

TP Cryptographie basée sur les codes

TP à faire PAR GROUPE de 2 (ne pas oublier de préciser le nom sur le rapport).  
A rendre pour vers fin mai sur le moodle (date à préciser plus tard, cela peut être à partir du 25 mai, ça dépend du jury).

**1) Algorithme ISD (Information Set Decoding)**

- a) expliquer rapidement le principe de l'algorithme vu en cours (version de base), rappeler sa complexité
- b) programmer une inversion de matrice binaire par la méthode du pivot de Gauss
- c) programmer l'algorithme ISD et le tester pour les paramètres suivants :
  - $n=400$   $k=200$  poids de l'erreur  $t=20$  (paramètres faciles pour un McEliece)
  - $n=1000$   $k=500$   $t=10$

Donnez vos temps de calcul.

**2) Système de chiffrement MDPC**

**Remarque :** vous pouvez vous référer au document cbc\_rev2.pdf sur le discord, paragraphe 1.4.3 (ce schéma correspond au schéma BIKE-2 soumis au NIST).

- a) rappeler le principe de l'algorithme BitFlip vu en TP (ne pas oublier le seuil  $T$  dans l'algo)
- b) décrire le système de chiffrement MDPC vu en TP (section 1.4.3 du document cbc\_rev2.pdf)
- c) programmer le système de chiffrement MDPC pour des paramètres (quasi) réels :

poids de  $x$  et  $y$  :  $w=39$ , longueur de  $x$  et  $y$  :  $n=4813$   
poids total de l'erreur  $e$  : 78, seuil  $T$  pour l'algo bitflip = 26

Donnez vos temps de calcul pour : chiffrement, déchiffrement, création des clés.

Que se passe-t-il au niveau du décodage lorsqu'on fait varier le seuil autour de 26 ou que l'on augmente  $w$  (de 10 par exemple) ?

**3) Travail à rendre** : un fichier pdf décrivant les divers algo demandés et les résultats obtenus avec les temps, ainsi que les fichiers source (langage de votre choix : C ou magma), considérer une approche polynomiale pour les calculs matriciels.