INSTITUTO FEDERAL DO PIAUÍ - CAMPUS PAULISTANA
DISCIPLINA: NOÇÕES DE SEGURANÇA DA INFORMAÇÃO
PROFESSORA: MAÍLA DE LIMA CLARO
ALUNOS: DANILO, ERIK, Mª EDUARDA BONFIM, PIETRO

Trabalho Prático: Criptografia Simétrica vs. Assimétrica

CRIPTOGRAFIA SIMÉTRICA

A criptografia simétrica utiliza uma única chave secreta para proteger as informações. Essa mesma chave é usada tanto para criptografar quanto para descriptografar os dados, o que exige cuidado no seu compartilhamento e armazenamento.

Principais algoritmos utilizados:

- **AES (Advanced Encryption Standard)**: é o padrão mais utilizado atualmente, por ser rápido e seguro.
- **DES e 3DES (Data Encryption Standard)**: são algoritmos antigos. O DES já não é considerado seguro e o 3DES vem sendo descontinuado.

CRIPTOGRAFIA ASSIMÉTRICA

A criptografia assimétrica utiliza duas chaves diferentes, mas relacionadas entre si. A chave pública pode ser divulgada, enquanto a chave privada deve permanecer em sigilo, sendo essencial para a segurança do processo.

Principais algoritmos utilizados:

- **RSA**: amplamente usado em certificados digitais, sistemas de autenticação e segurança na web.
- **ECC (Criptografia de Curvas Elípticas)**: alternativa mais moderna, que oferece alto nível de segurança com chaves menores.

DIFERENÇAS ENTRE CRIPTOGRAFIA SIMÉTRICA E ASSIMÉTRICA

Em relação às chaves:

- Na criptografia simétrica, utiliza-se apenas uma chave secreta.
- Na criptografia assimétrica, utiliza-se um par de chaves, uma pública e outra privada.

Em relação ao desempenho:

- A criptografia simétrica é mais rápida e adequada para grandes volumes de dados.
- A criptografia assimétrica é mais lenta, pois depende de cálculos matemáticos mais complexos.

Em relação ao uso prático:

- A criptografia simétrica é usada diretamente na proteção dos dados.
- A criptografia assimétrica é usada principalmente para troca segura de chaves e autenticação.

APLICAÇÕES NO DIA A DIA

SSL/TLS (HTTPS): utiliza criptografia assimétrica no início da comunicação para garantir a troca segura de chaves e, em seguida, criptografia simétrica para a transmissão dos dados.

Arquivos criptografados: ferramentas como BitLocker e VeraCrypt utilizam criptografia simétrica, principalmente o algoritmo AES.

E-mails seguros: sistemas como PGP utilizam criptografia assimétrica para proteger a troca de chaves, enquanto o conteúdo das mensagens é criptografado de forma simétrica.

Aplicativos de mensagens: aplicativos como WhatsApp e Signal combinam criptografia simétrica e assimétrica para garantir a confidencialidade das comunicações.

Tempo de Execução (AES)

Tamanho da mensagem	Criptografia (ms)	Descriptografia (ms)
100 caracteres	0,05	0,05
1.000 caracteres	0,08	0,08
10.000 caracteres	0,30	0,30

Tempo de Execução (RSA)

Tamanho da mensagem	Criptografia (ms)	Descriptografia (ms)
100 caracteres	1,5	3,0
1.000 caracteres	Não recomendado	Não recomendado
10.000 caracteres	Inviável	Inviável

Tamanho das Chaves

Algoritmo	Tipo	Tamanho da chave
AES	Simétrica	256 bits
RSA	Assimétrica	2048 bits

Tamanho do Texto Cifrado

Algoritmo	Mensagem original	Tamanho do texto cifrado
AES	100 caracteres	~112 bytes
AES	1.000 caracteres	~1.016 bytes
AES	10.000 caracteres	~10.016 bytes
RSA	Até ~190 bytes	256 bytes (fixo)

Comparação Geral e Indicação de Uso

Critério	AES	RSA
Velocidade	Muito alta	Baixa
Uso de memória	Baixo	Alto
Dados grandes	Ideal	Não indicado
Troca de chaves	Não indicado	Ideal
Segurança prática	Muito alta	Muito alta
Uso real	Criptografia de dados	Criptografia de chaves

Conclusão

Aspecto	Resultado
Mais rápido	AES
Mais eficiente para grandes mensagens	AES
Ideal para troca de chaves	RSA

Reflexão final:

• Qual dos dois tipos de criptografia é mais fácil de entender?

A **criptografia simétrica** é a mais fácil de entender porque usa só uma chave. A mesma chave serve para criptografar e para descriptografar a mensagem. A ideia é simples. Quem tem a chave consegue ler o conteúdo.

• O que foi mais difícil no trabalho

O mais difícil no trabalho foi a **criptografia assimétrica**. Entender o uso de duas chaves, uma pública e outra privada. Também foi difícil entender por que o RSA não serve para mensagens grandes e é usado apenas para proteger chaves.

• Dificuldades técnicas encontradas e como resolveram.

As dificuldades técnicas foram principalmente na hora de programar. No AES, surgiram erros por causa do tamanho da mensagem, que precisou de padding para funcionar corretamente. No RSA, o problema foi o limite de tamanho da mensagem e a configuração correta do padding. Esses problemas foram resolvidos com testes no código e ajustes até a criptografia funcionar corretamente.