Table des matières

1. Contraintes administratives
2. Rendu
3. Description
4. Étape 1
5. Étape 2

1 Contraintes administratives

- Le projet est à rendre pour le dimanche soir 23h 42min 42s,
- Le sujet est à faire par groupe de 2 personnes,
- La soutenance est *obligatoire*, même si vous n'avez rien fait,
- Vous serez notés par groupe (une note pour tout le groupe),
- Tout ajout ou complément au sujet est susceptible de se produire et se trouvera dans le forum,
- Vous devez valider votre participation au rush et donc à la soutenance sur l'intra. En cas d'absence la sanction sera -21,
- Vous n'avez le droit qu'à la libc.

2 Rendu

2.1 Géneralité

- Vous devez obligatoirement rendre toutes vos sources.

2.2 Dépôt

- Le rendu se fait via *git* sur le compte du chef de groupe,
- Vous devez mettre les droits en lecture pour le compte rush,
- Le nom du dépôt est *elcrypt*.

2.3 Makefile

Il doit y avoir un Makefile qui contient :

- Règle *clean* qui efface tous les objets,
- Règle *fclean* qui efface tous les objets et les exécutables,
- Règle *re* qui procède à un fclean puis à un all,
- Règle *all* qui compile le projet,
- Vous devez obligatoirement compiler sans warning avec les options de compilation suivantes : *-W -Wall -ansi -pedantic*,
- La règle par defaut est *all*.
- Faites attention à ne pas relinker vos fichiers s'ils n'ont pas été modifiés. Sachez faire un Makefile !

2.4 Ficher auteur

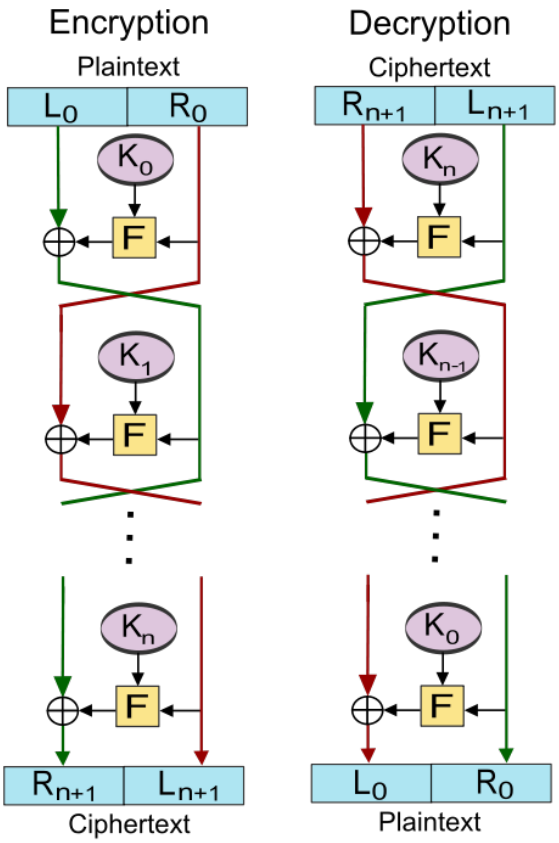
Il doit y avoir un fichier nommé auteur qui contiendra les logins de toutes les personnes du groupe, chacun suivi d'un \n, tel que :

```
(elbarto@atlantis) cat -e auteur
elbarto$
sha-1$
(elbarto@atlantis)
```

3 Description

ElCrypt est un algorithme de chiffrement symétrique.
Il chiffre les données par bloc de 64 bits avec une clef, elle aussi de 64 bits.
L'algorithme utilise un réseau de Feistel avec un nombre de tours de huit.

3.1 Réseau de Feistel



http://en.wikipedia.org/wiki/Feistel_cipher#mediaviewer/File:Feistel_cipher_diagram_en.svg

3.2 Clef

La clef primaire est composé de 64 bits. Dans ces 64 bits le bit de poids faible de chaque octets est un bit de parité.
Dans la version 1 de l'algorithme ElCrypt nous omettrons ces bits, ce qui nous donne une clef de 56 bits.
Dans la suite du sujet, lorsque nous parlons de clef primaire, c'est la clef sans les bits de parité que nous évoquons.

3.3 Rotation de clef

Pour chaque tour du réseau de Feistel, une clef est générée à partir de la clef primaire.
Pour obtenir la clef secondaire il suffit d'effectuer une rotation de la clef primaire vers la gauche de 4 bits et de répeter cette opération N fois par rapport au tour actuel.
Il suffit ensuite de prendre seulement les 32 derniers bits.
Les tours commencent à 0 donc la première clef secondaire est simplement les 32 derniers bits de la clef primaire.

3.4 Fonction de Feistel

La fonction de Feistel de ElCrypt version 1 est un simple ou-exclusif entre le bloc de 32 bits et la clef secondaire.

3.5 Algorithme

Pour chaque bloc de 64 bits :

1. Séparer le bloc en deux sous-bloc de 32 bits,
2. Appliquer les opérations du réseau de Feistel. (clef secondaire, fonction de Feistel, ou-exclusif ...)

3.6 Padding

Si la taille du fichier n'est pas un multiple de 64 bits nous devons padder le dernier bloc.
La méthode choisie pour ElCrypt est le padding PKCS5.
Cette méthode *padde* tous les octets avec le nombre d'octets à *padder*.

Par exemple si le bloc est 0xDE 0xAD,
Alors, le bloc *paddé* est 0xDE 0xAD 0x06 0x06 0x06 0x06 0x06 0x06.

Si la taille du fichier est un multiple de 64 bits, nous rajoutons simplement un bloc en plus avec uniquement des octets de padding.
Il faut bien sûr prendre en compte cela lors du déchiffrage.

4 Etape 1

Vous devez fournir un binaire nommé *elcrypt* qui prend en paramètre :

- *-d* le binaire va procéder à un déchiffrement,
- *-e* le binaire va procéder à un chiffrement,
- *-f fichier* le fichier source,
- *-o fichier* le Fichier qui contiendra le résultat de l'opération,
- *-k clef* la clef primaire de 64 bits.

Les opérations de chiffrement et de déchiffrement sont mutuellement exclusives.

5 Etape 2

Les conditions d'accès à l'étape 2 seront annoncées sur le forum en temps voulu.

6 Pour finir

- Toutes les modifications de sujet seront annoncées sur le forum, s'en suivra une mise à jour du sujet sur l'intra.
- Le sujet pourra changer jusqu'a 1H avant le rendu.
- Toutes vos questions doivent être posées sur le forum.
- La section du forum à utiliser est:
    1. B4 - C - Systeme Unix

Bon travail.