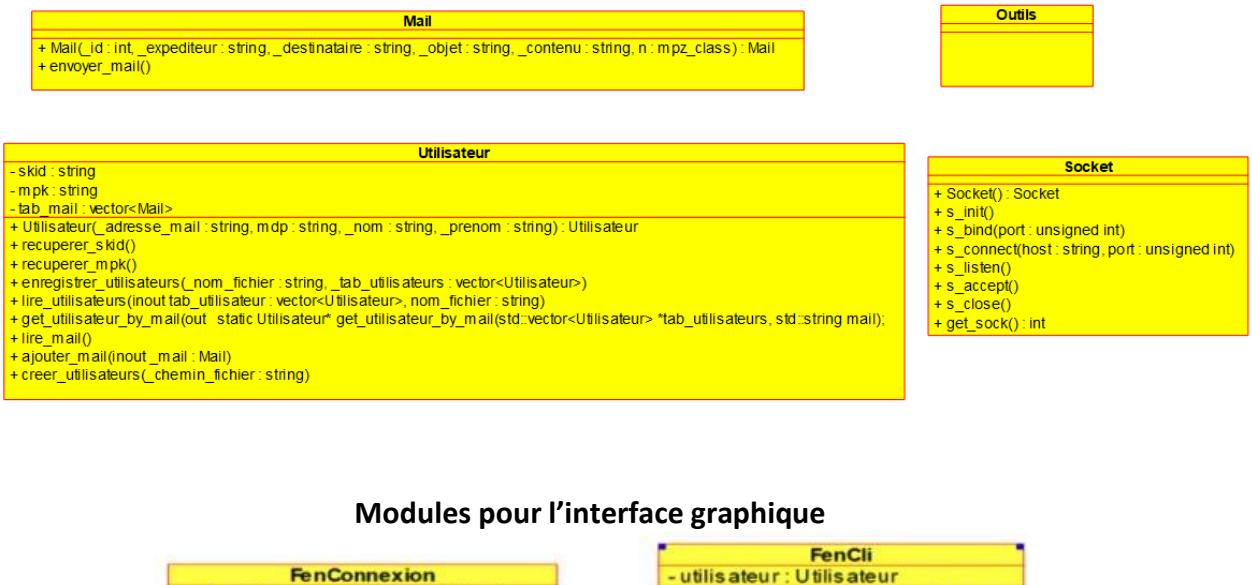
1. Recherches sur le sujet
2. Réalisation du cœur du projet (Chiffrement/Déchiffrement et PKG)
3. Interface graphique Qt

c. Modules

Modules principaux pour IBE



Module pour le client mail



Modules pour l'interface graphique

d. Outils

C++ : langage choisi pour la réalisation du projet.

GMP : bibliothèque permettant la manipulation de très grands nombres.

openSSL : bibliothèque permettant la gestion des fonctions de hash tel que SHA-256 + AES.

Qt : permet la création de fenêtres graphiques

SMTP : reprise d'un projet (LIFASR5) permettant l'envoi d'e-mail.

IMAP via CURL : pour consulter boite e-mail.

III. Bilan du projet

a. Difficultés rencontrées

- Début avec GMP
- Documentation pas toujours de qualité
- Hash de l'ID
- Enregistrer le cipher dans un fichier texte puis le lire
- Utiliser IMAP !!
- Difficile de tester l'envoi de mail car nos IP sont considérées comme des sources de SPAM (car on fait beaucoup de tests)

b. Améliorations

- Multidestinataires des mails (la gestion de plusieurs destinataires implique plusieurs chiffrements)
- Pièces jointes (intégration des pièces-jointes dans le corps du mail + chiffrement)

c. Ce que ça nous a apporté

- Découverte d'IBE
- Découverte de librairies (GMP, openSSL, Curl)
- Travail en groupe
- Développement d'interface graphique