# Introduction à la cryptographie

## Introduction

La cryptographie consiste généralement à prendre un texte (appelé texte clair) et à lui appliquer un algorithme de chiffrement avec des paramètres bien choisis. L'exécution de cet algorithme produit un texte qui semble ne plus avoir aucune signification (appelé texte chiffré). Le seul moyen de retrouver le texte clair est d'appliquer un algorithme de déchiffrement sur le texte chiffré.

Nous considérons pour le reste de ce projet que nos textes sont des suites de chiffres binaires (0 ou 1), que le nombre de chiffres est un multiple de 3 et qu'un bloc est une séquence de 3 chiffres consécutifs dans le texte. Ainsi, un texte pourrait être : 100001111000110. Dans ce texte, le premier bloc est 100, le second est 001, le troisième 111 etc.

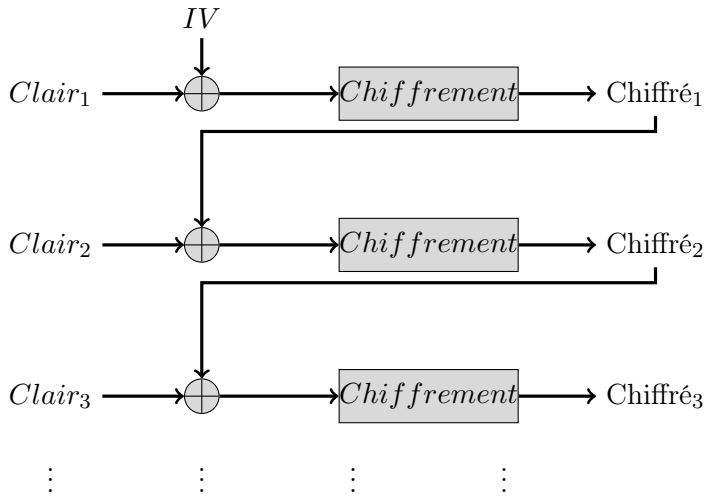
Nous allons implémenter dans le cadre de ce projet une technique de chiffrement utilisée de nos jours : le chiffrement par enchainement de blocs ou Cipher Bloc Chaining (CBC). Cette technique consiste à :

- combiner le bloc courant au bloc précédent
- chiffrer le nouveau bloc combiné au moyen d'une fonction de chiffrement prédéfinie
- combiner le bloc ainsi chiffré avec le bloc suivant et recommencer

Bien entendu il faut, pour que cette méthode fonctionne, fournir à l'algorithme un bloc supplémentaire à combiner avec le premier bloc du texte clair. Ce bloc est appelé vecteur d'initialisation ou initialization vector (IV).

Pour ce TP, nous combinerons les blocs en leur appliquant l'opération XOR (« ou exclusif »). Le XOR entre deux nombre binaires est le résultat du XOR de chacun de leurs bits : 100 XOR 010 = 110.

La fonction de chiffrement sera, quant à elle, simpliste : elle consistera juste à inverser chaque bit du bloc : chiffrement(100) = 011.




## 1 Travail

On vous demande d'écrire un programme C permettant de chiffrer n'importe quelle suite de chiffres binaires dont le nombre de chiffres est un multiple de trois. Pour représenter cette suite de chiffres binaires, utilisez des files (Queue).

Le programme contiendra une méthode main, où l'utilisateur est invité à entrer une chaine de nombres binaires et un vecteur d'initialisation, ainsi qu'une fonction de chiffrement. La fonction de chiffrement à implémenter correspond à la signature et aux spécifications suivantes :

```
/*
 * PRE: iv, suite de chiffres binaires initialisee (!=NULL) et de taille 3
 *      plaintext, suite de chiffres binaires initialisee (!=NULL) de taille multiple de 3
 * POST: renvoie une suite de chiffres binaires dont la taille vaut
 *      taille(plaintext).  Elle correspond au chiffrement de la
 *      suite de chiffres binaires plaintext avec pour vecteur d'initialisation
 *      iv.
 *      plaintext et iv n'ont pas ete modifies
 * */
Queue_t chiffrer(Queue_t iv, Queue_t plaintext);
```