

Cryptographie

Mathis Deloge, Antoine Petot, Ange Picard

13 décembre 2016

Sommaire

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

Descriptif

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

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

Diffie-Hellman

Principe

Diffie-Hellman

Principe

- Alice et Bob choisissent un groupe fini G d'ordre n et un générateur g de ce groupe publiquement.

Diffie-Hellman

Principe

- Alice et Bob choisissent un groupe fini G d'ordre n et un générateur g de ce groupe publiquement.
- Alice choisit au hasard a tel que $1 < a < n$ puis communique à Bob g^a .

Diffie-Hellman

Principe

- Alice et Bob choisissent un groupe fini G d'ordre n et un générateur g de ce groupe publiquement.
- Alice choisit au hasard a tel que $1 < a < n$ puis communique à Bob g^a .
- Bob choisit au hasard b tel que $1 < b < n$ puis communique à Alice g^b .

Diffie-Hellman

Principe

- Alice et Bob choisissent un groupe fini G d'ordre n et un générateur g de ce groupe publiquement.
- Alice choisit au hasard a tel que $1 < a < n$ puis communique à Bob g^a .
- Bob choisit 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.

Diffie-Hellman

Principe

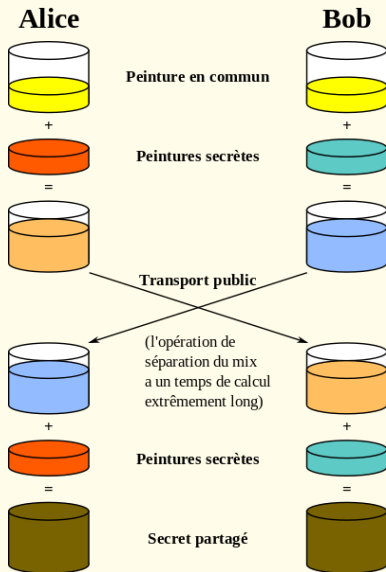
- Alice et Bob choisissent un groupe fini G d'ordre n et un générateur g de ce groupe publiquement.
- Alice choisit au hasard a tel que $1 < a < n$ puis communique à Bob g^a .
- Bob choisit au hasard b tel que $1 < b < n$ puis communique à Alice g^b .
- Alice élève à la puissance a le nombre communiqué par Bob.
- Bob élève à la puissance b le nombre communiqué par Alice.

Diffie-Hellman

Principe

- Alice et Bob choisissent un groupe fini G d'ordre n et un générateur g de ce groupe publiquement.
- Alice choisit au hasard a tel que $1 < a < n$ puis communique à Bob g^a .
- Bob choisit 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

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 l'ordre croissant de la clé de chiffrement.

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 l'ordre croissant de 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

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 l'ordre croissant de 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.
- On fera attention de retirer les espaces avant le cryptage et de les remettre lors du décryptage pour ne pas donner d'indication concernant les suites de mots.

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							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

Prolongements possibles

Les différents prolongements du sujet

- Conseillez Alice et Bob sur le choix du protocole de partage de clé.

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 ?

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.

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.
- Expliquez le problème du logarithme discret et son lien avec Diffie-Hellman.

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.
- Expliquez le problème du logarithme discret et son lien avec Diffie-Hellman.
- Algorithme “baby step giant step” et résolution du problème du logarithme discret dans Diffie-Hellman.

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.
- Expliquez le problème du logarithme discret et son lien 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 du programme**
- 3 Prolongements
- 4 Résultats
- 5 Conclusion

Présentation du programme

```
1 public class main{
2     public static void main(String[] args) {
3         PerfectGenerator generator = new PerfectGenerator()
4             ;
5         BigInteger g = generator.getG();
6         BigInteger p = generator.getP();
7
8         Person Alice = new Person(p,g, "Alice");
9         Person Bob = new Person("Bob");
10
11         Network network = new Network(Alice,Bob);
12
13         Alice.givePublicKey(network.initiateConversation(p,
14             g, Alice.getSelfPublicKey()));
15
16         network.send(Alice.encrypt("Bonjour, j'envoie un
17             message crypté!"));
18     }
19 }
```

Sommaire

1 Présentation du sujet

2 Présentation du programme

3 Prolongements

- Choix du protocole
- Prérequis des protocoles
- Attaque MITM
- TLS-SSL
- Logarithme discret
- Baby step giant step
- Attaque du chiffrement par transposition

4 Résultats

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

A 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 et appartient au domaine de la cryptographie à clé publique.

Prérequis des protocoles

Diffie-Hellman

A 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 et appartient au domaine de la cryptographie à clé publique.

Chiffrement par transposition

Nécessite une clé secrète connue des deux personnes pour permettre le cryptage et le décryptage des messages échangés. Dans notre cas, il pourrait être utilisé par Alice et Bob si ils s'étaient connus à l'Université et avaient échangé une clé de cryptage. Dans le cas où ils n'ont pas de clé en commun, ils devraient en mettre une en place.

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.

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.

Contre 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.

Principe

- Bob met en place une certification avec AC

Principe

- Bob met en place une certification avec AC
- Alice -> Bob ouvrir une communication sécurisée

Principe

- Bob met en place une certification avec AC
- Alice -> Bob ouvrir une communication sécurisée
- Bob -> Alice son certificat, sa clé publique et sa signature

Principe

- Bob met en place une certification avec AC
- Alice -> Bob ouvrir une communication sécurisée
- Bob -> Alice son certificat, sa clé publique et sa signature
- Alice vérifie que le certificat de Bob est valide

Principe

- Bob met en place une certification avec AC
- Alice -> Bob ouvrir une communication sécurisée
- Bob -> Alice son certificat, sa clé publique et sa signature
- Alice vérifie que le certificat de Bob est valide
- Alice -> Bob une clé de chiffrement (type Diffie-Hellman)

Principe

- Bob met en place une certification avec AC
- Alice -> Bob ouvrir une communication sécurisée
- Bob -> Alice son certificat, sa clé publique et sa signature
- Alice vérifie que le certificat de Bob est valide
- Alice -> Bob une clé de chiffrement (type Diffie-Hellman)
- Bob déchiffre et l'utilise pour communiquer (Diffie-Hellman)

Principe

- Bob met en place une certification avec AC
- Alice -> Bob ouvrir une communication sécurisée
- Bob -> Alice son certificat, sa clé publique et sa signature
- Alice vérifie que le certificat de Bob est valide
- Alice -> Bob une clé de chiffrement (type Diffie-Hellman)
- Bob déchiffre et l'utilise pour communiquer (Diffie-Hellman)
- Well Done ! La communication TLS est établie

Logarithme discret

Problème et lien avec Diffie-Hellman

Très utilisé en cryptographie à clé publique, 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

Baby step giant step

Principe

- p un nombre entier premier.
- $x = \log D(h) = m * q + r$ avec q et r entiers où $0 \leq r < m$
- $m = \lceil \sqrt{p} \rceil$

Baby step giant step

Principe

- p un nombre entier premier.
- $x = \log D(h) = m * q + r$ avec q et r entiers où $0 \leq r < m$
- $m = \lceil \sqrt{p} \rceil$
- On calcule g^i pour i allant de 0 à $m - 1$ et on stocke les résultats dans une table de hashage.

Baby step giant step

Principe

- p un nombre entier premier.
- $x = \log D(h) = m * q + r$ avec q et r entiers où $0 \leq r < m$
- $m = \lceil \sqrt{p} \rceil$
- 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 $q = 0$

Baby step giant step

Principe

- p un nombre entier premier.
- $x = \log D(h) = m * q + r$ avec q et r entiers où $0 \leq r < m$
- $m = \lceil \sqrt{p} \rceil$
- 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.

Baby step giant step

Principe

- p un nombre entier premier.
- $x = \log D(h) = m * q + r$ avec q et r entiers où $0 \leq r < m$
- $m = \lceil \sqrt{p} \rceil$
- 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.

Baby step giant step

Principe

- p un nombre entier premier.
- $x = \log D(h) = m * q + r$ avec q et r entiers où $0 \leq r < m$
- $m = \lceil \sqrt{p} \rceil$
- 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 $\log D(h) = q * m + 1$.

Baby step giant step

Utilisation

- Permet de réduire à un maximum de $2\sqrt{n}$ multiplications la recherche du logarithme discret dans un groupe G .
- 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

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

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.

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

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

Conclusion

Pour finir..

Nous avons découvert avec ce sujet les différents aspects de la cryptographie à clé publique et les mathématiques sur lesquelles ils sont basés. L'implémentation des algorithmes s'est révélée complexe afin de respecter les principes mathématiques comme celui du logarithme discret.

Nous avons pu aborder des sujets comme la recherche de nombre entiers premier très grand, les attaques possibles du programme mis en place, mais aussi la résolution du problème du logarithme discret.

Sommaire

1 Présentation du sujet

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

2 Présentation du programme

3 Prolongements

- Choix du protocole
- Prérequis des protocoles
- Attaque MITM
- TLS-SSL
- Logarithme discret
- Baby step giant step
- Attaque du chiffrement par transposition

4 Résultats

5 Conclusion