# TP Cryptographie - Analyse et Traitement de l’Énoncé

## Partie 1 : Pré-requis et Calculs

Adresse réseau principale : 192.178.12.0/24

Masque de sous-réseau utilisé : /28

### 1. Calculs Initiaux pour un Sous-Réseau /28 :

a. Masque en notation décimale pointée : 255.255.255.240

b. Bits alloués - Réseau : 28 bits, Hôtes : 4 bits

c. Nombre total d’adresses IP par sous-réseau : 16

d. Nombre maximal d’hôtes utilisables par sous-réseau : 14

### 2. Plages d'Adresses IP des 4 premiers sous-réseaux /28 :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sous-réseau | Adresse Réseau | Première IP | Dernière IP | Adresse de 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 et Implémentation du Réseau

Topologie Réseau :  
- À réaliser dans un simulateur réseau (Cisco Packet Tracer, GNS3, etc.)  
- Connecter les 10 équipements selon une logique LAN (avec switch/routeur si nécessaire)

Plan d'adressage IP :  
- Convertir les adresses binaires en décimal  
- Vérifier que chaque adresse est unique et dans la plage

Tests de Connectivité :  
- Utiliser des commandes ping pour tester la communication entre les machines

Détection et Sécurité :  
- Identifier la machine mal placée  
- Trouver le sous-réseau correct, l'adresse réseau et de broadcast  
- Décrypter un fichier texte crypté (cryptage asymétrique CBC 256 bits) avec la clé basée sur l’adresse broadcast et un préfixe MAC