1º MINI-TESTE DE SEGURANÇA INFORMATICA E DAS TELECOMUNICAÇÕES

Turma: LEIT I42 [Pontuação máxima: 50] Data: 02 Abril 2024

1º Semestre **Guião de correção** Duração: 40 min

Docente: Eng. Emírcio Zeca Vieira

NOME: Nº

1. Um certificado digital é um documento eletrônico cuja utilização possibilita que transações digitais sejam realizadas de forma segura. Alguns aspectos e requisitos da segurança da informação que podem ser implementados com o uso de certificados digitais são: 4

Em relação aos itens apontados, pode-se afirmar que:

A) Integridade e Disponibilidade;
B) Autenticidade e Rastreabilidade;
C) Autenticidade e Confidencialidade;
D) Confidencialidade e Disponibilidade.

2. A garantia de que o executor de determinada transação eletrônica não poderá posteriormente negar sua autoria diz respeito a qual atributo da Segurança da Informação? 8

Selecione a afirmação correcta e justifique:

A) Integridade;
B) Autenticidade;
C) Não-repúdio;
D) Disponibilidade;
E) Integridade.

Não-repúdio (Irretratabilidade), é a garantia de que o indivíduo ou entidade não negue a autoria de uma acção. por si feita.

3. O primeiro algoritmo de criptografia assimétrica disponibilizado ao público e utilizado amplamente para a transmissão segura de dados foi o … 8

Selecione a afirmação correcta e justifique:

A) DES;
B) 3DES;
C) AES;
D) RC4;
E) RSA.

Algoritmo criptográfico assimétrico criado no MIT, em 1977, por Ron Rivest, Adi Shamir e Len Adleman. É uma das mais poderosas formas de criptografia assimétrica conhecidas até os dias actuais.

4. A criptografia simétrica utiliza a mesma chave secreta para criptografar e decriptar uma mensagem sigilosa. Os algoritmos simétricos podem realizar uma cifragem de bloco ou de fluxo. Um exemplo de algoritmo simétrico que realiza a cifragem de fluxo é o … 8

   A) AES;

   B) DES;

   C) RC2;

   D) RC4.

RC4 é um algoritmo de criptografia de fluxo. Ele é um algoritmo de chave simétrica, o que significa que a mesma chave é usada tanto para criptografar quanto para descriptografar os dados.

5. O algoritmo de Diffie-Hellman é um método criptográfico utilizado para a troca de chaves secreta em um canal de comunicação não seguro, como a internet. Ele permite que duas partes concordem sobre uma chave de criptografia comum, mesmo que elas nunca tenham se comunicado antes, garantindo que essa chave permaneça secreta para um observador passivo. 10

   De forma resumida, indique 5 passos necessários para o funcionamento do algoritmo de Diffie-Hellman.

1. Escolha de Parâmetros.
2. Escolha de Chaves Privadas.
3. Cálculo das Chaves Públicas.
4. Troca das Chaves Públicas.
5. Cálculo da Chave Secreta Compartilhada.

6. O DSA e RSA são ambos algoritmos de criptografia assimétrica utilizados para fins diferentes, no entanto, frequentemente comparados devido à sua popularidade e aplicabilidade em segurança de dados. Faça uma comparação entre os dois algoritmos em termos de Desempenho e Padrões e uso. 12

Desempenho:

- O RSA é geralmente mais lento em comparação com DSA para a mesma operação, especialmente quando se trata de geração de chaves e verificação de assinaturas.
- O DSA é considerado mais rápido em assinaturas digitais do que o RSA.

Padrões e Uso:

- O RSA é mais amplamente utilizado em uma variedade de contextos, incluindo criptografia de dados, assinaturas digitais, SSL/TLS e muito mais.
- O DSA é frequentemente usado em conjunto com algoritmos de troca de chaves como o Diffie-Hellman para autenticar as partes envolvidas.

Bom trabalho!

"A força que você busca mora dentro de você."