1º TESTE DE SEGURANÇA INFORMATICA E DAS TELECOMUNICAÇÕES

Turma: LEIT41/42 [Pontuação máxima: 100] Data: 23 Abril 2024

1º Semestre **Correção** Duração: 80 min

Docente: Eng. Emírcio Zeca Vieira 1º Semestre

NOME: Nº

1. Em relação a segurança de redes, análise as afirmações abaixo e assinale V, se for Verdadeiras, ou F, se for Falsa.

   ( ) Conforme o conceito de segurança física, para todos os dispositivos de uma rede, há uma maneira de se fazer segurança.

   ( ) Equipamentos e dispositivos que ficam perto dos colaboradores da empresa devem ser filmados e monitorados por sistemas de segurança.

   ( ) Sobre a actualização das versões dos *softwares*, quando homologados, os testes são dispensados.

   ( ) Embora o cabeado esteja internamente no piso ou na parede, devem ser testados periodicamente.

   6

   Selecione a alinea correcta

   A) F – F – V – F;
   B) V – V – F – V;
   C) V – F – V – V;
   D) F – V – F – F;
   E) V – V – F – F**.**

2. Quando se deseja utilizar um algoritmo hash para criptografia, que gera um hash de 160 *bits* (ou 20 *bytes*) e que faz parte de alguns algoritmos de segurança (tipo TLS e SSL), deve-se utilizar o algoritmo conhecido como:

   6

   Selecione a afirmação correcta:

   A) AES;
   B) MD5;
   C) RC4;
   D) 3DES; e
   E) SHA-1.

3. Em termos de Segurança da Informação, ao assinar um pacote de dados com a chave privada do certificado digital e permitir que o conteúdo seja verificado no receptor através da chave pública, de acordo com o algoritmo RSA, é possível garantir a:

   10

   Selecione a afirmação correcta e justifique:

A) Confidencialidade;
B) **Integridade;**
C) Disponibilidade;
D) Veracidade.

Integridade dos dados, garante que os dados não sejam modificados durante a transmissão ou armazenamento. Isso é feito usando funções de hash criptográficas, que geram valores únicos para os dados e permitem verificar se foram alterados.

4. O *nobreak* é a ferramenta que garante qual princípio da segurança da informação?
   Selecione a afirmação correcta e justifique:

10

   A) Princípio da Confidencialidade;
   B) Princípio da Integridade;
   C) Princípio da Autenticidade;
   D) Princípio da Disponibilidade.

Nobreak é um equipamento que protege e mantém em funcionamento dispositivos eletroeletrônicos em situações de oscilação ou ausência da energia.

De acordo com o Princípio da Disponibilidade, a informação estará disponível sempre que for preciso. Esse aspecto é de suma importância, principalmente para sistemas que não podem ter falhas na Disponibilidade, pois essas falhas comprometem o serviço.

5. A empresa Z foi contratada para implementar uma solução de segurança onde: o algoritmo tem o tamanho do bloco de texto, às claras, igual a 64 *bits*; o tamanho do bloco de texto cifrado é de 64 *bits*; e o tamanho da sua chave é de 168 *bits*.

10

   Selecione a afirmação correcta e justifique:

   A) 3DES usa três chaves e uma execução do algoritmo DES;
   B) Algoritmo RC4 tem uma chave de comprimento variável entre 1 *byte* e 256 *bytes*;
   C) AES usa comprimento de chave que pode ser de 128, 256 ou 512 *bits*;
   D) Algoritmo RC4 é uma cifra de bloco com chave de tamanho variável;
   E) Cifra de bloco simétrica processa vários blocos de dados por vez.

A Criptografia 3DES (*Triple Data Encryption Standard*) é uma variante do algoritmo DES (*Data Encryption Standard*) que oferece maior segurança ao aplicar o algoritmo DES três vezes em sucessão. O DES é um algoritmo de criptografia simétrica que opera em blocos de 64 *bits* e usa uma chave de 56 *bits*. No entanto, devido ao aumento da capacidade computacional ao longo dos anos, a segurança do DES tornou-se insuficiente para muitas aplicações.

6. A criptografia de chave simétrica também é conhecida como secreta ou única, uma vez que utiliza a mesma chave tanto para codificar como para decodificar informações, garantindo a confidencialidade dos dados. Considere que um Técnico do Laboratório de Análises Clínicas, deseja enviar uma mensagem cifrada usando o algoritmo de cifra de chave simétrica. A figura a seguir ilustra a encriptação simétrica. É CORRECTO afirmar que o Técnico do Laboratório de Análises Clínicas deve usar o algoritmo: 10

A) Elgamal;

B) MD5 e RSA;

C) SHA-1;

D) AES e RC2;

E) AES.

O algoritmo AES é uma cifra de bloco simétrico que pode criptografar (codificar) e descriptografar (decifrar) informações.

A criptografia converte os dados em uma forma ininteligível chamada texto cifrado; descriptografar o texto cifrado converte os dados de volta em sua forma original, chamada de texto simples.

O algoritmo AES é capaz de usar chaves criptográficas de 128, 192 e 256 *bits* para criptografar e descriptografar dados em blocos de 128 *bits*."

7. Os Centro de Dados, são infra-estruturas complexas e compostas por diversos componentes que, quando equalizados correctamente, permitem o processamento e armazenamento de informações cruciais para a continuidade dos negócios de empresas. 12

Indique as funções do sistema de ar condicionado dedicado para *Data Center.*

Controlo da temperatura, Controlo da qualidade do ar e Controlo da humidade.

8. A construção de um Centro de Dados é um empreendimento complexo que requer uma consideração cuidadosa de vários factores. Indique cinco (5) aspectos a considerar para construir um Centro de Dados:

10

Alguns dos aspectos a considerar são: Acesso à rede de fibra óptica, Localização Geográfica, Segurança Física, Fontes de energia confiáveis, Acesso à mão-de-obra qualificada, Resfriamento eficiente, espaço para expansão ou requisitos da lei.

9. Tendo em conta o algoritmo RSA, com os parâmetros p = 2, q = 7.

   A) Faça a geração do par de chaves publica e privada.

16

1. Calcular o módulo: $n = p \times q = 7 \times 2 = 14$
2. Calcular o totiente de Euler: $\varphi(N) = (p - 1)(q - 1) = 6$
3. Escolher expoente $1 < e < 6$; e coprimo de 6 e 14
   - $e = 5$
   - 5 é primo e não é divisor de 6 e 14.
4. Calcular expoente d tal que $d \equiv e^{-1} \bmod \varphi(N)$
   - $d = 11$
   - $11 \times 5 \bmod \varphi(N) = 1$
5. **Chave pública** {n, e}: {14, 5}
6. **Chave privada** {n, d}: {14, 11}

   B) Tendo em conta as chaves obtidas e a mensagem m=2, calcule a mensagem Cifrada e a decifrada.

10

Cifrando ($m \rightarrow c$): $c \equiv m^e \bmod n = 2^5 \bmod 14 = 4$

Mensagem cifrada: $c = 4$

Decifrando ($m \rightarrow c$): $m \equiv c^d \bmod n = 4^{11} \bmod 14 = 2$

Bom trabalho! *"Sonhe, acredite, dedique-se e realize!"*