Exercice de Programmation en C : Brute Force d'une Encryption XOR Simple

Contexte

L'encryption XOR est une des méthodes de cryptographie les plus simples. Elle fonctionne en appliquant l'opérateur XOR (exclusif ou) à chaque octet du message avec un octet clé. Si la même clé est utilisée pour chiffrer et déchiffrer le message, cette méthode peut être efficace pour des usages basiques. Cependant, elle est vulnérable à une attaque par force brute si la clé est courte.

Objectif

Votre tâche est de développer un programme en C qui réalise une attaque par force brute sur un message chiffré avec une méthode XOR simple. Le but est de découvrir la clé utilisée pour le chiffrement.

Instructions

1. **Analyse du Message Chiffré** :
   - Le message chiffré vous sera fourni sous forme de chaîne de caractères hexadécimaux.
   - Vous savez que le message chiffré commence par `cst`
2. **Implémentation de la Force Brute** :
   - Écrivez un programme qui essaie toutes les combinaisons possibles de clés sur le message chiffré.
   - La taille de la clé sera spécifiée (par exemple, un octet).
   - Vous devez utiliser les threads pour paralléliser votre programme.
3. **Détection de la Clé Correcte** :
   - Une fois déchiffré, vérifiez si le texte résultant semble être un flag
   - Vous pouvez utiliser une heuristique simple, comme vérifier la présence de mots communs anglais ou le nombre de caractères imprimables.

4. **Affichage des Résultats** :
    - Si un texte clair plausible est trouvé, affichez ce texte ainsi que la clé utilisée.

Conseils

- Pensez à la façon dont l'opérateur XOR est inversible. Si `A XOR B = C`, alors `C XOR B = A`.
- Considérez des stratégies pour déterminer si un texte déchiffré est en anglais, comme chercher des mots communs ou des fréquences de lettres.