CST em Sistemas Para Internet
Segurança de Dados
Prof. Dr. Leandro Almeida
leandro.almeida@ifpb.edu.br

INSTITUTO FEDERAL
Paraíba
Campus João Pessoa

Desafio de Criptografia Simétrica:
Implementação do DES e Mecanismo de Troca de Chaves Diffie-Hellman

1 Introdução

Este desafio tem como objetivo proporcionar uma experiência prática na implementação de técnicas de criptografia simétrica e troca de chaves, especificamente utilizando o algoritmo DES (Data Encryption Standard) e o mecanismo de troca de chaves Diffie-Hellman. A atividade visa que os alunos desenvolvam suas próprias implementações desses algoritmos em Python, sem o uso de bibliotecas auxiliares, e elaborem um relatório no formato de artigo científico sobre o processo e os resultados obtidos.

2 Objetivos

- Implementar o algoritmo DES: O DES é um dos algoritmos mais conhecidos para criptografia simétrica e opera com chaves de 56 bits. Sua implementação incluirá a criação de funções para a criptografia e descriptografia de blocos de 64 bits.
- Implementar o mecanismo de troca de chaves Diffie-Hellman: Este protocolo permite que duas partes, sem uma chave prévia compartilhada, estabeleçam uma chave secreta compartilhada sobre um canal de comunicação inseguro. A implementação incluirá a geração de parâmetros, a troca de informações e o cálculo da chave compartilhada.
- Escrever um relatório científico: Os alunos deverão documentar suas implementações, discutir desafios encontrados e analisar a eficácia e segurança das soluções implementadas.

3 Implementação do DES

O algoritmo DES utiliza uma chave de 56 bits e opera em blocos de 64 bits. A implementação deve cobrir:

- Preparação dos Dados: Implementar a geração das dezesseis sub-chaves K_{1-16} de 48 bits e realizar a permutação inicial.
- Rodadas de Criptografia: Implementar as 16 rodadas de substituição e permutação, incluindo a função $f()$ e ao final executar "32 bit swap (left,right)"
- Permutação Final: Implementar a permutação final que é a inversão da permutação inicial.

Os alunos devem garantir que suas funções sejam capazes de criptografar e descriptografar blocos de texto utilizando uma chave fornecida.

4 Implementação do Mecanismo de Troca de Chaves Diffie-Hellman

O protocolo Diffie-Hellman permite a criação de uma chave compartilhada através dos seguintes passos:

1. Escolha de Parâmetros: Definir um número primo n e uma base g que serão usados por ambas as partes.
2. Cada parte gera uma chave secreta (x e y) e calcula sua chave correspondente (a e b).
3. Troca de Chaves Públicas: As partes trocam suas chaves correspondentes (a e b) do canal inseguro.
4. Cálculo da Chave Secreta Compartilhada: Cada parte usa a chave correspondente da outra parte e sua própria chave secreta para calcular a chave secreta compartilhada (S_a e S_b).

5 Diretrizes para o relatório

O relatório deve seguir o formato de um artigo científico e incluir as seguintes seções:

- Introdução: Descrever o problema e os objetivos do desafio.
- Metodologia: Explicar o processo de implementação dos algoritmos DES e Diffie-Hellman. Incluir detalhes sobre a abordagem utilizada e o código implementado.
- Resultados: Apresentar os resultados obtidos das implementações. Incluir exemplos de criptografia e descriptografia, bem como a troca de chaves e a criação da chave compartilhada.
- Discussão: Analisar os desafios encontrados durante a implementação, a eficácia dos algoritmos e possíveis vulnerabilidades.
- Conclusão: Resumir as descobertas e possíveis *insights*, além de sugerir melhorias ou pesquisas futuras.

6 Requisitos de implementação

- Linguagem: Python.
- Bibliotecas: Não é permitido o uso de bibliotecas auxiliares para criptografia. Todas as operações devem ser implementadas do zero.
- Artefatos: A implementação deve ser desenvolvida em arquivos separados, ou seja, um arquivo para executar as funções de emissor e criptografia ("sender.py") e outro para executar as funções de receptor e descriptografia ("receive.py").
- Documentação: O código deve ser bem documentado, com comentários explicativos sobre cada etapa do algoritmo.

7 Prazos e formato de entrega

O código-fonte e o relatório em formato PDF devem ser entregues até às 23:59 do dia 24-09-2024. Os alunos devem realizar o upload de um arquivo .ZIP contendo todos os artefatos utilizados neste desafio. Um formulário estará disponível na sala de aula do Google Classroom para receber os artefatos desenvolvidos pelos alunos.

8 Ética

Quaisquer tentativas de fraude ou cópia dos desafios, serão avaliadas e julgadas pelo professor da disciplina.

Happy Hacking!