MATH EN INFO

1 - Cryptographie

FICHE DE SUJET

1 Descriptif du sujet

Alice et Bob, deux scientifiques très réputés, souhaitent pouvoir communiquer régulièrement par mail. Ils souhaitent crypter leurs communications. Après quelques recherches, ils souhaitent utiliser un protocole de cryptographie symétrique réputé extrêmement sûr. Cependant, afin de mettre en place ce protocole, Alice et Bob doivent se mettre d'accord sur une clé (K) qui servira aussi bien à coder qu'à décoder leur message. Ne pouvant se rencontrer, Alice et Bob cherchent donc un moyen de partager une clé K sans que celle-ci puisse être déterminée par une autre personne. Pour cela, Alice propose d'utiliser le principe d'échange de clés de Diffie-Hellman. Bob n'est pas convaincu de l'intérêt de ce principe et propose à Alice de lui envoyer une clé en l'encodant à l'aide d'un chiffrement par transposition qu'ils utilisaient quand ils étaient ensemble à l'université.

2 Réalisation attendue

2.1 Objectifs principaux

- Réaliser un programme permettant le codage et le décodage d'une clé transmise à l'aide du principe de Diffie-Hellman.
- Réaliser un programme permettant le codage et le décodage d'une clé transmise par chiffrement par transposition.

2.2 Questions intermédiaires et prolongements

- Conseillez Alice et Bob sur le choix du protocole de partage de clé.
- Si Alice et Bob ne s'étaient pas connus à l'université, auraient-ils pu utiliser la méthode proposée par Bob ? Et celle proposée par Alice ?
- Diffie-Hellman : expliquez comment fonctionne le principe de l'attaque de l'homme du milieu et mettez en place un programme simulant une telle attaque.
- Diffie-Hellman : expliquez en quoi l'utilisation d'un certificat permet de contrer l'attaque de l'homme du milieu. Quelles sont les limites de cette méthode ?
- Diffie-Hellman : expliquez le problème du logarithme discret et son lien avec Diffie-Hellman.
- Diffie-Hellman : étudiez l'algorithme "baby step giant step" pour la résolution du problème du logarithme discret.
- Chiffrement par transposition : proposez et étudiez un protocole d'attaque pour ce chiffrement.