**TP1 Sécurité des réseaux et du web**

Gabrielle Bastien (BASG20549407)

Philippe Rheaume (RHEP12048808)

Remis à David Gagnon

le 19 octobre 2015

Université du Québec à Chicoutimi

Chez moi, sur Windows, on compile nos fichiers en ligne de commande dans le dossier bin lorsqu'on se trouve dans le dossier qui contient le dossier src, avec

javac -d bin src/\*.java

puis on part le client et le serveur avec

java -cp . TP1Securite.Server 10100 et java -cp . TP1Securite.Client 10100

Le client débute par demander l'algorithme à utiliser (choix entre 1 et 5) (le choix 5, CBC, n'est pas implémenté). Puis il offre le choix d'écrire le message directement dans la console ou de lire un fichier texte afin d'utiliser son contenu comme message. Les fichiers lus par le client doivent se situer dans le dossier data à côté du dossier src. Sont affichés les messages en clair, encrypté et décrypté.

CBC n'est pas implémenté par simple manque de temps. Considérant la complexité plus importante de Feistel, nous avons choisi de nous concentrer sur cette partie plutôt que sur le mode d'opération.

Finalement, l'algorithme MAC utilise HMAC avec la fonction de hachage simple implémentée dans le projet.