1º MINI-TESTE DE SEGURANÇA INFORMATICA E DAS TELECOMUNICAÇÕES

Turma: LECC I41 [Pontuação máxima: 50] Data: 03 Abril 2024

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

Docente: Eng. Emírcio Zeca Vieira

NOME: Nº

1. Sumaya assinou digitalmente um ofício e enviou ao Benildo. Ao verificar a assinatura digital, Benildo confirmou a veracidade da assinatura de Sumaya. 4

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

A) A mensagem é autenticada tanto em termos de origem quanto em termos de confidencialidade de dados;
B) A mensagem que está sendo enviada está a salvo de alteração, porém não de escuta por terceiros;
C) Mesmo no caso de cifração completa da mensagem, não há qualquer proteção de integridade da mensagem;
D) Sumaya usou uma função de hash segura para gerar um valor de hash para a mensagem, e então cifrou o código de hash com sua chave pública;
E) Quando Benildo recebe a mensagem mais a assinatura, ele calcula um valor do hash da mensagem e decifra a assinatura usando a chave privada de Sumaya.

2. Um dos benefícios fornecidos por assinaturas digitais de documentos eletrônicos é a possibilidade de verificar que o conteúdo assinado não foi alterado em trânsito. Ou seja, a possibilidade de verificar que um terceiro que teve acesso ao conteúdo antes que o mesmo chegasse em seu destinatário não alterou os dados. Esse conceito é chamado de … 8

Selecione a afirmação correcta e justifique:

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

A integridade se refere à garantia de que os dados não foram alterados ou corrompidos de forma não autorizada durante a transmissão, armazenamento ou processamento. É essencial para garantir a confiabilidade e a segurança dos dados.

3. Uma empresa de comunicações trabalha com mensagens com criptografia simétrica. Um exemplo de algoritmo para esse tipo de criptografia é … 8

Selecione a afirmação correcta e justifique:

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

O Triple DES (3DES), também conhecido como TDEA (*Triple Data Encryption Algorithm*), é um algoritmo de criptografia simétrica que aplica a cifra DES (*Data Encryption Standard*) três vezes em sequência para melhorar a segurança. O DES é um algoritmo de chave simétrica que foi amplamente utilizado, no entanto, com o tempo, tornou-se vulnerável a ataques de força bruta devido ao tamanho curto da chave.

4. O TLS é um protocolo desenvolvido para proteger comunicações. Considere que o processo que dá início a uma sessão, conhecido como *Handshake* TLS, utiliza chave pública e chave privada para compartilhar, entre o cliente e o servidor, uma chave que será utilizada na sessão. Baseado nisso, identifique a opção que contém o tipo de criptografia usada na sessão estabelecida, após o *Handshake*: 8

A) Simetrica;

B) Assimetrica;

C) Hash;

D) SSL.

Com a chave de sessão simétrica estabelecida, o TLS utiliza algoritmos de criptografia simétrica, como o AES, para criptografar os dados transmitidos entre o cliente e o servidor. Isso garante a confidencialidade dos dados, uma vez que só as partes autorizadas que possuem a chave de sessão podem decifrá-los.

5. Os algoritmos, em termos gerais, seguem uma série de passos para executar uma determinada tarefa ou resolver um problema específico. 10
   De forma resumida, indique 5 passos gerais que um algoritmo pode seguir.

1. Definição do Problema;
2. Entrada de Dados;
3. Processamento;
4. Tomada de Decisão;
5. Repetição (*Loops*);
6. Saída de Dados; e
7. Análise de Complexidade.

6. O Diffie-Hellman e o RSA são ambos algoritmos criptográficos usados para diferentes propósitos, contudo, frequentemente comparados devido à sua importância na criptografia de chave pública. Faça uma comparação entre os dois algoritmos em termos de Desempenho e a Segurança. 12

Desempenho:

- O Diffie-Hellman é geralmente mais rápido do que o RSA para a troca de chaves. Ele é especialmente eficiente em cenários onde a chave precisa ser estabelecida entre duas partes.
- O RSA é mais lento do que o Diffie-Hellman, especialmente quando se trata de operações de criptografia e descriptografia.

Segurança:

Ambos os algoritmos são considerados seguros quando usados com tamanhos de chave adequados. No entanto, o RSA tende a ter chaves maiores em comparação com o Diffie-Hellman para alcançar o mesmo nível de segurança.

Bom trabalho!

"Tem uma força dentro de você que é capaz de sempre te surpreender!"