Cryptographie et sécurité
Département d'Informatique
Université de Genève

9 novembre 2000

José Rolim, Frédéric Schütz

---

## Exercice 1

Prouver que le déchiffrement de DES peut se faire en utilisant l'algorithme de chiffrement dans lequel on a inversé l'ordre des sous-clés (*Stinson, ex. 3-1.*)

## Exercice 2

On note $\mathrm{DES}(x, K)$ le message chiffré par la clé $K$ du texte clair $x$ suivant le système DES. Si $y = \mathrm{DES}(x, K)$, et $y' = \mathrm{DES}(c(x), c(K))$ où $c(\cdot)$ est la fonction qui inverse tous les bits de son argument, montrer que $y' = c(y)$. Autrement dit, si l'on complémente le texte clair et la clef, on obtient le texte chiffré complémenté. Noter que cela se montre avec la description globale de DES (la structure des boîtes-S et autres composantes est inutile) (*Stinson, ex. 3-2.*).

## Exercice 3

Une manière de renforcer DES consiste à faire un *double chiffrement* : étant donnés deux clés $K_1$ et $K_2$, on définit $y = e_{K_2}(e_{K_1}(x))$ (c'est évidemment le produit de DES avec lui-même). Si la fonction de chiffrement $e_{K_2}$ est la même que la fonction de déchiffrement $d_{K_1}$, les clés $K_1$ et $K_2$ sont dites *duales*. De telles clés sont indésirables, car le texte chiffré est toujours égal au texte clair. Une clé est auto-duale si elle est sa propre duale.

(a) Montrer que si $C_0$ à tous ses bits identiques (à 0 ou à 1), et si $D_0$ aussi, alors $K$ est auto-duale.
(b) Montrer que les clés suivantes (en notation hexadécimale) sont auto-duales :

```
0101010101010101
FEFEFEFEFEFEFEFE
1F1F1F1F0E0E0E0E
E0E0E0E0F1F1F1F1
```

(c) Montrer que si $C_0 = 0101\ldots01$ ou $1010\ldots10$ (en binaire), alors le ou-exclusif des chaînes $C_i$ et $C_{17-i}$ sont $1111\ldots11$ pour $1 \leq i \leq 16$ (on montre la même chose avec $D$).
(d) Prouver que les paires de clés suivantes (en hexadécimal) sont duales :

```
E001E001F101F101    01E001E001F101F1
FE1FFE1FFE0EFE0E    1FFE1FFE0EFE0EFE
E01FE01FFF10FF10    1FE01FE00EF10EF1
```

(*Stinson, ex. 3-3.*)