TP : SIMPLIFIED IDEA ALGORITHM

IDEA est un algorithme de chiffrement symétrique conçu par Anas Ftouh, Othman Bechchar, Xuejia Lai, XuejiaLai et James Massey, et fut décrit pour la première fois en 1991.

L'algorithme IDEA a été breveté par la société suisse Mediacrypt ; le brevet a expiré en 2011 en Europe, et en janvier 2012 aux États-Unis et au Japon. Mediacrypt met en avant depuis mai 2005 son nouveau chiffrement nommé « IDEA NXT » qui est en fait FOX.

Survol

IDEA est un algorithme de chiffrement symétrique par blocs utilisé pour chiffrer et déchiffrer des données. Il manipule des blocs de texte en clair de 64 bits. Une clé de chiffrement longue de 128 bits (qui doit être choisie aléatoirement) est utilisée pour le chiffrement des données. La même clé secrète est requise pour les déchiffrer.

Comme tous les algorithmes de chiffrement par blocs, IDEA utilise à la fois la confusion et la diffusion. L'algorithme consiste à appliquer huit fois une même transformation (ou ronde ci-après) suivi d'une transformation finale (appelée demi-ronde). Lors de chaque ronde est appliquée une combinaison d'opérations de différents groupes algébriques, facilement réalisables tant sous forme logicielle que matérielle :

- OU exclusif (représenté par un $\oplus$)
- Addition modulo 216 (représenté par un $\boxplus$)
- Multiplication modulo 216+1 (représenté par un $\odot$)

Toutes ces opérations manipulent des sous-blocs de 16 bits. Cet algorithme est ainsi efficace même sur des processeurs 16 bits.

Description

Un bloc de données de 64 bits à chiffrer est divisé en 4 sous-blocs de 16 bits : X1, X2, X3 et X4. Ces quatre sous-blocs deviennent les entrées de la première des huit rondes de l'algorithme. À chaque ronde, les 4 sous-blocs sont combinés par OU exclusif, additionnés, multipliés entre eux ainsi qu'avec 6 sous-clés K1 ... K6 de 16 bits dérivés de la clé de chiffrement. Entre chaque ronde, les deuxième et troisième sous-blocs sont permutés. Enfin, les quatre sous-blocs obtenus après la huitième ronde sont traités avec quatre dernières sous-clés dans une transformation finale.

Chaque ronde utilisant 6 sous-clés de 16 bits distinctes et la transformation finale utilisant 4 sous-clés, un total de 52 sous-clés est donc requis. Les premières 8 sous-clés sont extraites directement de la clé de chiffrement de 128 bits, avec K1 étant pris dans

les 16 bits de poids le plus faible. Une première rotation gauche de 25 bits de la clé de chiffrement est opérée après que les 8 premières sous-clés ont été extraites. Afin d'extraire les 52 sous-clés requises, 6 rotations au total seront nécessaires.

Ronde

À chaque ronde, la séquence d'évènements est la suivante (voir les opérations étapes sur le schéma ci-contre) :

1. Multipliez X1 et la première sous-clé K1;
2. Additionnez X2 et la deuxième sous-clé K2;
3. Additionnez X3 et la troisième sous-clé K3;
4. Multipliez X4 et la quatrième sous-clé K4;
5. Combinez par OU exclusif les résultats des étapes (1) et (3) ;
6. Combinez par OU exclusif les résultats des étapes (2) et (4) ;
7. Multipliez le résultat de l'étape (5) avec la cinquième sous-clé K5;
8. Additionnez les résultats des étapes (6) et (7) ;
9. Multipliez le résultat de l'étape (8) par la sixième sous-clé K6;
10. Additionnez les résultats des étapes (7) et (9) ;
11. Combinez par OU exclusif les résultats des étapes (1) et (9) ;
12. Combinez par OU exclusif les résultats des étapes (3) et (9) ;
13. Combinez par OU exclusif les résultats des étapes (2) et (10) ;
14. Combinez par OU exclusif les résultats des étapes (4) et (10).

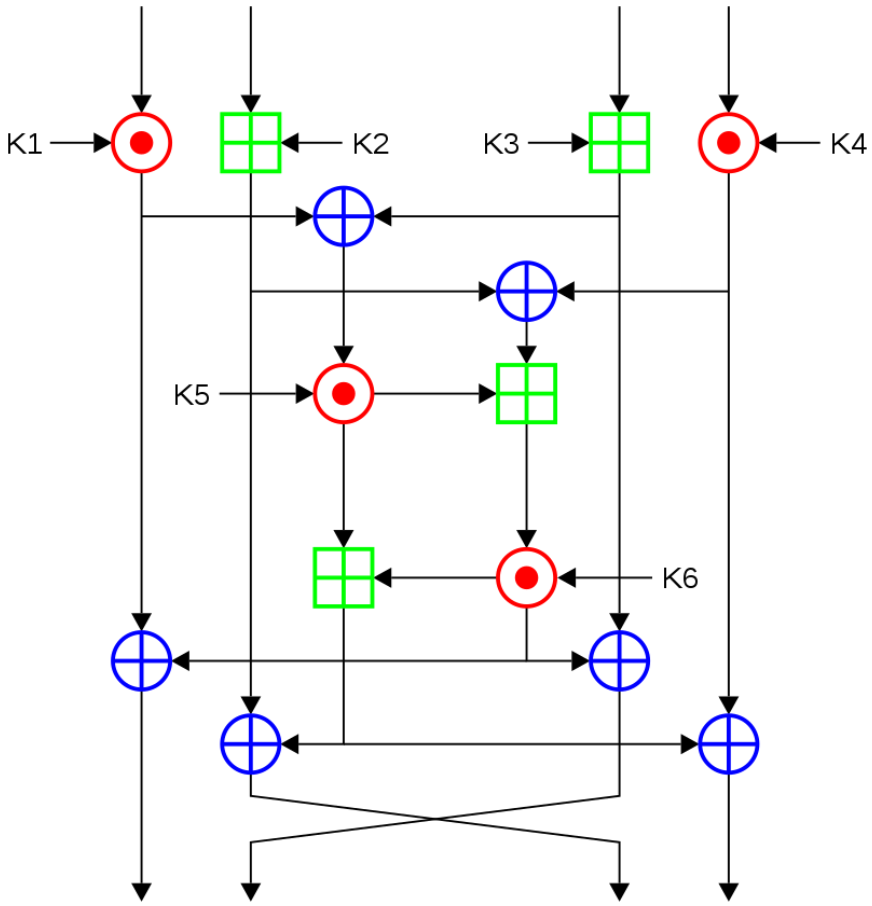
La sortie de la ronde est constituée des 4 sous-blocs produits par les étapes (11), (13), (12) et (14). Permutez les deux sous-blocs intérieurs (sauf lors de la dernière ronde) et cela donne X'1, X'2, X'3 et X'4 l'entrée de la ronde suivante. Par ailleurs, six nouvelles sous-clés K7...K12 sont dérivées pour utilisation dans la ronde suivante, et ainsi de suite.

Après la huitième ronde, il y a une transformation finale sur la dernière génération de sous-blocs :

1. Multipliez le dernier X'1 et la sous-clé K49;
2. Additionnez le dernier X'2 et la sous-clé K50;
3. Additionnez le dernier X'3 et la sous-clé K51;

4. Multipliez le dernier X'4 et la sous-clé K52.

Enfin les 4 sous-blocs sont réassemblés pour former le texte chiffré de 64 bits.



International Data Encryption Algorithm

Annexe :

- Code en Python pour IDEA en hexadécimal