# MODULE 06
## SÉANCE SYSTÈME 06
## TP D'INFORMATIQUE
**Durée 2h30**

# Chiffrement de la communication

## BLOC DE COMPÉTENCES
U6 - VALORISATION DE LA DONNÉE ET CYBERSÉCURITÉ

## COMPÉTENCE(S)
C08 - CODER

## OBJECTIF PÉDAGOGIQUE
Dans cette partie, vous utiliserez une classe documentée pour créer un serveur UDP sur une Raspberry.

## CONNAISSANCES ISSUES DU RÉFÉRENTIEL
- Programmation Orientée Objet — Niveau 3

## CONNAISSANCES OPÉRATIONNALISÉES
- Utiliser une classe — Niveau 2
- Créer une classe — Niveau 2

Gaëtan GEORGES
Pascal HAGOT
David IERVESE

Lycée Louis Armand
173 Bd de Strasbourg
Nogent sur Marne

# Le chiffrement de données

## Présentation

Dans le cadre de la protection des données, nous souhaitons mettre en place un chiffrement des données qui circulent sur le réseau entre le « sniffer » (le client) et le serveur TCP RS sur la Raspberry.

## Chiffrement symétrique

> Expliquer ce qu'est un chiffrement symétrique.

> Donner les contraintes de ce type de chiffrement : qui doit connaître la clé, comment la partager en toute sécurité…

## Le chiffrement dans le système Cirpark

Dans ce projet, nous utiliserons un chiffrement avec un ou exclusif et une clé de chiffrement sur 2 octets : 0xA3 et 0xC5. Supposons qu'on souhaite envoyer la trame suivante : 0x08 0x12 0x05 0x1F (capteur 0x0812, fonction 05 et bcc).

> Donner la valeur des octets de la trame chiffrée :

1er octet =

2ème octet =

3ème octet =

4ème octet =

> Rappeler le principe du déchiffrement et procéder au déchiffrement de la trame.

## Le chiffrement en C++

> Ecrire en C++ la déclaration de la clé de chiffrement sous forme de tableau de 2 octets non signés. Le tableau s'appellera « cle ».

Supposons que nous devions chiffrer le tableau d'octets « requete » suivant :

```
unsigned char requete[4] = {0x08, 0x12, 0x05, 0x1F};
```

dans le tableau « requete_chiffree » déclaré comme suit :

```
unsigned char requete_chiffree[4];
```

> Ecrire les 4 instructions en C++ qui permettront de chiffrer les 4 octets avec la clé précédente (sans faire de boucle).

```
requete_chiffree[0] =
```

> On souhaite optimiser ce code avec une boucle for. Proposer une solution :

## Le déchiffrement

> Que dire du déchiffrement ? Comment d'écrit-il en C++ ?

## Mise en place du chiffrement dans les applications et test.

### Sur le serveur :

> Ajouter le déchiffrement des données reçues et le chiffrement des données envoyées.

### Sur le sniffer :

> Ajouter le chiffrement des données envoyées et le déchiffrement des données reçues.

> Vérifier que les échanges se passent correctement. Avec Wireshark, justifier que vos données sont bien chiffrées.