MATH EN INFO

MODULE - COMMUNICATION

Phase 1

1 Présentation

Ce fichier contient les détails du protocole de communication avec le système de cryptage impérial ainsi que le descriptif des phases 2 et 3 du module de communication.

2 Protocole de communication

Le système de cryptage impérial utilise un protocole de communication standard TCP/IP. Voici les informations à connaitre pour établir une connexion avec le système :

- **Port utilisé :** 1977
- **Hôte :** le système étant émulé localement, l'hôte est donc : 127.0.0.1
- **Authentification :** Afin de pouvoir communiquer avec le système, l'utilisateur du système doit débuter sa communication par l'envoi d'un mot de passe variant d'une communication à l'autre. Une analyse plus approfondie du système devrait nous permettre de déterminer progressivement les différents mots de passe utilisés par l'empire.

3 Communication - Phase 2

Afin de tester votre protocole de communication, nous avons déployé une simulation de communication avec le logiciel disponible dans le module Communication - Phase 2. Pour cette simulation, votre outil devra juste établir une communication avec le logiciel de cryptage impérial et envoyer le mot de passe de la communication. Cette phase étant entièrement une simulation, le mot de passe a été fixé par nos soins à : ANEWHOPE. Nous vous recommandons de valider cette phase avant de vous attaquer aux suivantes.

4 Communication - Phase 3

Une fois ce premier test réalisé, nous pourrons communiquer directement avec le logiciel impérial. Nous commencerons par une communication simple afin de vérifier nos outils. Après avoir reçu le bon mot de passe, le logiciel impérial fournira une succession de nombres entiers qu'il vous suffira de renvoyer. La communication se terminera par "END" (qui n'attendra aucune réponse de la part de votre outil). Une étude du système nous a permis de déterminer que le mot de passe de cette communication a été encodé à l'aide d'un algorithme simple pour donner : "Mvy aol Ltwlyvy".