Aplicação Criptografia

Trabalho prático 1

Nome: Vasco Rodrigues Ribeiro

Número: al7038

**Introdução:**

Neste relatório, analisamos a aplicação desenvolvida para criptografar e descriptografar mensagens e arquivos, além de assinar digitalmente mensagens para garantir sua autenticidade. A aplicação utiliza diferentes técnicas e algoritmos de criptografia, incluindo criptografia simétrica, criptografia assimétrica e funções de hash. As principais características, vantagens e desvantagens de cada algoritmo são discutidas a seguir.

**Criptografia Simétrica:**

A aplicação utiliza o algoritmo Advanced Encryption Standard (AES) para criptografia simétrica. O AES é um algoritmo de criptografia de bloco que usa a mesma chave para criptografar e descriptografar os dados.

**Vantagens:**

Velocidade: O AES é mais rápido do que os algoritmos de criptografia assimétrica.

Eficiência: O AES é eficiente em termos de recursos, tornando-o adequado para dispositivos com capacidade de processamento limitada.

**Desvantagens:**

Distribuição de chaves: A maior desvantagem do AES é a necessidade de compartilhar a chave secreta entre as partes envolvidas na comunicação segura. A distribuição segura da chave é um desafio.

**Criptografia Assimétrica:**

A aplicação utiliza o algoritmo RSA para criptografia assimétrica. O RSA é um algoritmo de criptografia de chave pública que usa um par de chaves (uma chave pública e uma chave privada) para criptografar e descriptografar os dados.

**Vantagens:**

Segurança na distribuição de chaves: A chave pública pode ser compartilhada abertamente sem comprometer a segurança dos dados criptografados.

Autenticação: O RSA também pode ser usado para autenticação, pois apenas o detentor da chave privada correspondente pode descriptografar os dados criptografados com a chave pública.

**Desvantagens:**

Velocidade: O RSA é mais lento do que os algoritmos de criptografia simétrica.

Tamanho da chave: O RSA requer chaves de maior tamanho para fornecer o mesmo nível de segurança que os algoritmos simétricos.

**Funções de Hash:**

A aplicação permite ao usuário gerar hashes de mensagens usando o algoritmo de hash seguro (SHA) em sua versão SHA-256. As funções de hash são usadas para criar uma representação de tamanho fixo de um conjunto de dados, que é praticamente única para cada conjunto de dados.

**Vantagens:**

Integridade dos dados: As funções de hash podem ser usadas para verificar a integridade dos dados, pois qualquer alteração nos dados resulta em uma alteração no hash.

Eficiência: As funções de hash são geralmente rápidas e eficientes em termos de recursos.

**Desvantagens:**

Unidirecionalidade: As funções de hash são projetadas para serem unidirecionais, o que significa que não é possível recuperar os dados originais a partir do hash.

Assinatura Digital:

A aplicação utiliza o algoritmo RSA em conjunto com o algoritmo de hash SHA-256 para assinar digitalmente mensagens. Isso garante a autenticidade, integridade e não repúdio das mensagens trocadas entre as partes.

**Vantagens:**

Autenticidade: A assinatura digital confirma a identidade do remetente, garantindo que a mensagem seja originada de uma fonte autêntica.

Integridade: A assinatura digital garante que a mensagem não foi alterada durante o trânsito, garantindo a integridade dos dados.

Não repúdio: A assinatura digital impede que o remetente negue ter enviado a mensagem, pois apenas o detentor da chave privada correspondente pode criar uma assinatura válida.

**Desvantagens:**

Complexidade: A assinatura digital envolve o uso de algoritmos de criptografia assimétrica e funções de hash, aumentando a complexidade da implementação em comparação com a criptografia simétrica.

Desempenho: A assinatura digital pode ser mais lenta do que a criptografia simétrica devido à complexidade dos algoritmos de criptografia assimétrica e funções de hash envolvidos.

**Documentação de funcionalidades da aplicação:**























**Conclusão:**

A aplicação desenvolvida utiliza diferentes técnicas e algoritmos de criptografia para fornecer funcionalidades de criptografia simétrica e assimétrica, hashing e assinatura digital. Essas técnicas e algoritmos oferecem vantagens em termos de segurança, autenticidade e integridade dos dados. No entanto, também apresentam desafios em termos de distribuição de chaves, desempenho e complexidade. O uso de algoritmos e técnicas apropriadas para cada cenário específico é crucial para garantir a segurança e a eficiência das comunicações seguras.