TP2 - Chiffrement de Vernam ou *One-Time-Pad*

ING3 CS – Cryptographie

Exercice 1. Retour sur le chiffrement de César

(1) Démontrer que, si le message ne contient qu'une seule lettre, alors le chiffre de César vu dans le TD1 est parfaitement sécurisé. □

Exercice 2. Retour sur le chiffrement de Vigenère

(2) Montrer que le chiffrement de Vigenère vu dans le TD1 est parfaitement sécurisé dès lors que la longueur du message n'excède pas celle de la clé. Est-ce toujours le cas si le message est strictement plus long que la clé? □

Exercice 3. *One-Time-Pad*

(3) Déchiffrez $\mathbf{c} = \texttt{01011101}$ en sachant que la clé $\mathbf{k} = \texttt{10011011}$. Est-ce que le résultat est unique? □

(4) Soit $\mathscr{M} = \{0,1,2,3\}^l$ (on utilise l'alphabet quaternaire au lieu de l'alphabet binaire). Décrire le schéma de chiffrement symétrique OTP dans ce cas. Démontrer qu'il est parfaitement sécurisé (ou pas). □

(5) Combien de temps serait-il possible d'utiliser le chiffre de Vernam pour :

a. l'envoi d'un texte (vitesse d'écriture : 40 bits/s) ;

b. une communication audio (avec un encodage audio de 64 kbits/s) ;

c. une communication vidéo en haute résolution (140 Mbits/s) ;

si Alice et Bob partagent une clé secrète **k** constituée d'une séquence binaire aléatoire pré-enregistrée sur :

1. un CD-R (700 Mo) ;
2. un DVD (4.7 Go) ;
3. un Blueray (50 Go). □

Exercice 4. *One-Time-Pad* (suite)

En utilisant le chiffrement *One-Time-Pad* sur des messages de longueur l avec la clé $\mathbf{k} = 0^l$, nous avons $\mathbf{c} = \text{Enc}(\mathbf{k}, \mathbf{m}) = \mathbf{m}$; et le message est envoyé en clair !

On suggère donc de modifier le générateur de clés pour que celui-ci ne puisse pas retourner la clé nulle.

(6) Décrire la distribution *KeyGen* selon laquelle sont tirées les clés. □

(7) Est-ce vraiment une amélioration du *One-Time-Pad* ? Notamment, le chiffrement est-il toujours parfaitement sécurisé ? Justifier votre réponse. □

Exercice 5. *One-Time-Pad* (bonus)

(8) L'inconvénient majeur du protocole OTP est la difficulté de générer une clé secrète **k** de taille suffisante et de la communiquer à Alice et à Bob. Alice, débutante en cryptographie, a l'idée suivante pour simplifier la procédure d'échange des clés : au lieu d'une clé aléatoire, elle souhaite utiliser un texte (que Bob possède également). En se mettant d'accord sur la page, ligne et colonne du début du texte à utiliser, elle va ajouter les caractères aux caractères d'un message **m**, modulo le nombre de caractères dans le texte (on retourne au début du livre lorsque l'on atteint la fin de celui-ci). Est-ce une bonne idée ? Justifier votre réponse. □