**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.