M1MI2016 Codes et Cryptologie

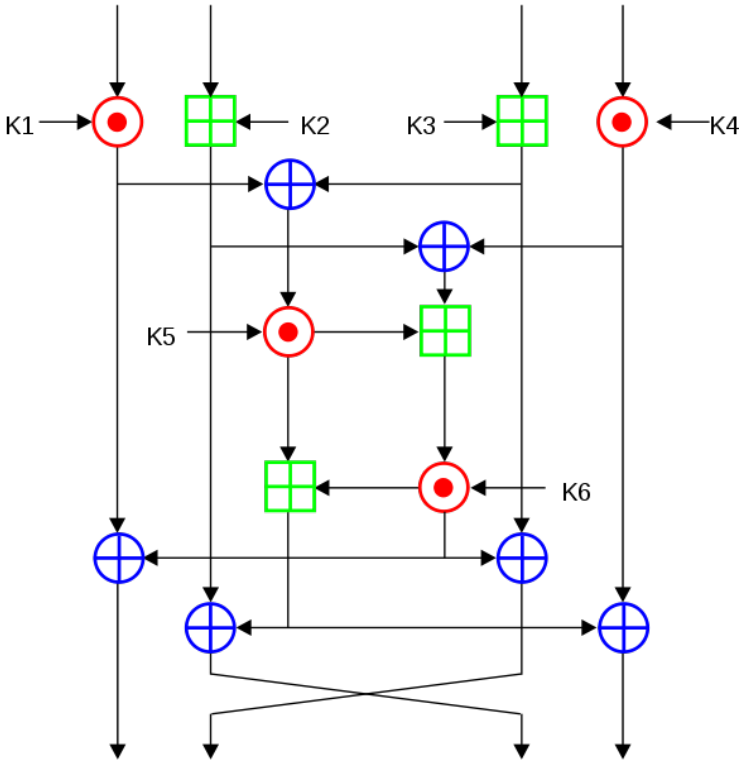
Feuille d'exercices n° 5.

Cryptographie symétrique

IDEA est un algorithme de chiffrement symétrique dû à Massey et Lay en 1991. C'est l'un des chiffrements proposés dans le standard de cryptographie OpenPGP.

IDEA est un algorithme itératif dont un tour est représenté par le schéma suivant. Cet algorithme opère sur des mots binaires de 64 bits qui sont groupés en 4 mots de 16 bits. La clé est de 128 bits, et pour chaque tour on extrait de la clé 6 sous-clés de 16 bits $K_1, \ldots, K_6$. Sur les mots de 16 bits, on utilise trois opérations différentes :

- $\oplus$: c'est l'addition bit à bit ou XOR.
- $\boxplus$: l'addition modulo 2^{16}, où un mot binaire vaut l'entier dont il est l'écriture binaire.
- $\odot$: la multiplication modulo $2^{16}+1$ où un mot binaire vaut l' entier dont il est l'écriture binaire, sauf 0^{16} qui représente 2^{16}. Noter qu'avec cette convention, aucun mot binaire ne correspond à 0, et que $2^{16}+1$ étant un nombre premier, tout entier compris entre 1 et 2^{16} est inversible modulo $2^{16}+1$.



1 Nous considérons une version "jouet" de IDEA, notée Mini-IDEA, qui opère sur des mots de 4 bits au lieu de 16, et exécute un seul tour, avec une clé K de 24 bits. Noter que $2^4 + 1 = 17$ est aussi un nombre premier.

1. Chiffrez $m = 1000010000111001$ avec $K = (K_1, K_2, K_3, K_4, K_5, K_6)$, et $K_1 = 0110$, $K_2 = 0111$, $K_3 = 1010$, $K_4 = 0000$, $K_5 = 0001$, $K_6 = 0010$.
2. Un schéma d'opérations analogue représente l'application inverse du tour, construisez-le.