1º MINI-TESTE DE SEGURANÇA INFORMATICA E DAS TELECOMUNICAÇÕES

Turma: LEIT I41 [Pontuação máxima: 50] Data: 02 Abril 2024

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

Docente: Eng. Emírcio Zeca Vieira

NOME: Nº

1. Em relação aos fundamentos sobre Assinatura Digital e Certificação Digital análise os itens a seguir: 4

I - Um certificado digital pode ser visto como uma carteira de identidade para uso na internet.
II - Tecnicamente, um certificado digital é um conjunto de dados (um arquivo), assinado digitalmente pela autoridade certificadora.
III - Um certificado digital contém a chave pública referente a chave privada da entidade especificada no certificado.

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

A) Os itens I, II e III são falsos
B) Somente o item II é verdadeiro.
C) Somente os itens I e II são verdadeiros.
D) Os itens II e III são falsos.
E) Os itens I, II e III são verdadeiros.

2. Mahumane recebeu um documento assinado digitalmente por seu chefe, Erwin, e, ao abri-lo, notou que Erwin havia assinado uma versão anterior do documento. Ao devolver o documento ao Erwin, este alegou não ter enviado a versão errada do documento. Contudo, o facto de haver nele a assinatura digital de Erwin permite que Mahumane tenha certeza de que foi o chefe que o enviou, assegurando o princípio da … 8

Selecione a afirmação correcta e justifique:

A) Confidencialidade;
B) Disponibilidade;
C) Integridade;
D) Irretratabilidade;

Irretratabilidade (Não-repúdio): 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. Os dados sensíveis devem ser protegidos por meio de práticas de segurança projetadas para impedir a divulgação não autorizada e a violação dos dados. Dentre as práticas usadas para proteção de dados em repouso, pode-se destacar a criptografia simétrica. 8
Um exemplo de um algoritmo de criptografia simétrica é o …

Selecione a afirmação correcta e justifique:

A) AES;

B) RSA;

C) Diffie-Hellman;

D) DES;

E) RC2.

AES (*Advanced Encryption Standard*), é um algoritmo de criptografia simétrica amplamente utilizado para proteger dados sensíveis. Ele é considerado um dos algoritmos de criptografia mais seguros e eficientes disponíveis actualmente. Utilizado para proteger a privacidade e a segurança dos dados.

5. A assinatura digital é um método de autenticação digital que valida a integridade e a autenticidade de um documento eletrônico ou uma mensagem. 10
De forma resumida, indique 5 passos que compõem o processo da assinatura digital:

1. Criação do Documento.
2. Geração do Hash.
3. Criptografia de Chave Pública e Privada.
4. Assinatura Digital.
5. Anexação da Assinatura ao Documento.
6. Envio do Documento.
7. Verificação da Assinatura.
8. Validação da Integridade e Autenticidade.

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 Segurança e o Tamanho da Chave. 12

Segurança:

- O RSA e DSA são considerados seguros quando usados correctamente, porém suas seguranças dependem da implementação e do tamanho das chaves.
- O RSA tem sido mais amplamente estudado e utilizado ao longo do tempo, enquanto DSA foi especificamente desenvolvido para atender aos requisitos do governo dos EUA.

Tamanho da Chave:

- O tamanho mínimo recomendado para chaves RSA é geralmente maior do que o tamanho mínimo recomendado para chaves DSA para alcançar um nível semelhante de segurança.
- Em geral, chaves DSA tendem a ser menores do que chaves RSA para a mesma segurança, o que pode ser uma vantagem em termos de eficiência computacional.

Bom trabalho! *"Tenha coragem para se tornar aquilo que sonha."*