MATH EN INFO

MODULE OPÉRATION

Phase 1

1 Présentation

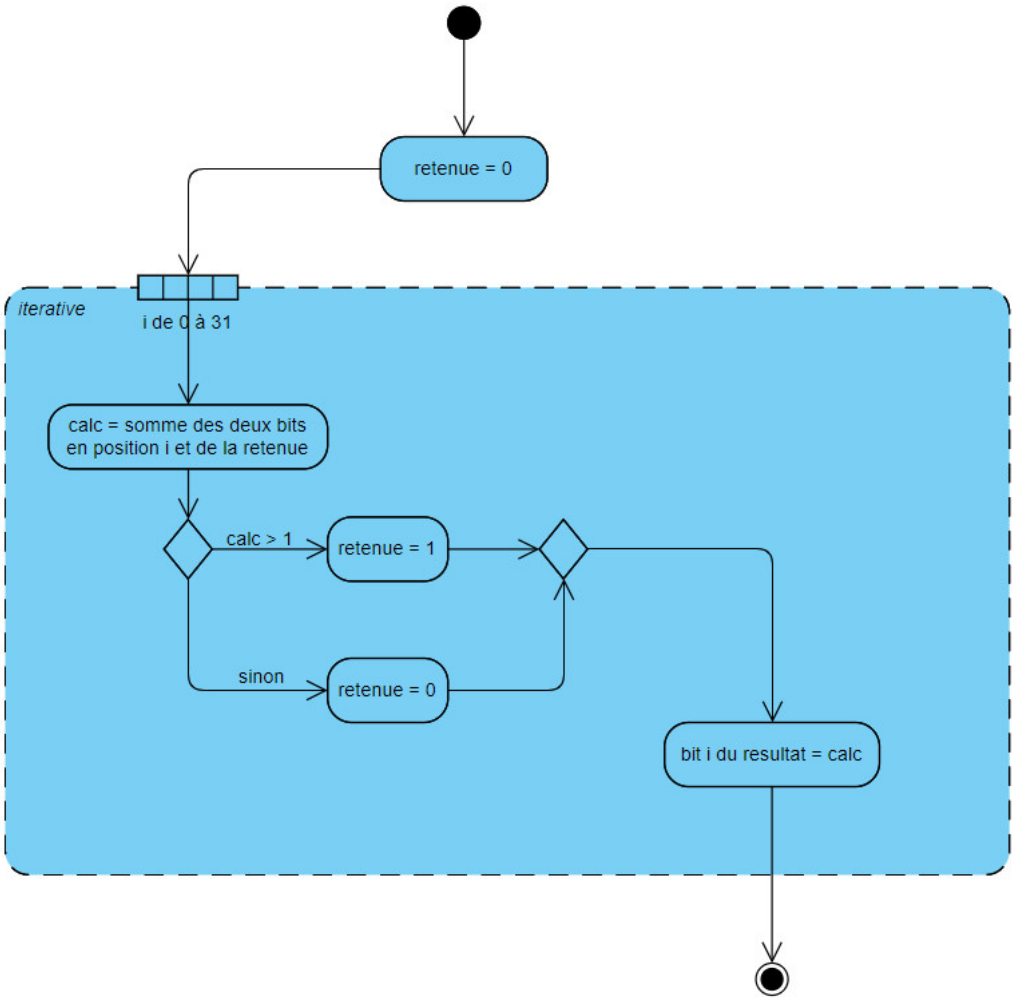
Ce fichier contient quelques indications sur les algorithmes pour les opérations Xor et d'addition sur les MotBinaire ainsi que des indications pour les phases 2 et 3 du module opération.

2 Indications sur les opérations binaires

2.1 Addition

Dans un schéma de Feistel, le symbole suivant :

représente une addition binaire modulo 2^{32} (sur 32 bits). On supposera toujours que les entrées et la sortie d'une addition sont des MotBinaires de longueur 32.



- MOS03 -
CRYPTAGE ET COMPRESSION

2.2 Xor

Dans un schéma de Feistel, le symbole suivant :

représente un xor entre deux mots binaires.

La classe BitSet dispose déjà d'une méthode xor. Attention, celle-ci modifie le BitSet courant, il est très fortement recommandé de toujours travailler sur une copie de ce BitSet. L'un des constructeurs de la classe MotBinaire fournie permet cela.

3 Indications pour les phases 2 et 3

3.1 Descriptif des phases

L'analyse du module d'opération du logiciel nous a permis de déterminer que celui-ci est composé de deux communications distinctes (phase 2 et phase 3).

Lors de la première communication le logiciel génèrera un nombre aléatoire de paires de mots binaires (envoyée chacune sous forme de deux messages successifs). Après l'envoi de chaque pair, le logiciel attendra le xor des deux nombres binaires envoyés (sous forme binaire). Ainsi si le logiciel envoie "10011" et "11001", il attendra en retour "01010".

Lors de la première communication le logiciel génèrera un nombre aléatoire de paires de mots binaires (envoyée chacune sous forme de deux messages successifs). Après l'envoi de chaque pair, le logiciel attendra la somme des deux nombres binaires envoyés (sous forme binaire).

Bien évidemment, chacune des communications devra commencer par l'envoi du mot de passe de celle-ci et se terminera par l'envoi par le logiciel de l'instruction "END".

3.2 Indications pour les mots de passes des communications

Le mot de passe de la phase 2 est un nombre décimal. On sait que ce nombre, après un encodage par un algorithme simple, est devenu : A,EF-KT.
Le mot de passe de la phase 3 a été encodé à l'aide du carré de Polybe pour donner : "5111334232221151".