**Rapport du Projet de Réseaux et Systèmes**

**A l’intention de Monsieur Bros Maxime**

****

**Membres du groupe : Dupont Rémi et Fauriat Mattieu**

**Promotion du Master Mathématiques CRYPTIS 2020-2021**

**1 – Présentation du sujet : Conception d’un protocole de communication basé TCP sécurisé par RSA**

Le but ici est de simuler une communication basée TCP sécurisée par RSA entre un client et un serveur sur un réseau.

Pour réaliser ce projet nous avons d’abord commencé par recopier les fonctions mises à disposition dans le sujet, puis nous avons créer quelques fonctions utiles pour le chiffrage RSA, telle que la fonction « decoupage » (voir ci-dessous) qui comme son nom l’indique servira à découper le message en plusieurs morceaux de même longueur.

Une image contenant texte

Description générée automatiquement

**2 – Déroulement de notre travail**

Nous avons commencé par RSA, en simulant un échange de nombres entiers entre Alice et Bob :

* Grâce à la méthode suggérée dans le sujet, Alice doit générer 2 nombres premiers p et q.
* Alice calcule ainsi que où ϕ est l’indicatrice d’Euler.
* Alice calcule aussi qui sera sa clef privée.
* Alice envoie à Bob la clef publique .
* Bob choisi son message M et le chiffre, grâce à la clef que lui a envoyée Alice, avec l’opération suivante : .
* Bob transmet le chiffré C à Alice.
* Alice déchiffre le message en effectuant le calcul suivant .

Jusqu’ici nous n’avons rencontré aucune difficulté dans la programmation car la plupart des fonctions à utiliser nous ont été données.

Ensuite, en nous aidant du cours nous avons essayé de coder un programme serveur qui représentera Bob et un programme client qui représentera Alice. Nous avons donc mis en place un système de communication qui implique que le premier message envoyé par Alice ne contient que la clef n. Pour cela nous avons mis en place un compteur qui s’incrémente pour chaque message envoyé et donc si le compteur est à 0 c’est qu’il s’agit du premier message.

Voici un screenshot du programme serveur, ainsi que du programme client :

* voici Bob :

Une image contenant texte

Description générée automatiquement

* et voici Alice

Une image contenant texte

Description générée automatiquement

Dans l’état actuel, ces programmes ne peuvent que chiffrer qu’un échange d’entiers. Ils fonctionnent comme suit :

* on lance en premier le serveur, puis le client
* Alice crée immédiatement sa paire de clefs et envoie à Bob la clef publique .
* Bob reçoit la clef, écrit le message qu’il veut envoyer (dans la cas présent un entier).
* Ensuite il chiffre son message avec la clef qu’il vient de recevoir.
* Il l’envoie à Alice
* Alice réceptionne le chiffré, et utilise sa clef privée pour obtenir le clair de base

Ensuite nous sommes passés à la manière de chiffrer des chaines de caractères. L’idée est la suivante : l’utilisateur (Bob) saisit au clavier une chaine de caractère. La chaîne de caractère est ensuite encodée en UTF-8. On peut ensuite convertir cette chaine de bytes en un entier avec la fonction *«  ».* Ainsi nous pouvons manipuler l’entier pour effectuer les calculs nécessaires aux chiffrements RSA. Puis Bob reconverti l’entier trouvé en bytes grâce à la commande La chaîne de bytes ainsi chiffrée est envoyé à Alice.

Maintenant Alice reconverti la chaine de bytes en un entier, retrouve l’entier originelle puis reconvertit cet entier en une chaîne de bytes toujours avec les commandes précédentes. La chaine de bytes peut à présent décodée. Si tout s’est bien passée Alice retrouve le message que Bob lui a envoyé.

Voici une nouvelle fois les screenshots des programmes :

* Bob :

Une image contenant texte

Description générée automatiquement

* Et Alice

Une image contenant texte

Description générée automatiquement