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 :

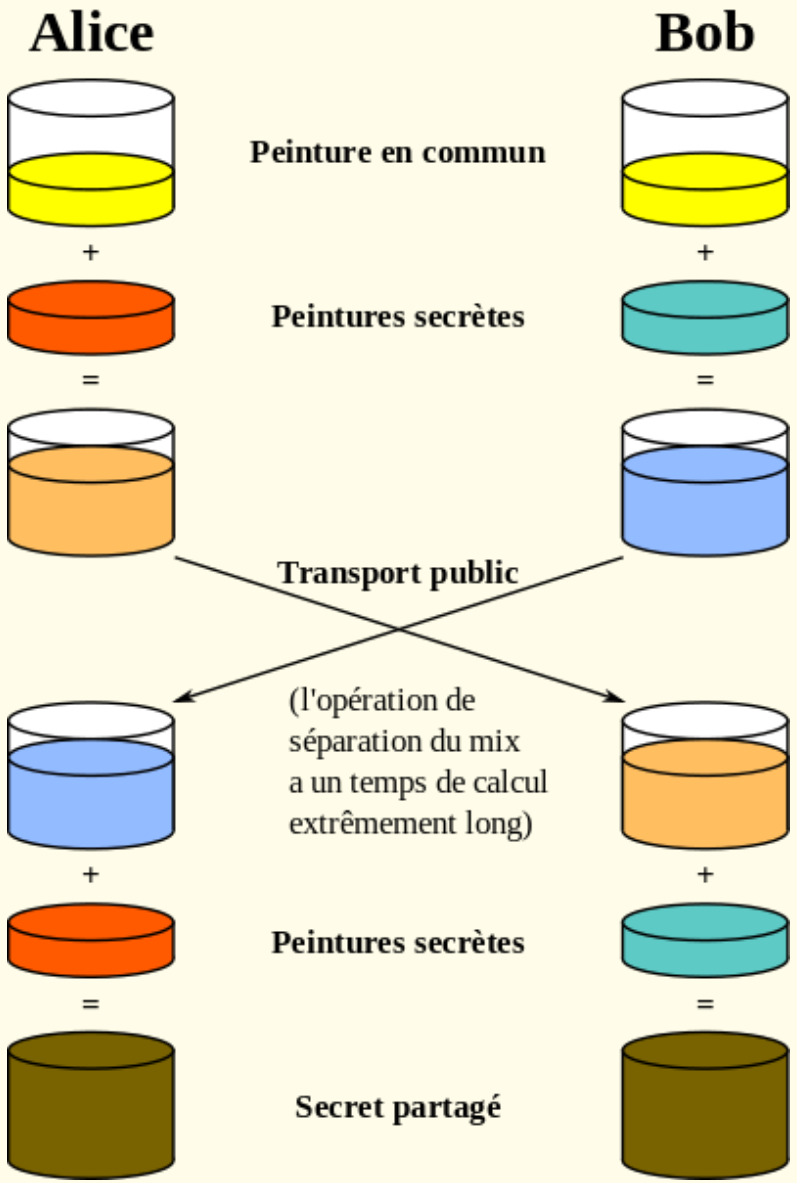
- Echange de clé de Diffie-Hellman
- Chiffrement par transposition

Diffie-Hellman

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 ga
- Bob choisi au hasard b tel que $1 < b < n$ puis communique à Alice gb
- 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) impssible 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 caractère à l'intérieur de ces blocs en suivant le 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						
B	O	N	J	O	U	R
J	E	S	U	I	S	E
T	U	D	I	A	N	T
A	L	I	U	T	D	E
D	I	J	O	N		

JTADUIU OSDIJEU LIIATNE TESND						
B	J	N	O	O	R	U
J	U	S	E	I	E	S
T	I	D	U	A	T	N
A	U	I	L	T	E	D
D	O	J	I	N		

B	J	N	O	O	R	U
J	U	S	E	I	E	S
T	I	D	U	A	T	N
A	U	I	L	T	E	D
D	O	J	I	N		

JTADUIU OSDIJEU LIIATNE TESND						
B	O	N	J	O	U	R
J	E	S	U	I	S	E
T	U	D	I	A	N	T
A	L	I	U	T	D	E
D	I	J	O	N		

B	O	N	J	O	U	R
J	E	S	U	I	S	E
T	U	D	I	A	N	T
A	L	I	U	T	D	E
D	I	J	O	N		

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

Diffie-Hellman

Diffie-Hellman

Chiffrement par transposition

Chiffrement par transposition

Sommaire

Résultats

Résultats

Sommaire

Conclusion

Conclusion

Sommaire