Trabalho segurança da informação

Algoritmos de Criptografia: Implementação e Análise

Alunos: Lucas Vinicius Silveira (202402390562)  
 Luis Gustavo Lobato De Melo(202404346285)   
 Leandro Nascimento de Paula (202304190615)

Pesquisa bibliográfica

**Conceitos Básicos:**

**Criptografia:** É o processo de transformação de dados em um formato ilegível chamado texto cifrado, para garantir confidencialidade e segurança durante a transmissão ou armazenamento de dados.

**Texto Claro:** É o texto original que precisa ser protegido.

**Texto Cifrado:** É o resultado do processo de criptografia, o texto transformado que não é facilmente legível sem a chave de decodificação.

**Chave Criptográfica:** É um valor usado pelos algoritmos de criptografia para criptografar e/ou descriptografar os dados. A segurança da criptografia geralmente depende da segurança desta chave.

Tipos de Criptografia:

**Tipos de Criptografia:**

**Criptografia Simétrica:** Utiliza a mesma chave para criptografar e descriptografar os dados. Exemplos incluem AES (Advanced Encryption Standard), DES (Data Encryption Standard), e 3DES.

**Criptografia Assimétrica (ou Criptografia de Chave Pública):** Usa um par de chaves, uma pública e uma privada. A chave pública é compartilhada para criptografar os dados, enquanto a chave privada é mantida em segredo e usada para descriptografar. Exemplos incluem RSA, ElGamal e ECC (Elliptic Curve Cryptography).

**Hashing:** Não é estritamente criptografia, mas é usado para garantir a integridade dos dados. Transforma dados em um valor hash fixo e único. Exemplos incluem SHA (Secure Hash Algorithm) e MD5.

**Aplicações:**

A criptografia no ambiente digital pode ser aplicada de diversas formas, sendo a mais popularizada delas nas trocas de mensagens entre usuários em aplicativos de conversação. Mas além disso, ela também é aplicada no armazenamento de arquivos, transações eletrônicas, assinaturas de contratos, entre outros pontos.  
  
Ou seja, onde há troca de dados entre usuários ou necessidade de proteger um item de acesso por cibercriminosos, ela pode ser adotada.

**Exemplos:**

-Segurança de Dados em Comunicações  
-Segurança de Dados em Armazenamento  
-Autenticação e Assinaturas Digitais  
-Segurança de Sistemas de Pagamento  
-Segurança de Sistemas de Arquivos

**Exemplos de algoritmos de criptografia:**

**Cifra de César:** A cifra de César é um dos métodos mais simples de criptografia. Funciona deslocando cada letra do texto original por um número fixo de posições no alfabeto. Por exemplo, com um deslocamento de 3, "A" seria substituído por "D", "B" por "E" e assim por diante. Para decifrar, basta aplicar o deslocamento inverso.

**Cifra de Substituição:** Este método substitui cada letra do texto original por outra letra do alfabeto, de acordo com um padrão predefinido. Por exemplo, a letra "A" pode ser substituída por "Q", "B" por "Z" e assim por diante. A chave neste caso é a tabela de correspondência entre as letras originais e suas substitutas.

**Cifra de Vigenère:** A cifra de Vigenère é uma extensão da cifra de César, mas em vez de usar um único deslocamento para todas as letras, utiliza uma palavra-chave. Cada letra da mensagem é deslocada de acordo com a letra correspondente na palavra-chave. Se a palavra-chave for mais curta do que a mensagem, ela é repetida. Isso torna a cifra de Vigenère mais resistente à análise de frequência do que a cifra de César simples.

**RSA (Rivest-Shamir-Adleman):** RSA é um algoritmo de criptografia assimétrica amplamente utilizado para comunicação segura na Internet. Ele envolve o uso de duas chaves: uma pública e uma privada. A chave pública é usada para criptografar a mensagem, enquanto a chave privada é usada para decifrá-la. A segurança do RSA baseia-se na dificuldade de fatorar números primos muito grandes.

**AES (Advanced Encryption Standard):** AES é um algoritmo de criptografia simétrica que substituiu o antigo padrão DES (Data Encryption Standard). Ele opera em blocos de dados de 128 bits e suporta chaves de 128, 192 e 256 bits. AES é altamente eficiente e amplamente utilizado em aplicativos que exigem alto desempenho de criptografia, como segurança de rede e proteção de dados.