Implémentation Diffie-Hellman & Blowfish dans un logiciel client serveur

Ollivier Romain - Bastide Vincent

Diffie Hellman

- Créé par Whitfield Diffie et Martin Hellman en 1976.
- Méthode d'échange de clés asymétrique pour les systèmes de chiffrement symétrique.

Diffie Hellman

- Principe :

  - Choix préalable d'un nombre premier p et d'une génératrice g communs à Alice et Bob.

Alice	Bob
- Choix d'un nombre a aléatoire 0 < a < p-1.	- Choix d'un nombre b aléatoire 0 < b < p-1.
- Calcul de $A = g^a \pmod p$.	- Calcul de $B = g^b \pmod p$.
Envoi A à Bob ◄——►	Envoi B à Alice
- Calcul de $k = B^a \pmod p$.	- Calcul de $k' = A^b \pmod p$.

k = k' : clé de cryptage qui sera utilisée par Blowfish.

Diffie Hellman

- Faiblesse de l'algorithme : attaque de l'homme du milieu.
- L'attaquant connait g et p.
- Se fait passer pour Alice auprès de Bob, et vice versa :

  - Réceptionne g^{a} d'Alice, transmet $g^{a'}$ à Bob.

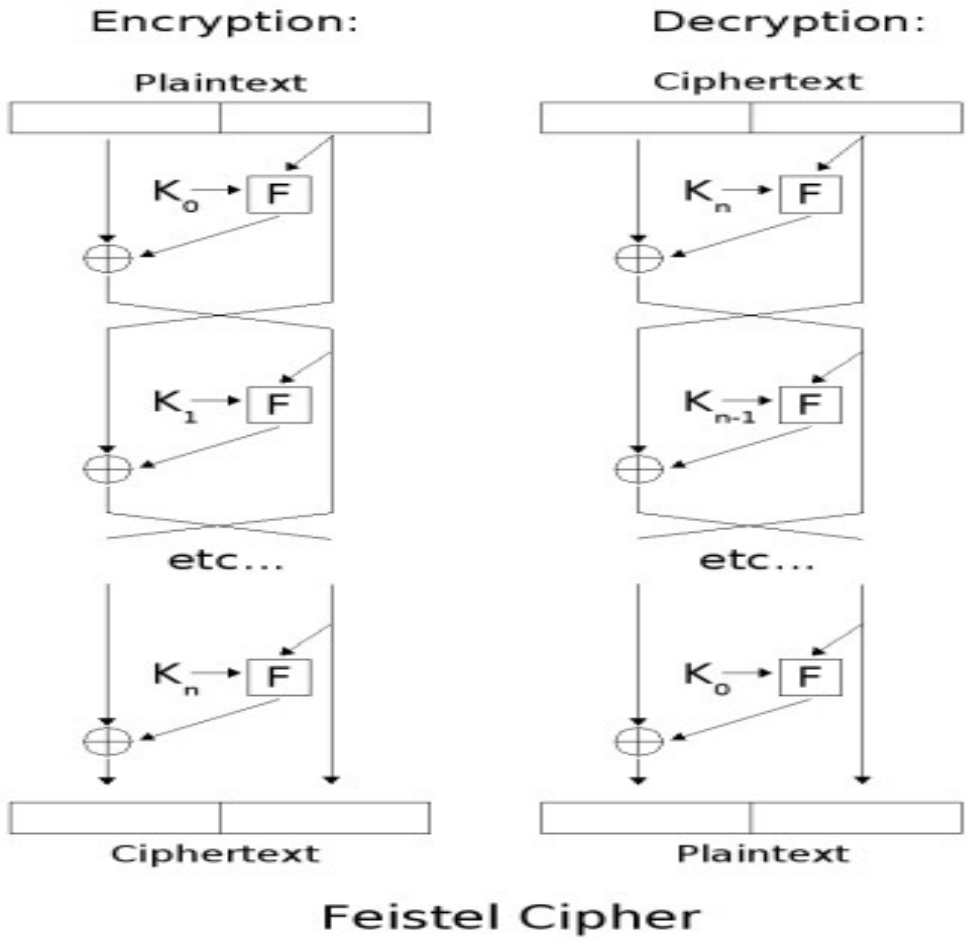
  - Réceptionne g^{b} de Bob, transmet $g^{b'}$ à Alice.
- Communique grâce à $g^{a'b}$ avec Bob, $g^{ab'}$ avec Alice.
- Parade : signer les messages échangés entre Alice et Bob à l'aide d'une paire de clé asymétriques.

Blowfish

- Inventé par Bruce Scheier en 1993
- Algorithme de chiffrement symétrique par blocs
- Utilise une combinaison de Réseau Feistel, S-Boxes et P-Boxes

Blowfish

- Réseau de Feistel:
  - Composé de « tours »
  - Constructions par blocs
  - Sous-clés Ki
  - Fonction F



Blowfish

- P-Boxes:
  - Tables de permutations
  - Tableaux 1D
  - Mélange les éléments

S-Boxes

Tables de substitutions

Tableaux 2D

A chaque entrée est associée une sortie

Pas forcément la même taille en entrée et en sortie

Blowfish

- Algorithme Blowfish:
- P-boxes et S-boxes contiennent des chiffres de Pi (forme hexa)
- P: 18 éléments, S: 4x256 éléments
- P et S sont ensuite initialisées avec la clé de chiffrement
- Réseau de Feistel en 16 tours

Blowfish

- Pour i de 1 à 16

xL = xL xor Pi

xR = F(xL) xor xR

switch xL, xR.

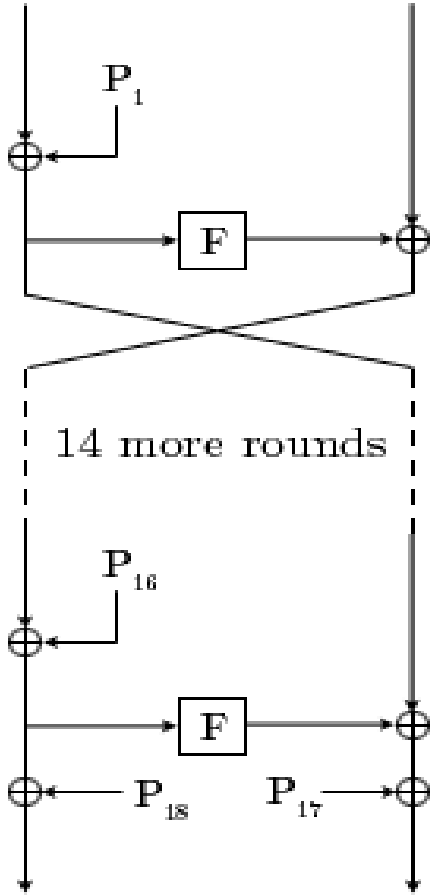
Fin boucle

- +2 opérations:

xR = xR xor P17

xL = xL xor P18

- D'où les 18 cases nécessaires à P
- F(xL) = [(S1,a + S2,b mod 2^32) xor S3,c] + S4,d mod 32
- a,b,c et d sont les 4 octets de xL (ou xR)



Le projet

- Logiciel client serveur en C
- Échange de messages & données avec TCP-IP + protocole
- Sources utilisées:

DH: gmp pour les grands nombres,

Blowfish: sources du site officiel

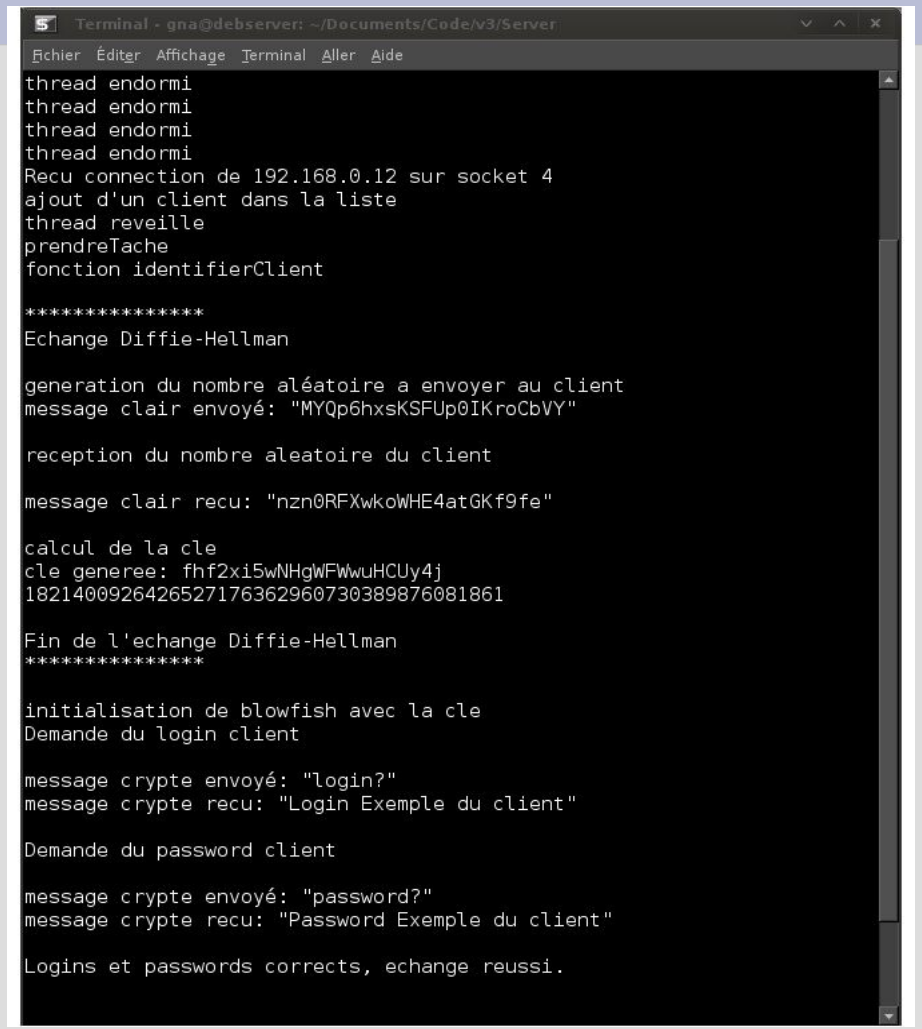
1- Échange de nombres

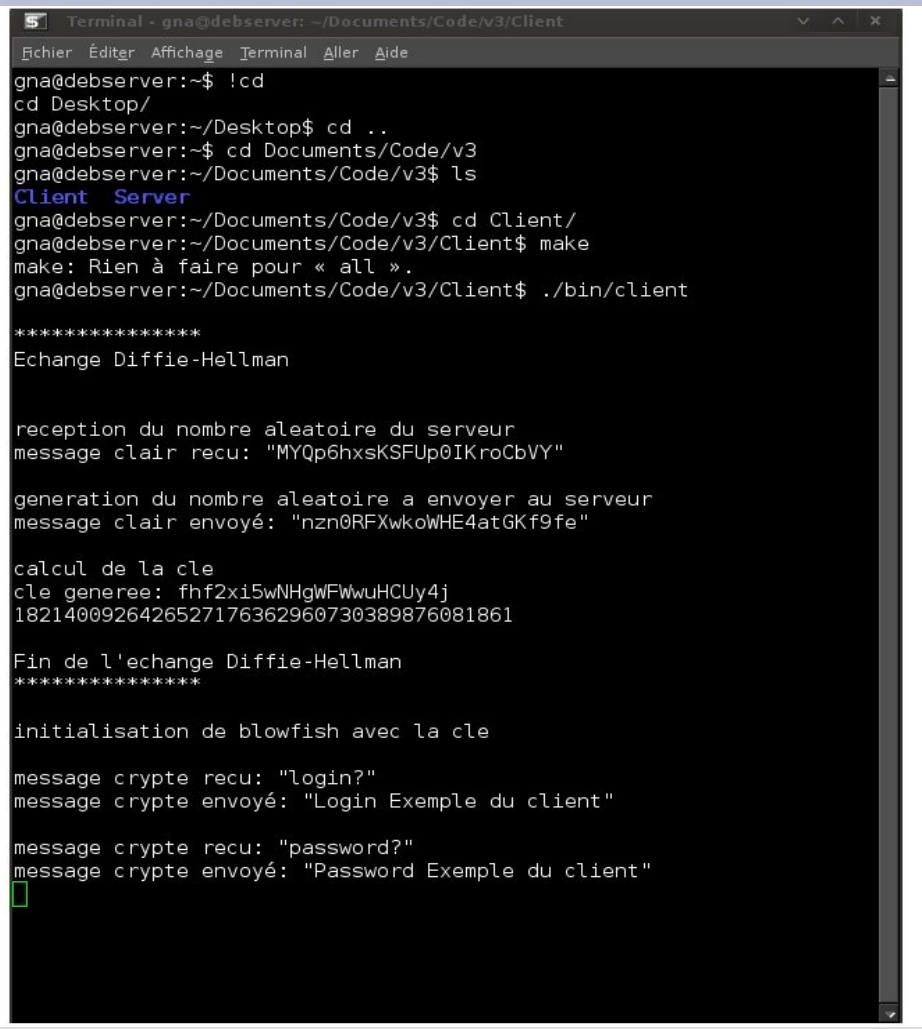
2- Génération de la clef

3- Initialisation de Blowfish (P-box et S-Box)

4- Les échanges chiffrés peuvent commencer.

Le projet


Terminal - gna@debserver: ~/Documents/Code/v3/Server
Fichier Éditer Affichage Terminal Aller Aide
thread endormi
thread endormi
thread endormi
thread endormi
Recu connection de 192.168.0.12 sur socket 4
ajout d'un client dans la liste
thread reveille
prendreTache
fonction identifierClient
****
Echange Diffie-Hellman
generation du nombre aléatoire a envoyer au client
message clair envoyé: "MYQp6hxsKSFUp0IKroCbVY"
reception du nombre aleatoire du client
message clair recu: "nzn0RFXwkoWHE4atGKf9fe"
calcul de la cle
cle generee: fhf2xi5wNHgWFWwuHCUy4j
1821400926426527176362960730389876081861
Fin de l'echange Diffie-Hellman
****
initialisation de blowfish avec la cle
Demande du login client
message crypte envoyé: "login?"
message crypte recu: "Login Exemple du client"
Demande du password client
message crypte envoyé: "password?"
message crypte recu: "Password Exemple du client"
Logins et passwords corrects, echange reussi.


Terminal - gna@debserver: ~/Documents/Code/v3/Client
Fichier Éditer Affichage Terminal Aller Aide
gna@debserver:~$!cd
cd Desktop/
gna@debserver:~/Desktop$ cd ..
gna@debserver:~$ cd Documents/Code/v3
gna@debserver:~/Documents/Code/v3$ ls
Client Server
gna@debserver:~/Documents/Code/v3$ cd Client/
gna@debserver:~/Documents/Code/v3/Client$ make
make: Rien à faire pour « all ».
gna@debserver:~/Documents/Code/v3/Client$ ./bin/client
****
Echange Diffie-Hellman
reception du nombre aleatoire du serveur
message clair recu: "MYQp6hxsKSFUp0IKroCbVY"
generation du nombre aleatoire a envoyer au serveur
message clair envoyé: "nzn0RFXwkoWHE4atGKf9fe"
calcul de la cle
cle generee: fhf2xi5wNHgWFWwuHCUy4j
1821400926426527176362960730389876081861
Fin de l'echange Diffie-Hellman
****
initialisation de blowfish avec la cle
message crypte recu: "login?"
message crypte envoyé: "Login Exemple du client"
message crypte recu: "password?"
message crypte envoyé: "Password Exemple du client"