Rapport final TP de Cryptographie

Partie 1 : Pré-requis et calculs

1- Calculs initiaux pour un sous-réseau /28

A- Le masque de sous réseau en rotation décimal pointée pour un /28
On a : 28 bits bloqués à 1 ; donc N=32-28=4 bits
Ainsi en rotation décimal pointée se sera 255.255.255.240

B- Pour le réseau on 28 bits et les hôtes on a 4 hôtes.

C- Adresses IP totales dans un /28
N=2^n=2^4=16
Donc on a 16 adresses IP par sous-réseau.

D- Nombre maximale d'hôtes utilisables :

X=2^n-2=2^4-2=14

Donc on a 14 hôtes utilisables.

2- Détermination des plages d'adresses IP :

Sous-réseau	Adresse réseau	1 ère IP utilisable	Dernière IP utilisable	Adresse broadcast
1	192.178.12.0	192.178.12.1	192.178.12.14	192.178.12.15
2	192.178.12.16	192.178.12.17	192.178.12.30	192.178.12.31
3	192.178.12.32	192.178.12.33	192.178.12.46	192.178.12.47
4	192.178.12.48	192.178.12.49	192.178.12.62	192.178.12.63

Partie 2 : conception du réseau

Analyse des IP utilisées :

- 192.178.12.1, .3, .6 sont valides
- 192.178.12.11 utilisé deux fois
- 192.178.12.17 hors du réseau initial /28
- 192.178.12.15 adresse de broadcast

Erreurs détectées :

- Adresse réseau assignée :192.178.12.0
- Adresse de broadcast utilisée :192.178.12.15
- Une imprimante est hors réseau /28 (192.178.12.17)
  Elle n'est pas dans le réseau et son dernier octet en binaire est 00011111

Partie 3 : Cryptanalyse

Données fournies :

* chiffrement asymétrique avec AES-256-CBC

* clé =concaténation de 00011111(broadcast binaire) et 00 (préfixe MAC)

Clé finale : 0001111100