

# Découverte de Tor : fiche « destinataire »

## 1 Votre rôle

Vous êtes le **destinataire** d'un message, composé par un **émetteur** qui souhaite le faire transiter par un circuit Tor. Il le transmettra à un **nœud d'entrée**, puis à un **nœud intermédiaire**, puis à un **nœud de sortie**, qui vous l'enverra directement. De même, vous serez amené à envoyer vos réponses à l'émetteur par le même chemin.

## 2 Organisation

Les participants sont répartis en cinq groupes :

- Les émetteurs ;
- Les nœuds d'entrée ;
- Les nœuds intermédiaires ;
- Les nœuds de sortie ;
- Les destinataires (dont vous faites partie).

Vous disposez du matériel suivant :

- Des feuilles de papier entrant dans les petites enveloppes ;
- Un crayon, une gomme ;
- La présente fiche.

## 3 Transmettre un message provenant d'un nœud de sortie

Un enveloppe représente le chiffrement utilisé pour protéger un message, et seules les personnes possédant la clé de chiffrement peuvent l'ouvrir. Dans cette version de l'exercice, vous n'aurez pas à manipuler d'enveloppe.

Un nœud de sortie peut être amené à vous transmettre un message.

1. Vérifiez que vous êtes bien identifié comme le destinataire de ce message, et prenez connaissance de son émetteur ;
2. Notez l'identifiant TCP indiqué sur l'enveloppe ;
3. Sur une nouvelle feuille, indiquez « émetteur : » suivi de votre identité, « destinataire : » suivi de l'identité de l'émetteur du message que vous venez de recevoir et « identifiant TCP : » suivi du numéro présent sur le message que vous venez de recevoir ;
4. Écrivez une réponse au message ;
5. Transmettez votre message au destinataire que vous avez identifié, à savoir le nœud de sortie qui vous l'a transmis.

## 4 Conclusions

- En tant que destinataire, pouvez-vous identifier l'émetteur d'un échange de messages ?
- En tant que destinataire, connaissez-vous le contenu du message ?
- Pouvez-vous identifier le nœud d'entrée du circuit Tor ?
- Pouvez-vous identifier le nœud intermédiaire du circuit Tor ?
- Pouvez-vous identifier le nœud de sortie du circuit Tor ?
- Qu'est-ce qui pourrait permettre de savoir que la personne qui vous a transmis le message n'est pas celle qui l'a rédigée ?
- Qu'est-ce qui pourrait vous permettre de savoir que le message est passé par un circuit Tor ?

- Qu'est-ce qui changera pour vous si l'émetteur décide d'utiliser, en plus de Tor, un chiffrement dit « de bout en bout » entre lui et vous (comme dans le cas d'une communication HTTPS) ?
- Quel est l'intérêt de l'identifiant TCP ? Pourrait-on s'en passer ? Pourquoi ?