Cryptographie

Mathis Deloge, Antoine Petot, Ange Picard

Dimanche 4 décembre 2016

Sommaire

Le sujet

Descriptif

Implémentation d'un programme virtualisant deux personnes, Alice et Bob voulant s'échanger des messages cryptés en réseau suivant les deux principes suivants :

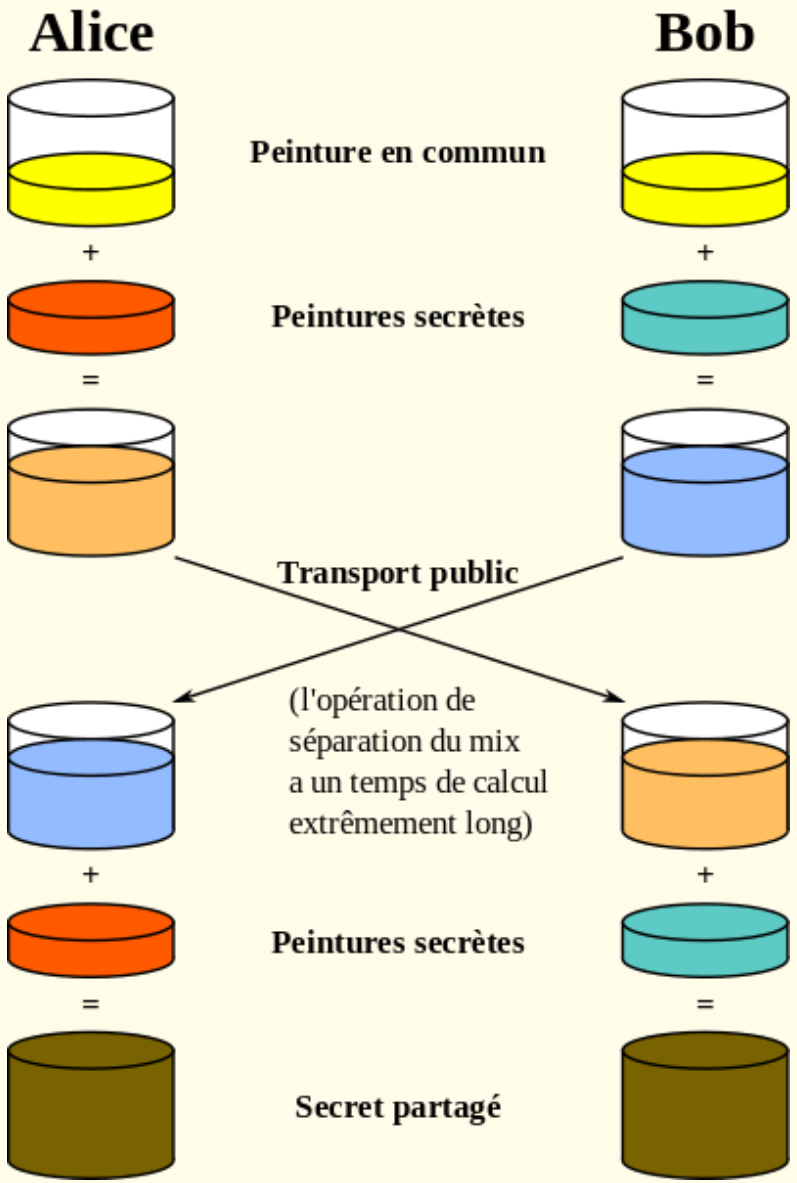
- Echange de clé de Diffie-Hellman
- Chiffrement par transposition

Diffie-Hellman

Principe

- Alice et Bob choisissent un groupe fini G d'ordre n et un générateur g de ce groupe publiquement.
- Alice choisis au hasard a tel que $1 < a < n$ puis communique à Bob ga.
- Bob choisis 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} impossible à déterminer par Eve.

Diffie-Hellman



Chiffrement par transposition

Principe

- Lors du chiffrement par transposition, on découpe le texte à crypter 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 le 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		

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

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	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

Présentation du programme

```
1  public class main{
2      public static void main(String[] args) {
3          PerfectGenerator generator = new PerfectGenerator()
               ;
4          BigInteger g = generator.getG();
5          BigInteger p = generator.getP();
6
7          Person Alice = new Person(p,g, "Alice");
8          Person Bob = new Person("Bob");
9
10         Network network = new Network(Alice,Bob);
11
12         Alice.givePublicKey(network.initiateConversation(p,
               g, Alice.getSelfPublicKey()));
13
14         network.send(Alice.encrypt("Bonjour, j'envois un
               message crypté !"));
15     }
16 }
```

Sommaire

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 messages cryptés lorsque l'on possède déjà une clé.

Prérequis 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 en utilisant une communication publique. Il appartient à la cryptographie à clé publique.

Chiffrement par transposition

Cet algorithme nécessite une clé secrète connue des deux personnes pour permettre le cryptage et le décryptage des messages échangés.

Attaque MITM : Man-in-the-middle

Principe et fonctionnement

Eve va intercepter les communications entre Alice et Bob puis mettre en place un échange de clé de Diffie-Hellman avec Alice et un autre avec Bob. Ainsi, pour Alice, Eve se fera passer pour Bob et pour Bob, elle se fera passer pour Alice.

Contrer l'homme du milieu

Utiliser des certificats, des signatures électroniques mises en place par un tiers de confiance pour s'assurer que Bob, communique avec Alice et Alice communique avec Bob.

Logarithme discret

Problème et lien avec Diffie-Hellman

Le logarithme discret est très utilisé en cryptographie à clé publique. En effet, il est impossible pour le moment de déterminer un entier l pour lequel $l = log_g y$ avec g étant un générateur d'une groupe cyclique G et $y \in G$.
Comme le groupe G choisi est un groupe cyclique, $log_g y$ est modulo n, n étant l'ordre du groupe G, il n'est pas possible de déterminer $l = log_g y$.

Baby step giant step

Principe

- On a p un nombre entier premier.
- On a $x = logDiscret(h) = m * q + r$ avec q et r des entiers où $0 \leq r < m$
- On a $m = \lceil \sqrt{p} \rceil$
- On calcule g^i pour i allant de 0 à $m - 1$ et on stocke les résultats dans une table de hashage.
- On initialise q avec $q = 0$
- On calcule $h(g^{-m})^q$ en incrémentant q à chaque calcul.
- On arrête de calculer dès qu'on trouve un résultats égal à un résultat de la table de hashage.
- On obtient $logDiscret(h) = q * m + 1$.

Baby step giant step

Utilisation

L'utilisation d'un tel algorithme permet de réduire à maximum de $2\sqrt{n}$ multiplication la recherche du logarithme discret dans un groupe G. On pourra cependant lui reprocher son usage intensif de la mémoire pour stocker la table de hashage dans le cas d'un nombre premier p très grand. D'autres algorithmes tels que le Rho de Pollard permettent la résolution du logarithme discret sans une telle utilisation de mémoire.

Attaque du chiffrement par transposition

Différentes propositions

- Faire une étude statistiques d'apparition de lettres pour déterminer la langue du document.
- Déterminer la longueur de la clé.
  - Récupérer différents messages d'un même expéditeur ou pour un même destinataire pour déterminer un début ou une fin récurrente.
- Découper le message en longueur de mot de la taille de la clé.
- Essayer des anagrammes en utilisant un dictionnaire de mot dans la langue déterminée auparavant.

Sommaire

Résultats

Programme

Le programme permet d'échanger des messages cryptés entre Alice et Bob et utilisant le principe de transposition et implicitement l'échange de clé de Diffie-Hellman.

Prolongements

Les 6 prolongements proposés dans le sujet ont été réalisés, nous permettant de compléter cette introduction à la cryptographie.

Sommaire

Conclusion

Sommaire