Canal de diffusion anonyme et génération de secret

Requirements

Ce projet a été développé en python 3. Ce projet ne nécessite pas d'autre installation particulière.

Contexte

> Deux utilisateurs souhaitent protéger leurs communications en les chiffrant en utilisant le chiffrement symétrique, ces deux utilisateurs doivent alors convenir d'un secret commun. Afin d'empêcher qu'un espion puisse intercepter le secret, nous souhaitons implémenter un mécanisme de génération de secrets via l'implémentation d'un canal de diffusion anonyme.

Questions

```
1. Un canal de diffusion anonyme est une primitive qui peut être utilisée comme
brique de base pour réaliser de nombreuses tâches. Imaginer deux autres
applications possibles du canal de diffusion anonyme et décrivez les chacune en
quelques phrases.
```

Une blockchain anonymisée dans le cadre des crypto-monnaies. Chaque transaction entre deux utilisateurs est sauvegardé dans la blockchain, l'utilisation d'un canal de diffusion anonyme permettrait de protéger les informations permettant d'identifier l'acheteur et le vendeur.

La communication peer to peer, où chaque noeud du réseau est à la fois client et serveur. Ce système peut servir pour le partage de fichiers (torrent par exemple) et le calcul distribué (entre processus par exemple).

```
2. Argumenter sur le fait que suite au protocole décrit dans la deuxième partie,
Alice et Bob se retrouvent en possession d’un secret sur lequel l’adversaire n’a
aucune information. Pourquoi est ce le cas ?
```

La primitive d'échange de clés repose sur le fait de pouvoir connaitre l'émetteur des bits échangés. Grâce à ce protocole, seuls les deux interlocuteurs ont cette capacité. En effet, l'émetteur d'un message sait ce qu'il a envoyé et ce qu'il n'a pas envoyé.

Étant donné que c'est un canal de diffusion anonyme, un espion n'a aucun moyen de déterminer la source du message, et donc quel bit est associé à quel message.

```
3. Expliquer en quelques mots pourquoi il est important d’avoir des primitives
permettant à deux entités de générer un secret commun à travers un canal de
communication qui est potentiellement surveillé par un espion.
```

Deux utilisateurs veulent ici chiffrer leurs communications sur un canal anonyme en utilisant un chiffrement symétrique. Pour cela, les deux utilisateurs doivent avoir un secret commun. Si ce canal de communication est surveillé par un espion, celui-ci pourra récupérer le secret et donc déchiffrer les communications. Il est donc important de définir des primitives qui permettent de générer un secret qu'aucun espion ne pourra reconstituer en seulement écoutant sur le canal et qui sera connu seulement des deux utilisateurs.