

S_DES Simplifiée

Module : Sécurité et théorie de l'information

Responsable Module : Mr Victor MORARU

Formation : M1 Informatique.

Fait par :

- BENNACER Djamila
- MEHRABI JEYHOUNABADI Milad

L'algorithme du Simplified-DES (ou SDES) est une version simplifiée du DES (Data Encryption Standard). Les principes sont identiques mais la mise en œuvre est plus simple.

L'algorithme d'encryptage du SDES travaille sur la représentation ASCII du texte. Chaque caractère étant codé par 8 bits, ce sont ces 8 bits qui seront modifiés par l'algorithme de cryptage.

Pour utiliser la méthode SDES, on utilisera également une clé initiale de 10 bits (ici c'est : 1010000010). Cette clé servira au cryptage et au décryptage du texte.

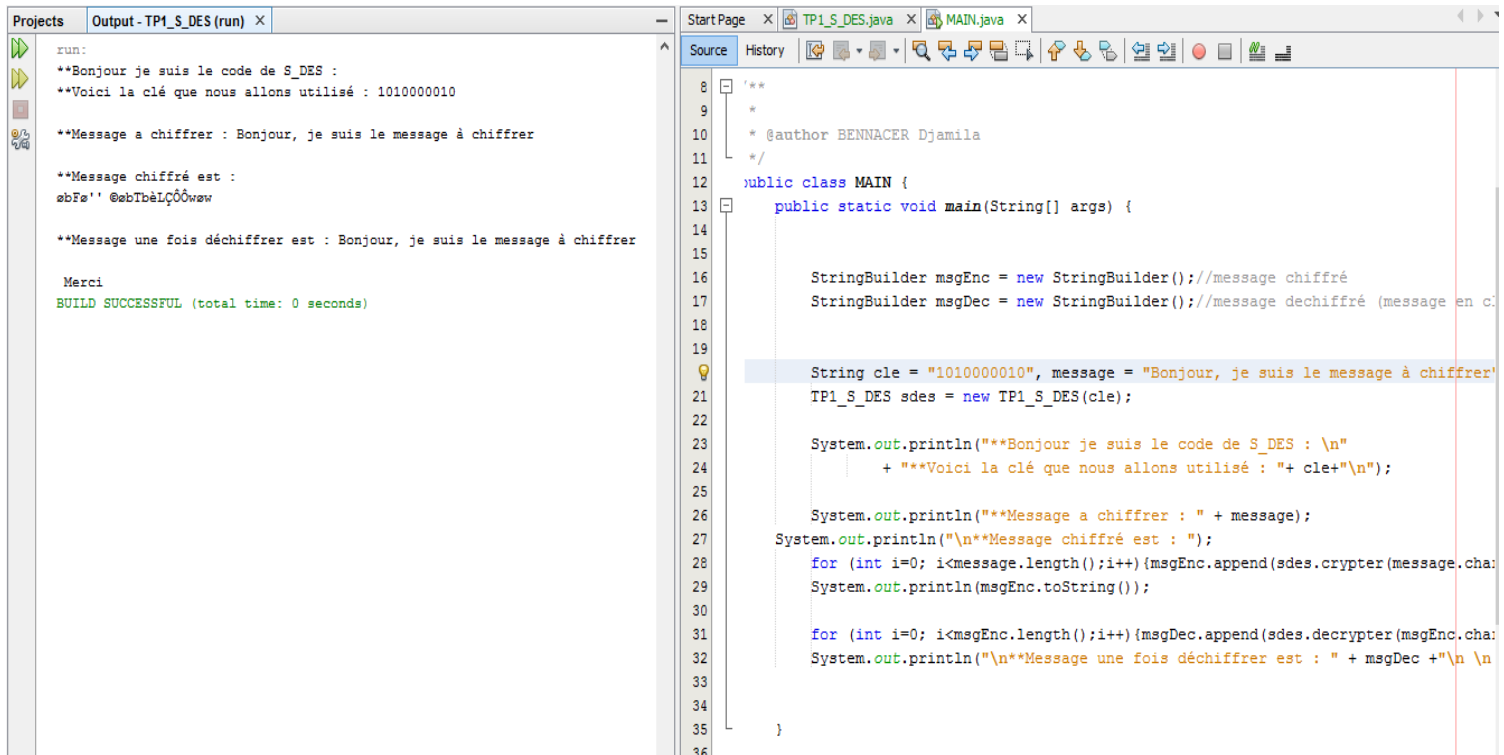
Ces étapes travaillent toutes sur un octet, et sont respectivement :

- Une permutation initiale des bits (IP).
- Une fonction complexe appelée f_k qui comprend des permutations, des substitutions et qui utilise la clé de cryptage.
- Une fonction de permutation (SW) qui échange les 4 premiers bits avec les 4 suivants.
- Appliquer une nouvelle fois f_k .
- Une permutation qui est l'inverse de la permutation initiale (IP⁻¹).

La partie complexe de l'algorithme qui utilise la clé de cryptage utilise en fait deux clés de cryptage de 8 bits appelées K1 et K2.

Une attaque par force brute sur l'algorithme S-DES est très simple. La clé ne mesure que 10 bits, il n'y a donc que 1024 possibilités.

Voici une capture d'écran du résultat obtenu :



```
run:
**Bonjour je suis le code de S_DES :
**Voici la clé que nous allons utilisé : 1010000010

**Message a chiffrer : Bonjour, je suis le message à chiffrer

**Message chiffré est :
ebFw'' @ebTbêLÇÔÔwew

**Message une fois déchiffrer est : Bonjour, je suis le message à chiffrer

Merci
BUILD SUCCESSFUL (total time: 0 seconds)
```

```
8  /**
9  *
10 * @author BENNACER Djamila
11 */
12 public class MAIN {
13     public static void main(String[] args) {
14
15
16         StringBuilder msgEnc = new StringBuilder();//message chiffré
17         StringBuilder msgDec = new StringBuilder();//message déchiffré (message en c
18
19
20         String cle = "1010000010", message = "Bonjour, je suis le message à chiffrer"
21         TP1_S_DES sdes = new TP1_S_DES(cle);
22
23         System.out.println("***Bonjour je suis le code de S_DES : \n"
24             + "***Voici la clé que nous allons utilisé : "+ cle+"\n");
25
26         System.out.println("***Message a chiffrer : " + message);
27         System.out.println("\n***Message chiffré est : ");
28         for (int i=0; i<message.length();i++){msgEnc.append(sdes.crypter(message,cha
29         System.out.println(msgEnc.toString());
30
31         for (int i=0; i<msgEnc.length();i++){msgDec.append(sdes.decrypter(msgEnc,cha
32         System.out.println("\n***Message une fois déchiffrer est : " + msgDec +"\n \n
33
34
35     }
36 }
```

Pour la répartition du travail :

La moitié du TP a été faite avant le confinement, ce qui nous a permis de travailler ensemble au même endroit.

Par la suite nous avons utilisé discord pour continuer le TP.

On a essayé de mettre sur le code du TP qui a fait quoi.

Je vous remercie pour votre attention.