Cryptographie

Mathis Deloge, Antoine Petot, Ange Picard

Dimanche 4 décembre 2016

Sommaire

Le sujet

Le sujet

Descriptif

Implémentation de deux programmes permettant le codage et le décodage d'information numériques suivant les deux principes suivant :

- Echange de clé de Diffie-Hellman
- Chiffrement par transposition

Diffie-Hellman

Chiffrement par transposition

Prolongements possibles

Les différents prolongements du sujet

- 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 ?
- Attaque de l'homme du milieu avec Diffie-Hellman.
- Algorithme "baby step giant step" et résolution du problème du logarithme discret dans Diffie-Hellman.
- Protocole d'attaque pour le chiffrement par transposition.

Sommaire

Diffie-Hellman

Diffie-Hellman

Chiffrement par transposition

Chiffrement par transposition

Sommaire

Résultats

Résultats

Sommaire

Conclusion

Conclusion

Sommaire