TP : CTF (Capture The Flag)

1- Introduction

Lors des séances de TP précédentes, vous avez étudié les notions de transposition de fréquence, de filtrage et de multiplexage. Dans ce TP vous devrez utiliser ces notions dans le cadre d'un CTF (Capture The Flag) dans le but de recevoir et de décoder des signaux. Pour cela, un multiplex de signaux sera transmis dans la salle pendant la durée du TP par ondes électromagnétiques. Le but est de créer divers diagrammes de flux dans GNURadio pour recevoir ces signaux à l'aide d'un module SDR Adalm Pluto.

2- Description du multiplex transmis

Les signaux transmis sont compris dans l'intervalle allant de 850 MHz à 850,5 MHz.

Les différents signaux transmis dans ce multiplex sont illustrés sur la figure ci-dessous.

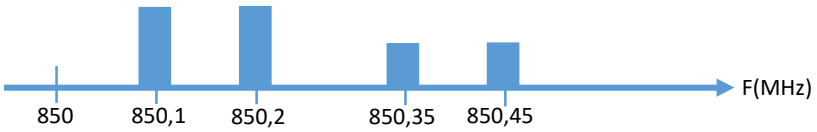

Figure 1 : contenu spectral du multiplex diffusé dans la salle.

3- Décodage de données numériques

Le signal diffusé sur la fréquence 850,1 MHz est une séquence de données binaires utilisant la modulation OOK et qui est répétée de manière continue (en boucle).

1- Réaliser un diagramme GNURadio pour recevoir le signal numérique transmis.
2- Relever son allure temporelle à l'aide d'un bloc « QT Gui time sink » sous GNURadio.
3- Analyser le signal reçu et mesurer la durée d'un symbole.
4- Donner la séquence binaire qui est diffusée de manière répétée.

4- Réception de signaux audio

Le signal diffusé sur la fréquence 850,2 MHz est un morceau musical de courte durée et répété en boucle.

5- Réaliser un diagramme GNURadio pour recevoir le signal numérique transmis et afficher son spectre.
6- Compléter votre diagramme pour permettre l'écoute de ce morceau musical sur les haut-parleurs de votre ordinateur.

5- Réception et recomposition d'un signal haché

L'une des techniques utilisées pour la transmission de messages secrets consiste à hacher l'information dans le temps et de la transmettre alternativement sur plusieurs fréquences. On peut également transmettre des leurres sur d'autres fréquences afin de rendre la recomposition du message d'origine plus difficile. Dans cette partie, nous expérimenterons une version simplifiée de transmission de signaux sur deux fréquences. Le message transmis est ici un message audio, audible sur les haut-parleurs de votre ordinateur. Le procédé qui a été utilisé est le suivant. Durant une seconde, le signal est transmis sur une première fréquence, puis, la suite du signal est transmise durant une seconde sur une deuxième fréquence. Ce cycle se répète indéfiniment. Ainsi, le signal complet est haché par tranches et transmis alternativement sur deux fréquences. Les deux fréquences utilisées sont : 850,35 MHz et 850,45 MHz.

7- Réaliser un diagramme de flux incluant un bloc « QT Gui Waterfall sink » afin de vérifier que le signal est transmis alternativement sur ces deux fréquences.
8- Réaliser un diagramme de flux permettant d'écouter le signal transmis sur la fréquence 850,35 MHz. Commentez.
9- Modifier le diagramme pour recevoir le signal transmis sur 850,45 MHz
10- Réaliser un nouveau diagramme permettant de recomposer le signal d'origine et de le diffuser à travers es haut-parleurs de votre ordinateur. Commentez.

6- Conclusion et discussion

11- Conclure sur le travail réalisé lors de ce TP.
12- Proposer des idées de transmission de signaux secrets pour améliorer le procédé utilisé dans la partie 5.