Théophile MOLINATTI TD3A, Gabriel DOS SANTOS TD4A

Rapport : Devoir maison IN603

Déchiffrement :

Pour le déchiffrement nous commençons par inverser la S-box ce qui nous donne :

indice	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
valeur	5	E	F	8	C	1	2	D	B	4	6	3	0	7	9	A

Nous inversons également la P-box : (voir fichier annexe pour plus d'information sur l'implémentation)

indice	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
valeur	0	4	8	12	16	20	1	5	9	13	17	21	2	6	10	14	18	22	3	7	11	15	19	23

Nous appliquons l'algorithme de chiffrement à l'envers : on commence par XOR le message avec la sous clé 11. On permute le message puis on le substitue et nous effectuons un XOR du message avec un sous clé. Ces trois étapes sont répétées dix fois de la sous clé 10 à la sous clé 1.

Attaque :

Nous avons décidé de stocker tous les chiffrés possibles pour le message 1 et tous les clairs possibles pour le chiffré 1 dans deux tableaux de type unsigned long long de taille 2^24. Nous remplissons les deux tableaux en même temps, ce qui nous permet de créer les sous clés une seule fois pour chiffrer et déchiffrer. Une case du tableau étant sur 64 bit on stocke sur les 24 premiers bits (bits de poids faible) le message, puis sur les 24 bit suivant la clé utilisée. Les bits restants sont laissés à zéro.

Représentation d'une case du tableau : avec K, un bit de la clé et M, un bit du message

00000000 00000000 KKKKKKKK KKKKKKKK KKKKKKKK MMMMMMMM MMMMMMMM MMMMMMMM

Nous trions ensuite les deux tableaux avec un algorithme de tri par base. Nous avons choisi ce dernier pour sa complexité en temps de O(nk) et son efficacité pour trier des nombres.

Une fois le tri terminé, on utilise un algorithme de recherche par dichotomie afin de trouver des collisions dans les deux tableaux. Lorsqu'une collision est trouvée (on trouve un message identique dans les deux tableaux), on vérifie les cases alentour dans le tableau afin de vérifier d'éventuelles autres collisions. Dans ce cas, on vérifie que les couples de clé (k1, k2) sont valides. Pour cela on chiffre le message 2 avec la clé k1, puis on re-chiffre la sortie avec k2 et on compare le résultat avec le chiffré 2. Si les messages sont identiques, alors nous affichons le couple de clé k1, k2 en précisant qu'il est valide. On répète les mêmes étapes pour la case trouvée par la recherche dichotomique.

Pour Théophile l'attaque nous donne le couple de clé (k1, k2) = (6deda7, e7141f).
Pour Gabriel l'attaque nous donne les couples de clé (k1, k2) = { (009dbe, 6c198b), (57f0b5, 28baf5), (37048e, 4af525) }.

Voir annexe pour plus d'information sur les choix d'optimisations et les performances du programme.