Découverte de Tor : fiche « nœud d'entrée »

1 Votre rôle

Vous êtes un **nœud d'entrée**. Vous représentez un serveur participant au projet Tor, destiné à être en contact direct avec les utilisateurs (**émetteurs**) en tant que premier élément du circuit qu'ils auront choisi pour joindre le **destinataire**. Votre rôle est de faire transiter les messages de l'émetteur au destinataire via un **nœud intermédiaire** et un **nœud de sortie**. De même, vous serez amené à transmettre les réponses du destinataire à l'émetteur par le même chemin.

2 Organisation

Les participants sont répartis en cinq groupes :
- Les émetteurs ;
- Les nœuds d'entrée (dont vous faites partie) ;
- Les nœuds intermédiaires ;
- Les nœuds de sortie ;
- Les destinataires.

Vous disposez du matériel suivant :
- Des enveloppes de grande taille (optionnel) ;
- Un crayon, une gomme ;
- La présente fiche.

3 Transmettre un message de l'émetteur

Un enveloppe représente le chiffrement utilisé pour protéger un message, et seules les personnes possédant la clé de déchiffrement peuvent l'ouvrir. On suppose que l'émetteur possède une copie de votre clé.

Un émetteur peut choisir de vous transmettre un message sous la forme d'une enveloppe de grande taille.

1. Vérifiez que vous êtes bien identifié comme pouvant ouvrir cette enveloppe (il doit y avoir indiqué « chiffré avec la clé de : . . . » sur l'enveloppe) ;
2. Ouvrez l'enveloppe et sortez-en une enveloppe de taille moyenne (cela simule le déchiffrement de la couche extérieure du chiffrement en oignon) ;
3. Prenez connaissance de l'identité du nœud Tor capable de déchiffrer l'enveloppe de taille moyenne ;
4. Attribuez à cette association entre l'émetteur et le nœud désigné un **numéro de circuit** que vous conserverez dans le tableau suivant (à moins que cette association ne vous soit déjà connue) :

Émetteur	Nœud intermédiaire	Numéro de circuit attribué

5. Inscrivez sur l'enveloppe de taille moyenne « numéro de circuit : » suivi de ce numéro ;
6. Transmettez l'enveloppe de taille moyenne au nœud intermédiaire désigné ;
7. Effacez les inscriptions sur l'enveloppe de grande taille et conservez-la pour une utilisation ultérieure.

4 Transmettre un message provenant d'un autre nœud Tor

Un nœud intermédiaire peut vous transmettre une enveloppe de taille moyenne, qui correspond à une réponse en train d'être acheminée depuis un destinataire vers un émetteur. Comme vous pouvez participer à plusieurs circuits simultanément, le tableau que vous avez construit vous aidera à identifier l'émetteur concerné.

1. Vérifiez que le nœud qui vous transmet l'enveloppe et le numéro de circuit qui est inscrit dessus correspond bien à l'une des lignes de votre tableau ;
2. Identifiez l'émetteur grâce au tableau ;
3. Placez l'enveloppe de taille moyenne dans une enveloppe de grande taille en inscrivant dessus « chiffré avec la clé de : » suivi de votre nom ;
4. Transmettez l'enveloppe à l'émetteur.

5 Conclusions

– En tant que nœud d'entrée, pouvez-vous identifier l'émetteur d'un échange de messages ?
– En tant que nœud d'entrée, pouvez-vous identifier le récepteur d'un échange de messages ?
– Pouvez-vous identifier le nœud intermédiaire du circuit ?
– Pouvez-vous identifier le nœud de sortie du circuit ?
– En tant que nœud d'entrée, connaissez-vous le contenu d'un échange de messages ?
– 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 le destinataire (comme dans le cas d'une communication HTTPS) ?
– Quel est l'intérêt des numéros de circuits ? Pourrait-on s'en passer ? Pourquoi ?