INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Département Sécurité et Technologies Informatiques

Cryptograhie – TD2

Jérémy Briffaut <jeremy.briffaut@insa-cvl.fr>

Jean-Christophe Deneuville <jean-christophe.deneuville@insa-cvl.fr>

Lundi 17 septembre 2018

Pour ce TD, un template vous est fourni. Téléchargez et décompressez l'archive `TD2.zip`.

Exercice 1 Étude des fichiers `bit.h` et `bit.c`

1. Pour chacune des fonctions suivantes, précisez :
   a. à quoi elles servent,
   b. à quoi correspondent les arguments, et
   c. quelle est la valeur retournée.

```
int bit_get(const unsigned char *bits, int pos);
```

Réponse :

a. _____

b. _____

c. _____

```
void bit_set(unsigned char *bits, int pos, int etat);
```

Réponse :

a. _____

b. _____

c. _____

```
void bit_xor(const unsigned char *bits1, const unsigned char *bits2,
↪  unsigned char *bitsx, int taille);
```

Réponse :

a. _____

b. _____

c. _____

```
void bit_rot_left(unsigned char *bits, int taille, int nbre);
```

Réponse :

a. _____

b. _____

c. _____

2. Que fait le code suivant ?

```
masque = 0x80;
for (i = 0; i < (pos % 8); i++)
    masque = masque >> 1;
```

Exercice 2 Étude tude du fichier `des.c`

1. À quoi correspondent les tableaux suivants :
   - `Des_Transform` : _____
   - `Des_Rotations` : _____
   - `Des_Permute` : _____
   - `Des_Initial` : _____
   - `Des_Expansion` : _____
   - `Des_Sbox` : _____
   - `Des_Pbox` : _____
   - `Des_Final` : _____
2. Décrire les différentes étapes de la fonction `main` :

   _____

   _____

   _____

Exercice 3 Chiffrement DES

1. Compléter le code du fichier `des.c` (Vous devez compléter les 4 balises TODO).
2. Tester votre fonction de chiffrement DES.
   a) Comment chiffrer ? _____
   b) Comment déchiffrer ? _____
3. À l'aide de ce code, réaliser une application qui permet de chiffrer/déchiffrer un fichier à l'aide d'une clé DES passée en paramètre.
4. Incorporer votre code dans votre librairie du projet.