NF05 Projet Cryptographie

Aya Abdala et Aurélien Dureux
Version Finale
Semestre Automne 2020

Table des matières

Table des matières

Documentation projet

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
#include <string.h>
#include <time.h>
```

Macros

- #define **CRYPT** 0
  Permet de définir l'opération effectuée.
- #define **DECRYPT** 1
  Permet de définir l'opération effectuée.
- #define **FALSE** 0
  Booléen pour contrôle sortie de certaines boucles.
- #define **NB_BIT** 8
  Valeur définie pour fixer le nombre de bit par octet.
- #define **NB_OCTET** 4
  Valeur définie pour fixer le nombre d'octet par paquet.
- #define **TRUE** 1
  Booléen pour contrôle sortie de certaines boucles.

Fonctions

- void **etape_1_crypt** (int *oct, const char *key)
  Etape de cryptage 1 - Associe à chaque valeur une autre valeur par ajout valeurs ASCII termes de clé
- void **etape_1_decrypt** (int *oct, const char *key)
  Etape de cryptage 1 - Associe à chaque valeur une autre valeur par retrait valeurs ASCII termes de clé

- void etape_2_crypt_decrypt (int *oct)
  Etape de cryptage et décryptage 2 - Associe à chaque x un y grâce au fichier permut_etape_2.txt.

- void **etape_3_crypt** (int **bits_oct)
  Etape de cryptage 3 - Calcul matriciel selon constantes imposées dans le sujet.
- void **etape_3_decrypt** (int **bits_oct)
  Etape de décryptage 3 - Calcul matriciel selon constantes imposées dans le sujet.

- void **etape_4_crypt** (int **bits_oct, int nb_iteration, int etape_iteration, char *key)
  Etape de cryptage 4 - Genere sous_clé via clé et étape pour ensuite faire XOR bit par bit.
- void **etape_4_decrypt** (int **bits_oct, int nb_iteration, int etape_iteration, char *key)
  Etape de décryptage 4 - Genere sous_clé via clé et étape pour ensuite faire XOR bit par bit.

- void **etape_5_crypt** (int *oct)
  Etape de cryptage 5 - Calcul système imposé par le sujet.
- void **etape_5_decrypt** (int *oct)
  Etape de décryptage 5 - Calcul inverse système etape 5 crypt imposée par le sujet.

- int **main** ()
  Saisie des informations necessaires et effecture lecture et écriture dans les fichiers.

- void **pass_binary** (int *oct, int **bits_oct)
  Passage de valeurs decimales a valeurs binaires.
- void **pass_decimal** (int **bits_oct, int *oct)
  Passage de valeurs binaires a valeurs decimales.

- char * saisie_chaine_dynam ()
  Saisie une chaîne dynamiquement sans connaître sa taille à l'avance.
- void **sous_cle** (int mode, int nb_it_tot, int etape_it, char *key, int sub_key[])
  Generation sous-cles a partir clé de cryptage et etape d'itération pour étape 4 cryptage

---

Documentation des macros

#define CRYPT 0

Permet de définir l'opération effectuée.

Définition à la ligne 11 du fichier code_cryptographie_Dureux_Abdala.c.

#define DECRYPT 1

Permet de définir l'opération effectuée.

Définition à la ligne 15 du fichier code_cryptographie_Dureux_Abdala.c.

#define FALSE 0

Booléen pour contrôle sortie de certaines boucles.

Définition à la ligne 19 du fichier code_cryptographie_Dureux_Abdala.c.

#define NB_BIT 8

Valeur définie pour fixer le nombre de bit par octet.

Définition à la ligne 33 du fichier code_cryptographie_Dureux_Abdala.c.

#define NB_OCTET 4

Valeur définie pour fixer le nombre d'octet par paquet.

Définition à la ligne 29 du fichier code_cryptographie_Dureux_Abdala.c.

#define TRUE 1

Booléen pour contrôle sortie de certaines boucles.

Définition à la ligne 23 du fichier code_cryptographie_Dureux_Abdala.c.

Documentation des fonctions

etape_1_crypt (int * *oct*, const char * *key*)

Description

Etape de cryptage 1 - Associe à chaque valeur une autre valeur par ajout valeurs ASCII termes de clé

Paramètres

**oct*	Passage par adresse tableau des octets
**key*	Passage clé de chiffrement (const : car même si passage par adresse aucune modification sur la clé)

Renvoie

N/A

Définition à la ligne 93 du fichier code_cryptographie_Dureux_Abdala.c.

void etape_1_decrypt (int * *oct*, const char * *key*)

Description

Etape de cryptage 1 - Associe à chaque valeur une autre valeur par retrait valeurs ASCII termes de clé

Paramètres

**oct*	Passage par adresse tableau des octets
**key*	Passage clé de chiffrement (const : car même si passage par adresse aucune modification sur la clé)

Renvoie

N/A

Définition à la ligne 114 du fichier code_cryptographie_Dureux_Abdala.c.

etape_2_crypt_decrypt (int * *oct*)

Description

Etape de cryptage et décryptage 2 - Associe à chaque x un y grâce au fichier permut_etape_2.txt.

Paramètres

**oct*	Passage par adresse tableau des octets

Renvoie

N/A

Définition à la ligne 142 du fichier code_cryptographie_Dureux_Abdala.c.

etape_3_crypt (int ** *bits_oct*)

Description

Etape de cryptage 3 - Calcul matriciel selon constantes imposées dans le sujet.

Paramètres

***bits_oct*	Passage par adresse tableau des octets de 8 bits

Renvoie

N/A

Définition à la ligne 183 du fichier code_cryptographie_Dureux_Abdala.c.

etape_3_decrypt (int ** *bits_oct*)

Description

Etape de décryptage 3 - Calcul matriciel selon constantes imposées dans le sujet.

Paramètres

***bits_oct*	Passage par adresse tableau des octets de 8 bits

Renvoie

N/A

Définition à la ligne 224 du fichier code_cryptographie_Dureux_Abdala.c.

etape_4_crypt (int ** *bits_oct*, int *nb_iteration*, int *etape_iteration*, char * *key*)

Description

Etape de cryptage 4 - Genere sous_clé via clé et étape pour ensuite faire XOR bit par bit.

Paramètres

***bits_oct*	Passage par adresse tableau des octets de 8 bits
nb_iteration	Nombre d'itération totale pour génération sous-clé
etape_iteration	Etape actuelle d'itération pour génération sous-clé
**key*	Clé de chiffrement via son adresse

Renvoie

N/A

Définition à la ligne 303 du fichier code_cryptographie_Dureux_Abdala.c.

etape_4_decrypt (int ** *bits_oct*, int *nb_iteration*, int *etape_iteration*, char * *key*)

Description

Etape de décryptage 4 - Genere sous_clé via clé et étape pour ensuite faire XOR bit par bit.

Paramètres

**bits_oct*	Passage par adresse tableau des octets de 8 bits
nb_iteration	Nombre d'itération totale pour génération sous-clé
etape_iteration	Etape actuelle d'itération pour génération sous-clé
**key*	Clé de chiffrement via son adresse

Renvoie

N/A

Définition à la ligne 325 du fichier code_cryptographie_Dureux_Abdala.c.

etape_5_crypt (int * *oct*)

Description

Etape de cryptage 5 - Calcul système imposé par le sujet.

Paramètres

**oct*	Passage par adresse tableau des octets

Renvoie

N/A

Définition à la ligne 347 du fichier code_cryptographie_Dureux_Abdala.c.

etape_5_decrypt (int * *oct*)

Description

Etape de décryptage 5 - Calcul inverse système etape 5 crypt imposée par le sujet.

Paramètres

**oct*	Passage par adresse tableau des octets

Renvoie

N/A

Définition à la ligne 372 du fichier code_cryptographie_Dureux_Abdala.c.

main ()

Description

Saisie des informations necessaires et effecture lecture et écriture dans les fichiers.

Paramètres

N/A	

Renvoie

N/A

Définition à la ligne 435 du fichier code_cryptographie_Dureux_Abdala.c.

pass_binary (int * *oct*, int ** *bits_oct*)

Description

Passage de valeurs decimales a valeurs binaires.

Paramètres

**oct*	Passage par adresse tableau des octets
***bits_oct*	Passage par adresse tableau octets de 8 bits

Renvoie

N/A

Définition à la ligne 43 du fichier code_cryptographie_Dureux_Abdala.c.

pass_decimal (int ** *bits_oct*, int * *oct*)

Description

Passage de valeurs binaires a valeurs decimales.

Paramètres

***bits_oct*	Passage par adresse tableau octets de 8 bits
**oct*	Passage par adresse tableau des octets

Renvoie

N/A

Définition à la ligne 67 du fichier code_cryptographie_Dureux_Abdala.c.

* saisie_chaine_dynam ()

Description

Saisie une chaîne dynamiquement sans connaître sa taille à l'avance.

Paramètres

N/A	

Renvoie

chaine Chaine de caractère saisie

Définition à la ligne 401 du fichier code_cryptographie_Dureux_Abdala.c.

void sous_cle (int *mode*, int *nb_it_tot*, int *etape_it*, char * *key*, int *sub_key*[])

Description

Etape de décryptage 4 - Genere sous_clé via clé et étape pour ensuite faire XOR bit par bit.

Paramètres

mode	Permet de savoir si l'on est en cryptage (0) ou en décryptage (1)
nb_it_tot	Nombre total d'itérations
etape_it	Etape actuelle d'itération
**key*	Pointeur de la clé de chiffrement
Sub_key[]	Variable de la sous_cle

Renvoie

N/A

Définition à la ligne 271 du fichier code_cryptographie_Dureux_Abdala.c.