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 aos fundamentos sobre assinatura digital e certificação digital, analise os itens a seguir:

   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. 6

   Em relação aos itens apontados, pode-se afirmar que:
   Selecione a afirmação correcta:

   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. Uma empresa possui duas filiais localizadas em diferentes cidades e precisa estabelecer uma comunicação segura entre elas para transmitir informações confidenciais. Está sendo considerado a adoção de uma solução que envolva uma chave pública e privada entre o remetente e o destinatário. Assinale a opção que mostre uma solução que NÃO utiliza chave pública e privada. 6
   Selecione a afirmação correcta:

   A) **Uso do algoritmo AES;**
   B) Uso do algoritmo Diffie-Helmann;
   C) Assinatura digital;
   D) Certificado digital; e
   E) Uso de criptografia de Curva Elíptica.

3. O reconhecimento biométrico consiste em reconhecer um indivíduo com base nas suas características físicas ou comportamentais. A técnica adotada pelo sistema de identificação biométrico que implica em detectar e comparar a posição das minúcias (*minutiae*), também conhecida como características de Galton, é utilizada no reconhecimento da … 10

   Selecione a afirmação correcta e justifique:

   A) Impressão digital;
   B) Íris;
   C) Retina;
   D) Geometria da mão;
   E) Reconhecimento facial.

Biometria por digitais é o tipo biométrico mais utilizado hoje em dia, por ter uma grande aceitação, uma vez que há muito tempo é utilizado no campo forense. Ele consiste em analisar os elementos principais e únicos, conhecidos como minutiae, que podem ser as linhas papilares e suas bifurcações ou mesmo poros no dedo.

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*:
   Selecione a afirmação correcta e justifique: 10

   A) Simétrica.
   B) Assimétrica.
   C) Hash.
   D) RSS.
   E) SSL.

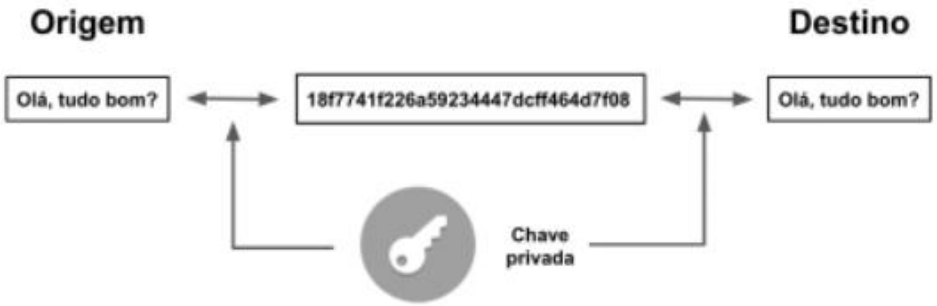
*É **simétrica** pois, ele usa a criptografia **assimétrica** para enviar uma "senha" que poderá ser utilizada para entrar na sessão.*

5. Cerlo, analista de segurança, recebeu a demanda de avaliar os algoritmos simétricos utilizados na rede do DSI. No parecer, o Cerlo afirmou correctamente que o(a):
   Selecione a afirmação correcta e justifique: 10

   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.

O algoritmo RC4 permite chaves de comprimento variável entre 1 *byte* (8 *bits*) e 256 *bytes* (ou 2048 *bits*), embora seja mais comum usar chaves de tamanho fixo, como 128 *bits*. Essa flexibilidade no comprimento da chave é uma das características do RC4 que o tornam amplamente utilizado em diversas 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) AES e RC2

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! *"É sem medo de errar que conseguimos os melhores acertos."*