Projet avancé : Cryptographie symétrique

Équipe :

P1 : Amirmahdi GHASEMI (Responsable de projet)

P2 : Ivan URIBE

P3 : Mohamed-Yâ-Sîn MAATI

P4 : Axel CARCY

1. Introduction

Ce projet porte sur le développement d'une application de cryptographie symétrique avec plusieurs étapes clés : chiffrement et déchiffrement, échange de clé sécurisé, et crackage de code. Le projet est divisé en trois phases principales avec des livrables à chaque étape.

1) Phase 1 ***(dépôt : 4 novembre)*** : Chiffrement et déchiffrement symétrique (XOR et CBC).
2) Phase 2 ***(dépôt : 2 décembre)*** : Échange de clés Diffie-Hellman.
3) Phase 3 ***(livraison finale : 16 décembre)*** : Crackage de code et intégration finale.

2. Explications Techniques

● *Partie 1 : Chiffrement et Déchiffrement (XOR et CBC)*

Cette partie consiste à implémenter deux méthodes de chiffrement : le chiffrement caractère par caractère avec XOR et le chiffrement par blocs avec le mode CBC.

● *Partie 2 : Échange de clés Diffie-Hellman*

Mise en œuvre de l'algorithme Diffie-Hellman pour l'échange sécurisé de clés. Ce module sera implémenté en C pour la génération des groupes, et en Python pour simuler l'échange.

● *Partie 3 : Crackage de code*

Cette partie se concentre sur le développement d’attaques pour casser les messages chiffrés en utilisant des statistiques, l’analyse de fréquences, et un dictionnaire.

3. Répartition des Tâches

Membre	Tâches
P1	Responsable de projet, Développement chiffrement (XOR), Participation à l'échange Diffie-Hellman (tests et validation), Intégration finale.
P2	Développement chiffrement CBC, Support partie crackage de code, Responsable des tests Diffie-Hellman.
P3	Développement partie crackage de code (Crack C1 et C2), Aide au développement de la méthode CBC, Tests finaux.
P4	Développement partie crackage de code (Crack C3), Support chiffrement XOR, Responsable de la documentation et validation globale.

4. Échéancier

Partie du projet	Début	Fin	Durée
Chiffrement et déchiffrement (XOR)	01/10/2024	20/10/2024	20 jours
Chiffrement par blocs (CBC)	21/10/2024	02/11/2024	12 jours
Dépôt de la Partie 1	04/11/2024	04/11/2024	1 jour
Échange de clés Diffie-Hellman	03/11/2024	25/11/2024	23 jours
Dépôt de la Partie 2	02/12/2024	02/12/2024	1 jour
Crackage de code (C1, C2, C3)	26/11/2024	12/12/2024	17 jours
Tests et validation de l'application	13/12/2024	15/12/2024	3 jours
Livraison finale*	16/12/2024	16/12/2024	1 jour