Final SR50
UTBM – A2017

abderrahim.chariete@utbm.fr

Protocoles de sécurité

-Documentations autorisées-

Faites un exercice au choix !

Exercice 1 : **(30 mn, 5 pts) Protocole D.E.S.**

Supposons que les sous-clés k_i sont toutes égales.

1. **(2 pts)** Montrer que les bits de G_0 sont tous égaux, ainsi que ceux de D_0.
2. **(1 pts)** En déduire les 4 clés D.E.S. pour lesquelles toutes les sous-clés sont les mêmes.
3. **(2 pts)** Déterminer ces 4 clés faibles.

Exercice 2 : (30mn, 5 pts) Protocole D.E.S.

Soit le message en clair M écrit en hexadécimale (64 bits). M = 0123456789ABCDEF

Soit la clé K écrite en hexadécimale (64 bits). K = 133457799BBCDFF1

Nous allons donc réaliser **la première ronde** du protocole D.E.S.

1. **(1 pt)** Ecrire M en binaire et déduire G_0 et D_0. Puis, écrire K en binaire et déduire G_0 et D_0.
2. **(2 pts)** Calculer k_0 (48 bits). Donner toutes les étapes de calcul.
3. **(2 pts)** Calculer G_1 (32 bits) et D_1 (32 bits). Donner toutes les étapes de calcul.