

Cryptographie

Mathis Deloge, Antoine Petot, Ange Picard

Dimanche 4 décembre 2016

Sommaire

- 1 Présentation du sujet
 - Le sujet
 - Prolongements possibles
- 2 Présentation des programme
- 3 Prolongements
- 4 Résultats
- 5 Conclusion

Le sujet

Le sujet

Descriptif

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

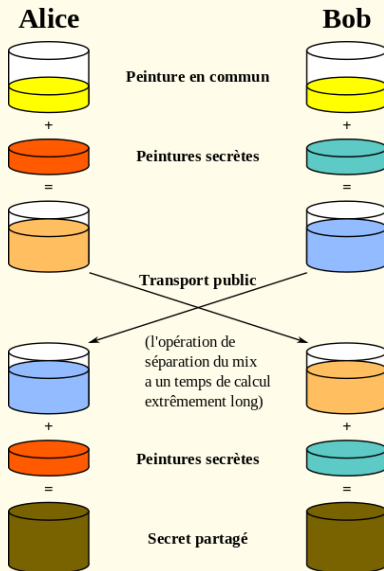
- Echange de clé de Diffie-Hellman
- Chiffrement par transposition

Diffie-Hellman

Principe

- Alice et Bob choisissent un groupe fini G d'ordre n et un générateur g de ce groupe publiquement
- Alice choisi au hasard a tel que $1 < a < n$ puis communique à Bob g^a
- Bob choisi au hasard b tel que $1 < b < n$ puis communique à Alice g^b
- Alice élève à la puissance a le nombre communiqué par Bob
- Bob élève à la puissance b le nombre communiqué par Alice
- Alice et Bob connaissent le nombre $g^{(ab)}$ impossible à déterminer par Eve

Diffie-Hellman



Chiffrement par transposition

Principe

- Avec le chiffrement par transposition, il est nécessaire que Alice et Bob connaissent une clé de chiffrement.
- Lors du chiffrement par transposition, on découpe le texte codé en bloc de la taille de la clé de chiffrement pour ensuite permuter l'ordre des caractères à l'intérieur de ces blocs en suivant la clé de chiffrement.
- Pour déchiffrer un message, il suffit de remettre les caractères à leur place au sein de chaque bloc de texte en s'aidant de la clé de chiffrement

Chiffrement par transposition

On peut représenter la chiffrement d'un message par transposition à l'aide d'un tableau :

Je suis étudiant à l'IUT de Dijon							JTADUIU OSDIJEU LIATNE TESND						
B	O	N	J	O	U	R	B	J	N	O	O	R	U
J	E	S	U	I	S	E	J	U	S	E	I	E	S
T	U	D	I	A	N	T	T	I	D	U	A	T	N
A	L	I	U	T	D	E	A	U	I	L	T	E	D
D	I	J	O	N			D	O	J	I	N		
B	J	N	O	O	R	U	B	O	N	J	O	U	R
J	U	S	E	I	E	S	J	E	S	U	I	S	E
T	I	D	U	A	T	N	T	U	D	I	A	N	T
A	U	I	L	T	E	D	A	L	I	U	T	D	E
D	O	J	I	N			D	I	J	O	N		
JTADUIU OSDIJEU LIATNE TESND							Je suis étudiant à l'IUT de Dijon						

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

- 1 Présentation du sujet
- 2 Présentation des programme**
- 3 Prolongements
- 4 Résultats
- 5 Conclusion

Présentation des programme

Sommaire

1 Présentation du sujet

2 Présentation des programme

3 Prolongements

- Choix du protocole
- Utilisation des protocoles
- Attaque de l'homme du milieu
- Logarithme discret
- Baby step giant step
- Attaque du chiffrement par transposition

4 Résultats

5 Conclusion

Choix du protocole

Quel protocole de partage de clé choisir ?

- Diffie-Hellman est un protocole d'échange de clé tout à fait adapté dans notre cas.
- Chiffrement par transposition est un protocole de chiffrement de message à partir d'une clé. Plus adapté à l'échange de message cryptés

Utilisation des protocoles

Diffie-Hellman

Diffie-Hellman à l'avantage de ne demander aucun prérequis pour être mis en place. Il est utilisé pour échanger des clés de cryptage.

Chiffrement par transposition

Besoin d'échanger une clé secrète pour permettre le cryptage et le décryptage des messages envoyés.

Attaque de l'homme du milieu

Principe et fonctionnement

Logarithme discret

Problème et lien avec Diffie-Hellman

Baby step giant step

Utilisation de l'algorithme

Attaque du chiffrement par transposition

Proposition de protocole

Sommaire

- 1 Présentation du sujet
- 2 Présentation des programme
- 3 Prolongements
- 4 Résultats**
- 5 Conclusion

Résultats

Résultats

Sommaire

- 1 Présentation du sujet
- 2 Présentation des programme
- 3 Prolongements
- 4 Résultats
- 5 Conclusion**

Conclusion

Conclusion

Sommaire

1 Présentation du sujet

- Le sujet
 - Diffie-Hellamn
 - Chiffrement par transposition
- Prolongements possibles

2 Présentation des programme

3 Prolongements

- Choix du protocole
- Utilisation des protocoles
- Attaque de l'homme du milieu
- Logarithme discret
- Baby step giant step
- Attaque du chiffrement par transposition

4 Résultats

5 Conclusion