[Module sécurité informatique]

Échange des clés Diffie-Hellman

[Réalisé par]:

Temebr Omaima ,Sebgag safia ,belkhir Safaa

**Échange des clés Diffie-Hellman**

**1-Déffinition:**

L'échange de clés **Diffie-Hellman** est une méthode de cryptage spécifique développée par **Whitfield Diffie** et **Martin Hellman** et publiée

En 1976, l'une des premières mises en œuvre dans le domaine de la cryptographie

Et l’algorithme Diffie-Hellman est un des algorithmes les plus utilisés dans le cadre de la première étape : l’échange de clé.

L’objectif de Diffie-Hellman est de permettre l’établissement d’une clé privée entre deux parties, via l’échange de messages sur un canal non sécurisé. Lors de l’établissement d’une clé avec Diffie-Hellman, les messages sont en effet envoyés en clair sur le réseau, et toute personne qui intercepte les messages transmis ne doit pas pouvoir en déduire la clé générée.

**2-L'Application du Diffie-Hellman**

Tout le monde peut utiliser l'algorithme Diffie-Hellman, car ses brevets (logiciels, valables uniquement aux États-Unis) De manière générale, un tel protocole résout les situations d'échange d'informations privée sur un réseau totalement public.

Par exemple, sur une page web on peut trouver que toutes les pages sont accessibles à tous et il n'existe aucun moyen entre deux contributeurs d'avoir une

discussion privée sur le site. Avec Diffie-Hellman, c'est possible ; il suffit d'appliquer le protocole précédent.

**3-Fonctionnement de l’algorithme de Diffie-Hellman:**

le concept d'échange de clés

Dans un premier temps, un nombre commune est partagée entre A et B, qui peut être observée par un tiers intéressé

par la communication entre les deux.

L'étape suivante consiste pour A et B à choisir chacun leur clé secrète, qui n'est partagée avec personne.

Chacun fait un primaire avec des nombres commune et nombres leurs secrètes.

L'étape clé du processus est que A et B n'échangent que leurs nombres . Ces nombres, résultat

des combinaisons de nombre commune et des nombre secrètes, peuvent difficilement s'inverser et déterminer quelles nombre

secrètes A et B ont utilisées si un tiers écoute la communication.

A et B emploient alors leurs nombres secrètes sur nombres qu'ils ont reçus, générant des nombres

secondaires (clé commune) qui seront les mêmes pour A et B, sans qu'une tierce partie observant la communication

puisse produire ce mélange secondaire. A et B utilisent ainsi leur clé commune pour crypter et décrypter secrètement

leurs messages.

**4- Les éléments composent Diffie-Hellman (Les clés):**

Le principe de Diffie-Hellman est :

A et B disposent enfin d'un nombre, Bag mod n, qu'ils sont les seuls à connaître et qui, donc, peut leur servir de clef ; et pourtant, leurs échanges se sont faits devant tout le monde. Comment est-ce possible ?

est composé de suivant:

clé public(A) :est le clé de "A" qui connue par tout le monde.

clé privé(A): est le clé secret "A" qui générer par ex par le A .

Générateur (A,B),prime (A,B): sont des nombres qui sont commun entre les deux partie "A" et "B" et sont public aussi.

"privée" le génère au hasard .

"public"="Générateur" ^ "privée"(moi) mod "prime"

"secret" = "public"(l'autre) ^ "privé"(me) mod "prime"

"prime" et "Générateur" :génère par les deux parties "A" et "B" ;

pour le déchiffrement on utilise les mêmes fonctions de chiffrement

si l'on regarde bien on a trouver que

Finalement, les deux nombres sont identiques !

**5)** **Comment Calculer les clés et le message chiffrée...?**

"publique"="Générateur" ^ "privée"(moi) mod "prime"

"secret" = "publique"(l'autre) ^ "privée"(moi) mod "prime"

"prime" et "Générateur" sont connue ;

comment les nombre sont identiques ...!

Car

secret (A)="public"(B) ^ "privée"(A) mod "prime" => secret (A)= "Générateur"^ ”privé” (B)^mod “prime” ^ “privé” (A) mod “prime” .

secret (B)="public"(A) ^ "privée"(B) mod "prime" => secret (B)="Générateur" ^ “privé” (A)^mod “prime” ^ ”privé” (B) mod “prime” .

secret (A)= " Générateur "^privé (B) ^privé(A) ^mod prime)mod "prime” .

secret (B)=" Générateur "^privé (A) ^privé(B) ^mod prime)mod "prime” .

" Générateur "^privé (B)^ ^privé(A)=" Générateur "^privé (A) ^privé(B) =C

Donc

secret (A)= “C “^mod prime)mod ”prime”

secret (B)= ”C “^ mod prime)mod "prime”

Alors en fin

secret (A)= secret (B) .