Iniciado em	Sunday, 26 May 2019, 09:05
Estado	Finalizada
Concluída em	Sunday, 26 May 2019, 11:45
Tempo empregado	2 horas 40 minutos
Notas	35,00/42,00
Avaliar	**8,33** de um máximo de 10,00(**83**%)

Questão **1**

Correto

Atingiu 1,00 de 1,00

[Analista de redes e comunicação de dados - FUNCAB - 2010]
Para garantir que intrusos não possam comprometer uma conexão, qual o tipo de criptografia o protocolo SSL utiliza?

Escolha uma:

- a. Criptografia Assimétrica.
- b. Não utiliza criptografia.
- c. Criptografia Simétrica.
- d. Combinação de Criptografia Simétrica com Criptografia Assimétrica. ✔
- e. Combinação de sistema de chaves simétricas com criptografia de chave secreta.

A resposta correta é: Combinação de Criptografia Simétrica com Criptografia Assimétrica..

Questão **2**

Correto

Atingiu 1,00 de 1,00

[CEITEC - Analista de Sistemas 2012]
Mike e Meg desejam trocar mensagens de forma segura. Para tanto, decidem usar um aplicativo de criptografia assimétrica. Meg, descuidadamente, cria sua chave privada combinando a data de seu aniversário com o nome de seu cão de estimação. Apenas Mike tem a chave pública de Meg. Alan, todavia, é vizinho de Meg e é sempre convidado para sua festa de aniversário. Alan é Veterinário e tem em sua clínica um banco de dados com informações detalhadas de todos os animais de sua rua, inclusive o cão de Meg. Podemos afirmar então que Alan tem informações suficientes para:

Escolha uma:

- a. Ler as mensagens cifradas com a chave privada de Meg.
- b. Ele não poderá ler mensagens cifradas com a chave pública de Meg.
- c. Deduzir a chave de Meg, e, passar-se por ela criando mensagens assinadas que levariam todos que conhecem sua chave pública a pensar estarem se comunicando com ela. ✔
- d. Ler as mensagens cifradas com a chave pública de Mike.
- e. Ler as mensagens cifradas com a chave privada de Mike.

A resposta correta é: Deduzir a chave de Meg, e, passar-se por ela criando mensagens assinadas que levariam todos que conhecem sua chave pública a pensar estarem se comunicando com ela..

Questão **3**

Incorreto

Atingiu 0,00 de 1,00

[CTA - Técnico em Informática (2013) - VUNESP]
Os acessos aos sistemas bancários pela internet (internet banking) são realizados por meio de um sistema de criptografia que utiliza o esquema de chaves:

Escolha uma:

- a. públicas.
- b. simétricas.
- c. distribuídas. ✖
- d. privadas.
- e. compartilhadas.

A resposta correta é: públicas..

Questão **4**

Correto

Atingiu 1,00 de 1,00

[Defensoria Pública do Estado do Mato Grosso (DPE-MT) - Analista de Sistemas (2015) - FGV]
As funções de hashes criptográficos devem possuir determinadas características para o seu funcionamento adequado. Assinale a opção que indica uma delas.

Escolha uma:

- a. O valor de entrada possa ser facilmente achado, dado o hash de saída.
- b. O valor de entrada da função tenha um tamanho fixo.
- c. Os dois tipos de chaves assimétricas sejam utilizados.
- d. O número de colisões seja o menor possível. ✔
- e. O valor de saída da função tenha tamanho variável.

A resposta correta é: O número de colisões seja o menor possível..

Questão **5**

Correto

Atingiu 1,00 de 1,00

[Ministério da Fazenda (MF) - Analista de Finanças e Controle (2013) - ESAF]
O protocolo de segurança WEP (Wired Equivalent Privacy) do padrão 802.11 opera no nível de enlace de dados. A criptografia do WEP utiliza uma cifra de fluxo baseada no algoritmo:

Escolha uma:

- a. RC4. ✔
- b. 3DES.
- c. MD5.
- d. AES.
- e. RSA.

A resposta correta é: RC4..

Questão **6**

Correto

Atingiu 1,00 de 1,00

[Ministério da Fazenda (MF) - Analista de Finanças e Controle (2013) - ESAF]
A desvantagem dos algoritmos de chave simétrica é a exigência de uma chave secreta compartilhada. A fim de garantir a comunicação segura entre toda uma população de 4 pessoas, o total de chaves necessárias é:

Escolha uma:

- a. 12.
- b. 8.
- c. 6. ✔
- d. 4.
- e. 10.

A resposta correta é: 6..

Questão **7**

Correto

Atingiu 1,00 de 1,00

[Operador de Computador (2012) - IESES - 2012]
Criptografia de chave simétrica: também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Casos nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave).
Com base no texto acima, identifique os métodos criptográficos que usam chaves simétricas:
I. ECC; II. AES; III. DSA; IV. 3DES; V. RSA; VI. RC4.

Escolha uma:

- a. Estão corretas apenas as afirmativas I, III e IV.
- b. Estão corretas apenas as afirmativas I, IV e V.
- c. Apenas a afirmativa IV está correta.
- d. Estão corretas apenas as afirmativas II, IV e VI. ✔

A resposta correta é: Estão corretas apenas as afirmativas II, IV e VI..

Questão **8**

Correto

Atingiu 1,00 de 1,00

[Q15 - UEPB - 2012]
Analise as seguintes afirmações sobre criptografia: I) A criptografia simétrica realiza a cifragem e decifragem de informação através de algoritmos que utilizam a mesma chave. II) A criptografia de chave pública operam com duas chaves distintas: chave privada e chave pública. III) O resumo criptográfico é obtido através de uma função de hash (espalhamento). IV) O SSL é uma implementação popular da criptografia de chave pública.

Escolha uma:

- a. Apenas II e IV.
- b. Apenas I e III.
- c. Apenas I, II e IV.
- d. I, II, III e IV. ✔
- e. Apenas II, III e IV.

A resposta correta é: I, II, III e IV..

Questão **9**

Correto

Atingiu 1,00 de 1,00

[Q19 - VUNESP - Perito Criminal - 2013]
A criptografia hash permite que seja calculado um identificador digital de tamanho fixo, chamado de valor hash, a partir de uma string de qualquer tamanho. Assinale a alternativa que contém o algoritmo hash que trabalha com o valor fixo de 20 bytes.

Escolha uma:

- a. SHA-1. ✔
- b. MD4.0.
- c. MD5.
- d. SHA-2.
- e. MD2.

A resposta correta é: SHA-1..

Questão **10**

Incorreto

Atingiu 0,00 de 1,00

[Q38 - Analista Judiciário - 2010]
Acerca de criptografia, assinale a opção correta.

Escolha uma:

- a. A criptografia assimétrica baseia-se no conceito de par de chaves. O RSA é um algoritmo assimétrico que utiliza duas chaves criptográficas e cuja segurança fundamenta-se na dificuldade de fatoração de números inteiros extensos.
- b. Uma das vantagens da criptografia simétrica em relação à assimétrica é a maior velocidade de cifragem ou decifragem das mensagens. Embora os algoritmos de chave assimétrica sejam mais rápidos que os de chave simétrica, uma das desvantagens desse tipo de criptografia é a exigência de uma chave secreta compartilhada.
- c. Enquanto mecanismo de cifragem de bloco, a criptoanálise diferencial e linear tem como objetivo predizer a saída do bloco a partir das entradas, comparando-se as características entre os textos cifrados e decifrados byte a byte. Tais modalidades são utilizadas para decifrar o algoritmo simétrico RSA e facilitar a descoberta da chave. ✖
- d. Na criptografia assimétrica, cada parte da comunicação possui um par de chaves. Uma chave é utilizada para encriptar e a outra para decriptar uma mensagem. A chave utilizada para encriptar a mensagem é privada e divulgada para o transmissor, enquanto a chave usada para decriptar a mensagem é pública.
- e. Por definição, as funções de criptografia devem ser reversíveis. Alguns algoritmos como o DES (data encryption standard) e o DSS (digital signature standard) utilizam três chaves, uma para criptografar os dados (denominada chave pública), uma para decifrar os dados (denominada chave privada) e uma para aumentar a confiabilidade da encriptação (denominada chave confiável).

A resposta correta é: A criptografia assimétrica baseia-se no conceito de par de chaves. O RSA é um algoritmo assimétrico que utiliza duas chaves criptográficas e cuja segurança fundamenta-se na dificuldade de fatoração de números inteiros extensos..

Questão **11**

Correto

Atingiu 1,00 de 1,00

[Q63 - Perito Criminal - RJ - 2013]
Quanto a segurança de redes em fio existe uma tecnologiaque inclui duas melhorias em relação ao protocolo WEP (Wired Equivalent Privacy) incluindo melhor criptografia para transmissão de dados e autenticação de usuário. Estamos falando da tecnologia chamada de

Escolha uma:

- a. AP
- b. WAP
- c. WPE
- d. WPA ✔
- e. EP

A resposta correta é: WPA.

Questão **12**

Correto

Atingiu 1,00 de 1,00

[Q67 - Perito Criminal - DF - 2012]
A segurança em redes de computadores é um tema de grande debate atualmente, principalmente em redes sem fio (wireless). Assinale a alternativa que apresenta somente siglas de protocolos de segurança para redes wireless.

Escolha uma:

- a. WEP, WPA, WPA-2. ✔
- b. RST, FIN, ACK.
- c. HTTPS, TFTP, ICMP.
- d. CLP, HEC, GFC.
- e. DES, RSA, IDEA.

A resposta correta é: WEP, WPA, WPA-2..

Questão **13**

Correto

Atingiu 1,00 de 1,00

[Q68 - Perito Criminal - DF - 2012]
Com relação aos ataques a sistemas, assinale a alternativa que apresenta a definição de phreaking.

Escolha uma:

- a. Envio de quantidade excessiva de solicitações a um servidor com intenção de sobrecarregá-lo.
- b. Uso indevido de linha telefônicas, fixas ou móveis, para comunicação por voz ou dados. ✔
- c. Técnica usada para capturar informações que trafegam por uma rede de computadores.
- d. Envio de e-mail malicioso com o objetivo de pescar senhas e dados pessoais ou financeiros.
- e. Envio de sucessivos pings para um endereço de broadcast, fraudando-se o endereço de origem.

A resposta correta é: Uso indevido de linha telefônicas, fixas ou móveis, para comunicação por voz ou dados..

Questão **14**

Correto

Atingiu 1,00 de 1,00

[Q68 - Perito Criminal - RJ - 2013]
O fato de se poder conectar qualquer computador em qualquer lugar a qualquer outro computador pode torná-lo vulnerável. O recurso técnico para proteger essa conexão de dados é através de:

Escolha uma:

- a. Esteganografia
- b. Proxy
- c. Firewall ✔
- d. Certificação digital
- e. PKI

A resposta correta é: Firewall.

Questão **15**

Correto

Atingiu 1,00 de 1,00

[Q69 - Perito Criminal - RJ - 2013]
A criptografia vem de palavras gregas que significam ``escrita secreta'', permitindo assim que mensagens codificadas sejam enviadas. Existem dois tipos famosos de chaves criptográficas que são:

Escolha uma:

- a. chaves analógicas e chaves digitais.
- b. chaves simples e chaves compostas.
- c. chaves vetoriais e chaves matriciais.
- d. chaves curtas e chaves longas.
- e. chaves simétricas e chaves assimétricas. ✔

A resposta correta é: chaves simétricas e chaves assimétricas..

Questão **16**

Correto

Atingiu 1,00 de 1,00

[Q70 - Perito Criminal - RJ - 2013]
Existe um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. Estamos falando do método de:

Escolha uma:

- a. Sociologia criptográfica.
- b. Colarinho Branco.
- c. Engenharia de Serviço.
- d. Criptografia Privada.
- e. Engenharia Social. ✔

A resposta correta é: Engenharia Social..

Questão **17**

Correto

Atingiu 1,00 de 1,00

[Q72 - Perito Criminal - RJ - 2013]
Os protocolos criptográficos que conferem segurança de comunicação na Internet para serviços como email (SMTP), navegação por páginas (HTTP) e outros tipos de transferência de dados são caracterizados pela sigla:

Escolha uma:

- a. OSI.
- b. WPA.
- c. SSL. ✔
- d. EAP.
- e. IDS.

A resposta correta é: SSL..

Questão **18**

Correto

Atingiu 1,00 de 1,00

[Q73 - Perito Criminal - DF - 2012]
Assinale a alternativa que apresenta somente exemplos de algoritmos criptográficos de chave simétrica.

Escolha uma:

- a. RSA, ElGamal, DES.
- b. RC4, RC5, RSA.
- c. ElGamal, Diffie-Helman, Curvas Elípticas.
- d. Diffie-Helman, RSA, RC4.
- e. DES, IDEA, AES. ✔

A resposta correta é: DES, IDEA, AES..

Questão **19**

Correto

Atingiu 1,00 de 1,00

[Q73 - Perito Criminal - RJ - 2013]
Programa de computador de encriptação ou descriptografia de dados que fornece autenticação e privacidade criptográfica para comunicação de dados. Frequentemente utilizado, por exemplo, para assinatura digital, criptografia de textos, e-mails, arquivos, diretórios e partições inteiras de disco para incrementar a segurança de comunicações. Este programa é conhecido por:

Escolha uma:

- a. Cookie.
- b. ICP.
- c. PGP. ✔
- d. Cifra de César.
- e. Crypt.

A resposta correta é: PGP..

Questão **20**

Incorreto

Atingiu 0,00 de 1,00

[Q74 - Perito Criminal - DF - 2012]
A criptografia de chaves públicas usa o processo de certificação digital.
Assinale a alternativa que melhor define um certificado digital.

Escolha uma:

- a. Mecanismo que realiza a cifragem e a decifragem da informação por meio de algoritmos que utilizam uma mesma chave criptográfica.
- b. Credencial que identifica uma entidade, seja ela uma pessoa física ou jurídica, ou mesmo um computador.
- c. Processo criptográfico utilizado na transmissão da informação no qual o emissor não tem como negar a autoria de uma mensagem. ✖
- d. Entidade que emite, suspende, renova ou revoga chaves públicas e privadas para serem usadas em sistemas criptográficos.
- e. Arte de escrever em códigos, de forma a transformar a informação em um texto cifrado, incompreensível a quem possa lê-lo.

A resposta correta é: Credencial que identifica uma entidade, seja ela uma pessoa física ou jurídica, ou mesmo um computador..

Questão **21**

Correto

Atingiu 1,00 de 1,00

[Q74 - Perito Criminal - RJ - 2013]
Quanto à criptografia, as mensagens a serem criptografadas, conhecidas como texto simples, são transformadas por uma função que é parametrizada por uma chave. Em seguida, a saída do processo de criptografia, é conhecida como texto cifrado, e transmitida. Neste contexto, criptografia simétrica é um método de codificação que utiliza:

Escolha uma:

- a. Duas chaves privadas para codificar e decodificar a mensagem.
- b. Duas chaves públicas para codificar e decodificar a mensagem.
- c. A mesma chave para codificar e decodificar a mensagem. ✔
- d. Uma chave pública e uma chave privada para codificar e decodificar a mensagem.
- e. Uma chave simples e uma chave composta para codificar e decodificar a mensagem.

A resposta correta é: A mesma chave para codificar e decodificar a mensagem..

Questão **22**

Correto

Atingiu 1,00 de 1,00

[Q76 - Perito Criminal - DF - 2012]
A função hashing é um método criptográfico que gera uma sequência de bits de tamanho fixo, a partir de uma quantidade qualquer de caracteres de uma mensagem original, com a finalidade de assegurar a integridade da informação contida na mensagem. Acerca dos algoritmos de hash, assinale a alternativa correta.

Escolha uma:

- a. O algoritmo MD-5 produz um valor hash de 128 bits, para uma mensagem de entrada de qualquer tamanho. ✔
- b. A função hash MD-1 é uma evolução do MD-4 e MD-5 e gera uma sequência de 512 bits.
- c. O SHA-1, criado pelo MIT (Massachusetts Institute of Technology), é usado no IPSec.
- d. O RSA é um algoritmo de espalhamento unidirecional que gera um valor de 160 bits.
- e. O S/MIME é uma função hashing desenvolvida para uso em mensagebs de e-mail.

A resposta correta é: O algoritmo MD-5 produz um valor hash de 128 bits, para uma mensagem de entrada de qualquer tamanho..

Questão **23**

Correto

Atingiu 1,00 de 1,00

[Q76 - Perito Criminal - RJ - 2013]
RSA é um algoritmo de criptografia de dados, que deve a sua sigla ao nome dos três professores do Instituto MIT. Considerado como um dos mais seguros, as chaves geradas pelo RSA são baseadas:

Escolha uma:

- a. nos números primos. ✔
- b. no seno hiperbólico.
- c. matrizes de três dimensões.
- d. raízes triplas.
- e. nas funções tangenciais.

A resposta correta é: nos números primos..

Questão **24**

Correto

Atingiu 1,00 de 1,00

[Q77 - Perito Criminal - DF - 2012]
Esteganografia é um termo pouco utilizado no âmbito da segurança da informação, mas que exige cuidados especiais de quem se preocupa com o tema. Assinale a alternativa que apresenta a definição de esteganografia.

Escolha uma:

- a. Sinônimo de criptografia, é técnica de codificar a informação para que não seja entendida por terceiros.
- b. Técnica de esconder informações dentro de arquivos como imagens, sons, vídeos ou textos. ✔
- c. Algoritmo matemático que converte um texto claro em uma mensagem cifrada, e vice-versa.
- d. Estudo de técnicas de quebra de sigilo de mensagens eletrônicas criptografadas.
- e. Método para codificação de arquivos binários, transformando-os em texto ASCII.

A resposta correta é: Técnica de esconder informações dentro de arquivos como imagens, sons, vídeos ou textos..

Questão **25**

Incorreto

Atingiu 0,00 de 1,00

[Q81 - Perito Criminal - RJ - 2013]
Uma forma de evitar fraudes através de ataques conhecidos por man-in-the-middle é certificar-se que, quando acessar um site seguro (Exemplo: Bancos, Lojas de compras, etc) o navegador:

Escolha uma:

- a. apresente a identificação http.
- b. apresente o cadeado fechado (obtenção da aprovação da certificadora digital).
- c. apresente a identificação do fabricante do Sistema Operacional como Site Confiável.
- d. apresente a identificação https. ✖
- e. esteja indicando o nome correto do site acessado.

A resposta correta é: apresente o cadeado fechado (obtenção da aprovação da certificadora digital)..

Questão **26**

Correto

Atingiu 1,00 de 1,00

[Q82 - Perito Criminal - RJ - 2013]
Um site oficial do governo foi vítima de um ataque foi promovido por um programa semelhante ao vírus, mas se diferenciam por se espalharem sem a intervenção do usuário e se distribuem através de replicação automática, algumas vezes com mutações para dificultar sua identificação. Eles são conhecidos como:

Escolha uma:

- a. Adwares.
- b. Trojans.
- c. Hoaxs.
- d. Worms. ✔
- e. Backdoors.

A resposta correta é: Worms..

Questão **27**

Correto

Atingiu 1,00 de 1,00

[TCE - Analista Administrativo - Informática (2013) - CESPE]
Assinale a opção correta acerca de criptografia.

Escolha uma:

- a. Na criptografia assimétrica, a confidencialidade da mensagem é garantida de forma absoluta, uma vez que, nessa modalidade de criptografia, são utilizados pares de algoritmos na comunicação de dados.
- b. SHA-1 é um algoritmo voltado para criptografia de 128 bits.
- c. A criptografia simétrica garante a autenticidade da mensagem, uma vez que exclusivamente o emissor, detentor de chave privada, pode criptografar uma informação que será decriptografada pela chave pública.
- d. Os métodos criptográficos RSA, DAS e Diffie-Hellman implementam criptografia de chave secreta ou única, que visa, principalmente, garantir a confidencialidade. Nesse tipo de criptografia, utiliza-se uma mesma chave tanto para codificar como para decodificar os dados.
- e. O HMAC (Hash Message Authentication Code) pode ser considerado um suplemento do MD5, visto que se trata de um código de autenticação de mensagem criado com base em um valor-chave que é incluído no hash, de maneira que os dados originais e o MAC sofram hash na mesma resenha. ✔

A resposta correta é: O HMAC (Hash Message Authentication Code) pode ser considerado um suplemento do MD5, visto que se trata de um código de autenticação de mensagem criado com base em um valor-chave que é incluído no hash, de maneira que os dados originais e o MAC sofram hash na mesma resenha..

Questão **28**

Correto

Atingiu 1,00 de 1,00

[Tecnologia da Informação - 2012]
Na negociação de um[a] ..... o browser pode fazer uso de uma lista de CAs nas quais confia. O browser, para tanto, dispõe de ..... de todas aquelas CAs. De acordo com o protocolo SSL preenche corretamente a seguinte alternativa:

Escolha uma:

- a. Sessão/Chaves privadas.
- b. Sessão/Chaves públicas. ✔
- c. Socket/Chaves privadas.
- d. Algoritmo/Certificado.
- e. Assinatura/Chaves privadas.

A resposta correta é: Sessão/Chaves públicas..

Questão **29**

Correto

Atingiu 1,00 de 1,00

[Tribunal de Justiça do Estado de Minas Gerais (TJ-MG) - Oficial Judiciário (2012) - FUMARC]
Sobre os conceitos de criptografa, é correto afirmar que

Escolha uma:

- a. apesar de consumir mais recursos computacionais que a criptografa simétrica, a criptografa de chave pública apresenta grande vantagem em relação à segurança do processo de distribuição de chaves. ✔
- b. a criptografa de chave pública é mais segura contra criptoanálise do que a criptografa simétrica.
- c. a criptografa de chave pública praticamente substituiu os algoritmos de chave simétrica para aplicações web que necessitam de transferência segura de dados através da internet.
- d. os algoritmos de criptografa (simétrica e assimétrica) apresentam o mesmo nível de resistência quando utilizam chaves de mesmo tamanho.

A resposta correta é: apesar de consumir mais recursos computacionais que a criptografa simétrica, a criptografa de chave pública apresenta grande vantagem em relação à segurança do processo de distribuição de chaves..

Questão **30**

Correto

Atingiu 1,00 de 1,00

[Tribunal de Justiça do Estado do Amapá (TJ-AP) - Analista Judiciário (2014) - FCC]
Para prover segurança à rede sem fio da empresa, um especialista em segurança de redes adotou o padrão WPA2, que possui um método de
criptografia mais forte e algoritmos mais rápidos que padrões anteriores. O WPA2 adota a criptografia

Escolha uma:

- a. RC4 que permite chaves de 256 ou 512 bits.
- b. AES que permite chaves de 256 bits. ✔
- c. AES que permite chaves de 512 bits.
- d. 3DES que permite chaves de 168 bits.
- e. RC4 que permite chaves de 256 bits.

A resposta correta é: AES que permite chaves de 256 bits..

Questão **31**

Correto

Atingiu 1,00 de 1,00

[Tribunal Regional do Trabalho (TRT) - 12ª Região (SC) (2013) - FCC]
Trabalha com algoritmos que necessitam de pares de chaves, ou seja, duas chaves diferentes para cifrar e decifrar uma informação. A mensagem codificada com a chave 1 de um par somente poderá ser decodificada pela chave 2 deste mesmo par.O método de criptografia e os nomes das duas chaves referenciadas no texto são, respectivamente, criptografia.

Escolha uma:

- a. de chave secreta, chave privada e chave pública.
- b. assimétrica, chave pública e chave privada. ✔
- c. de curvas elípticas, chave pública e chave de hash.
- d. simétrica, chave pública e chave privada.
- e. de chave pública, chave primária e chave estrangeira.

A resposta correta é: assimétrica, chave pública e chave privada..

Questão **32**

Correto

Atingiu 1,00 de 1,00

[Tribunal Regional do Trabalho (TRT) - 18ª Região (GO) (2013) - FCC]
Fazendo uma analogia com documentos do mundo real, ...I.... seria o similar eletrônico do RG, enquanto ....II...., seria o equivalente ao carimbo acompanhado de selo que os cartórios brasileiros utilizam para reconhecer firma em documentos. Juntos, esses dois elementos, aliados à ....III...., garantem a autenticidade, a integridade, o não repúdio à transação e a confidencialidade da informação. Ou seja, as partes são mesmo quem dizem ser e a transação on- line é legítima, autêntica, segura e não sofreu alterações ao longo do caminho. Preenchem, correta e respectivamente, as lacunas:

Escolha uma:

- a. a assinatura digital - o certificado digital - segurança das informações.
- b. o certificado digital - a assinatura digital - criptografia. ✔
- c. a criptografia simétrica - a criptografia assimétrica - certificação digital.
- d. a chave pública - a chave privada - criptografia de chave única e à criptografia de chave dupla.
- e. a criptografia assimétrica - a criptografia simétrica - assinatura digital.

A resposta correta é: o certificado digital - a assinatura digital - criptografia..

Questão **33**

Correto

Atingiu 1,00 de 1,00

[Tribunal Regional do Trabalho (TRT) - 18ª Região (GO) (2013) - FCC]
Observe as regras de um algoritmo de criptografia:
Para criptografar uma mensagem, fazemos: c = m^e mod n Para descriptografá-la: m = c^d mod n. Onde: m = texto simples c = mensagem criptografada n = é o produto de dois números primos o par (e, n) = chave pública o par (d, n) = chave privada ^ = é a operação de exponenciação (a^b: a elevado à potência b) mod = é a operação de módulo (resto da divisão inteira) Este algoritmo é de domínio público e é amplamente utilizado nos navegadores para sites seguros e para criptografar e-mails. Trata-se do algoritmo.

Escolha uma:

- a. simétrico AES - Advanced Encryption Standard.
- b. simétrico DES - Data Encryption Standard.
- c. assimétrico RSA - Rivest, Shamir and Adleman. ✔
- d. simétrico RSA - Rivest, Shamir and Adleman.
- e. assimétrico AES - Advanced Encryption Standard.

A resposta correta é: assimétrico RSA - Rivest, Shamir and Adleman..

Questão **34**

Correto

Atingiu 1,00 de 1,00

[Tribunal Regional Eleitoral do São Paulo (TRE-SP) - Técnico Judiciário - Operação de Computador (2012) - FCC]
Com relação à criptografia é correto afirmar:

Escolha uma:

- a. Na encriptação por fluxo de dados, um bloco inteiro de texto claro de tamanho fixo é transformado em um bloco de texto cifrado. Em geral, os algoritmos que trabalham com fluxo de dados são mais lentos do que aqueles que trabalham com blocos.
- b. A segurança do algoritmo criptográfico RSA está diretamente relacionada com a dificuldade de realizar fatorações. É utilizado para garantir confidencialidade e autenticidade. ✔
- c. A força de uma chave criptográfica está unicamente relacionada ao seu algoritmo, independente do tamanho em bits da chave.
- d. A criptografia simétrica baseia-se na utilização de duas chaves, sendo uma mantida secreta, enquanto outra pode ser divulgada publicamente.
- e. O DES é um algoritmo de criptografia assimétrica que substitui os bits da mensagem clara pelos bits da mensagem criptografada. Sua principal desvantagem é a lenta execução.

A resposta correta é: A segurança do algoritmo criptográfico RSA está diretamente relacionada com a dificuldade de realizar fatorações. É utilizado para garantir confidencialidade e autenticidade..

Questão **35**

Incorreto

Atingiu 0,00 de 1,00

[Tribunal Regional Federal da 2ª Região (TRF - 2ª REGIÃO) - Analista Judiciário - Informática (2012) - FCC]
Paulo resolveu criptografar um texto simples de 227 bytes de comprimento utilizando um algoritmo de cifragem simétrica de blocos. A cifragem utilizada opera com blocos de 16 bytes. Nesse caso, o algoritmo pega os primeiros 16 bytes de dados, encripta-os, utilizando a tabela de chaves, e produz 16 bytes de texto cifrado. Em seguida, ele inicia novamente o processo, encriptando os próximos 16 bytes de texto simples. Após encriptar 14 blocos (224 bytes)

Escolha uma:

- a. deve-se acrescentar um byte cifrado a cada um dos últimos 3 blocos encriptados tornando-os blocos de 17 bytes cifrados.
- b. deve-se adicionar bytes extras aos 3 bytes restantes, formando um bloco de 16 bytes e, em seguida, encriptá-lo.
- c. o algoritmo encripta os 3 bytes restantes em um bloco de texto cifrado e anexa esse bloco ao último bloco de 16 bytes encriptado, formando um bloco final de 19 bytes.
- d. o algoritmo opera sobre os 3 bytes restantes, encriptando-os sozinhos em uma nova operação.
- e. o algoritmo cria um bloco com os 3 bytes restantes e anexa uma referência a esse bloco no último bloco de 16 bytes encriptado. ✖

A resposta correta é: deve-se adicionar bytes extras aos 3 bytes restantes, formando um bloco de 16 bytes e, em seguida, encriptá-lo..

Questão **36**

Correto

Atingiu 1,00 de 1,00

[Tribunal Superior do Trabalho (TST) - Analista Judiciário - Tecnologia da Informação (2012) - FCC]
No processo de gerenciamento da segurança da informação, a criptografia se apresenta como um dos recursos mais utilizados. Em uma transmissão de informação por meio da rede de computadores, a criptografia tem a função de

Escolha uma:

- a. garantir a disponibilidade do canal de transmissão de dados.
- b. confirmar a veracidade da autoria da informação recebida.
- c. verificar a confiabilidade do meio de transmissão por meio do Checksum.
- d. proteger os dados transmitidos contra acesso indevido. ✔
- e. recuperar o conteúdo de pacotes de dados recebidos de forma incompleta.

A resposta correta é: proteger os dados transmitidos contra acesso indevido..

Questão **37**

Correto

Atingiu 1,00 de 1,00

[Tribunal Superior do Trabalho (TST) - Analista Judiciário - Tecnologia da Informação (2012) - FCC]
O DES (Data Encryption Standard), padrão para criptografia de dados, apesar de não mais ser considerado seguro, é ainda amplamente utilizado para a segurança da informação em sua forma modificada 3-DES. O principal problema do DES é o comprimento da chave utilizada que possui

Escolha uma:

- a. 24 bits.
- b. 64 bits.
- c. 56 bits. ✔
- d. 96 bits.
- e. 32 bits.

A resposta correta é: 56 bits..

Questão **38**

Correto

Atingiu 1,00 de 1,00

[Q50 - Perito Criminal - PF - 2012]
Certificados digitais se baseiam no conceito de assinatura digital. O mecanismo usual para se assinar um documento eletrônico é primeiro gerar o hash do documento e então cifrar esse hash com um algoritmo assimétrico, utilizando-se sua chave privada. O valor assim obtido constitui a assinatura, que irá permitir, posteriormente, não apenas verificar a autoria do documento como também a sua integridade.

Escolha uma opção:

- Verdadeiro ✔
- Falso

A resposta correta é 'Verdadeiro'.

Questão **39**

Incorreto

Atingiu 0,00 de 1,00

[Q50 - Perito Criminal - PF - 2012]
O padrão de certificados largamente utilizado hoje em dia é o X.509, em sua versão 3. Um certificado gerado nesse padrão inclui, essencialmente, um identificador da versão utilizada para gerar o certificado (1, 2 ou 3); um número serial que deve ser único para cada certificado emitido por dada AC; um identificador do algoritmo de assinatura utilizado pela AC; um identificador da AC (DN – distinguished name da AC); período de validade do certificado; um identificador do sujeito (DN – distinguished name do sujeito) para o qual está sendo emitido o certificado; a chave pública do sujeito; a chave privada do sujeito; outras informações opcionais padronizadas; por fim, a própria assinatura da AC desse conjunto de informações.

Escolha uma opção:

- Verdadeiro ✖
- Falso

A resposta correta é 'Falso'.

Questão **40**

Correto

Atingiu 1,00 de 1,00

[Q50 - Perito Criminal - PF - 2012]
Certificados digitais são comumente emitidos para pessoas (físicas ou jurídicas), máquinas e processos. A utilização dos certificados requer o estabelecimento do que se denomina uma Infraestrutura de Chaves Públicas (ICP), como recentemente estabelecido pelo governo brasileiro, a ICP-Brasil. ICPs como a ICP-Brasil pressupõem a existência de pelo menos uma AC, cujo próprio certificado é auto-assinado, ou seja, ela própria atesta sua identidade e a detenção de seu par de chaves assimétricas, sendo ao mesmo tempo, para esse fim, emissor e sujeito no ato de certificação.

Escolha uma opção:

- Verdadeiro ✔
- Falso

A resposta correta é 'Verdadeiro'.

Questão **41**

Incorreto

Atingiu 0,00 de 1,00

[Q50 - Perito Criminal - PF - 2012]
A Internet já dispõe de recursos básicos para a utilização de certificados digitais por meio do protocolo SSL (Secure Sockets Layer), desenvolvido pela empresa Netscape com vistas ao desenvolvimento do comércio eletrônico, e, mais recentemente, o TLS (Transport Layer Security), desenvolvido a partir do SSL como um padrão do IETF (Internet Engineering Task Force). A utilização do SSL/TLS permite: a autentificação mútua das partes em comunicação por meio da verificação de seus certificados digitais apresentados no início de uma sessão; o estabelecimento de uma chave simétrica segura para ser utilizada entre as partes naquela sessão; a cifração com um algoritmo simétrico de toda a comunicação de dados, de forma transparente, no qual é utilizada a chave previamente estabelecida.

Escolha uma opção:

- Verdadeiro
- Falso ✖

A resposta correta é 'Verdadeiro'.

Questão **42**

Correto

Atingiu 1,00 de 1,00

[Q50 - Perito Criminal - PF - 2012]
Um dos pontos sensíveis na utilização de um sistema de chaves públicas é a geração do par de chaves de um usuário. Não somente o processo de geração deve resultar em uma chave privativa imprevisível, como esta deve ficar tão-somente sob a guarda de seu proprietário, com a maior segurança possível. O comprometimento da chave privativa de um usuário ou o acesso à mesma por terceiros compromete a segurança em sua utilização. Uma forma segura para a geração e a guarda de chaves e certificados disponível atualmente é o uso de cartões inteligentes (smart cards) para tal finalidade.

Escolha uma opção:

- Verdadeiro ✔
- Falso

A resposta correta é 'Verdadeiro'.

◄ sha256.c

Seguir para...