Primeira Bateria de Questões Com Resolução Assistida

Criptografia Simétrica e Assimétrica

1. No que diz respeito aos fundamentos de criptografia e certificação digital, julgue os itens subsecutivos. Nesse contexto, considere que a sigla AC, sempre que utilizada, se refira a autoridade certificadora.

[95] Na criptografia simétrica, a mesma chave compartilhada entre emissor e receptor é utilizada tanto para cifrar quanto para decifrar um documento. Na criptografia assimétrica, utiliza-se um par de chaves distintas, sendo a chave pública do receptor utilizada pelo emissor para cifrar o documento a ser enviado; posteriormente, o receptor utiliza sua chave privada para decifrar o documento.

[96] A utilização adequada dos mecanismos de criptografia permite que se descubra qualquer alteração em um documento por partes não autorizadas, o que garante a confidencialidade do documento.

[97] Para a utilização de criptografia assimétrica, a distribuição das chaves públicas é comumente realizada por meio de certificado digital, que contém o nome do usuário e a sua chave pública, sendo a autenticidade dessas informações garantida por assinatura digital de uma terceira parte confiável, denominada AC.

1. No que diz respeito aos fundamentos de criptografia e certificação digital, julgue os itens subsecutivos. Nesse contexto, considere que a sigla AC, sempre que utilizada, se refira a autoridade certificadora.

[95] Na criptografia simétrica, a mesma chave compartilhada entre emissor e receptor é utilizada tanto para cifrar quanto para decifrar um documento. Na criptografia assimétrica, utiliza-se um par de chaves distintas, sendo a chave pública do receptor utilizada pelo emissor para cifrar o documento a ser enviado; posteriormente, o receptor utiliza sua chave privada para decifrar o documento.

~~[96] A utilização adequada dos mecanismos de criptografia permite que se descubra qualquer alteração em um documento por partes não autorizadas, o que garante a confidencialidade do documento.~~

[97] Para a utilização de criptografia assimétrica, a distribuição das chaves públicas é comumente realizada por meio de certificado digital, que contém o nome do usuário e a sua chave pública, sendo a autenticidade dessas informações garantida por assinatura digital de uma terceira parte confiável, denominada AC.

2. No que diz respeito à criptografia, julgue os itens a seguir

[51] O texto cifrado F é obtido a partir do texto aberto C, utilizando-se o método monoalfabético de criptografia com chave igual a 3.

[52] As funções HASH são utilizadas para autenticar mensagens, não possuem chave de encriptação e são irreversíveis.

[53] Nos métodos mais seguros de criptografia, a função e a chave utilizadas na encriptação devem ser de conhecimento exclusivo do remetente da mensagem.

2. No que diz respeito à criptografia, julgue os itens a seguir

[51] O texto cifrado F é obtido a partir do texto aberto C, utilizando-se o método monoalfabético de criptografia com chave igual a 3.

[52] As funções HASH são utilizadas para autenticar mensagens, não possuem chave de encriptação e são irreversíveis.

~~[53] Nos métodos mais seguros de criptografia, a função e a chave utilizadas na encriptação devem ser de conhecimento exclusivo do remetente da mensagem.~~

3. Acerca dos conceitos de segurança de redes, criptografia e certificação digital, julgue os itens seguintes.

[97] AES, SHA-3 e RSA correspondem, respectivamente, a um algoritmo de criptografia simétrica, a uma função de hash criptográfico e a um algoritmo de criptografia assimétrica.

[98] É desaconselhável a implementação do algoritmo AES em sistemas embarcados, como smartphones e smart cards, visto que esses sistemas dispõem de pouco espaço físico e limitado poder de processamento.

3. Acerca dos conceitos de segurança de redes, criptografia e certificação digital, julgue os itens seguintes.

[97] AES, SHA-3 e RSA correspondem, respectivamente, a um algoritmo de criptografia simétrica, a uma função de hash criptográfico e a um algoritmo de criptografia assimétrica.

~~[98] É desaconselhável a implementação do algoritmo AES em sistemas embarcados, como smartphones e smart cards, visto que esses sistemas dispõem de pouco espaço físico e limitado poder de processamento.~~

4. Julgue os próximos itens, relativos ao uso de soluções criptográficas.

[62] As soluções criptográficas, ainda que possam ser quebráveis, são empregadas para tornar o ataque custoso, em termos econômicos e procedimentais, e, consequentemente, inviabilizar o objetivo malicioso.

[63] A colisão de hashes ocorre quando duas entradas de mensagens idênticas resultam em dois valores diversos de message digest ou hash, e pode decorrer, por exemplo, de exploração do tipo força bruta (ataque de dicionário).

[64] O algoritmo AES, em relação ao DES, seu antecessor, apresenta as seguintes vantagens: maior tamanho de blocos, uso de chaves de tamanho variável e variabilidade do número de rounds.

4. Julgue os próximos itens, relativos ao uso de soluções criptográficas.

[62] As soluções criptográficas, ainda que possam ser quebráveis, são empregadas para tornar o ataque custoso, em termos econômicos e procedimentais, e, consequentemente, inviabilizar o objetivo malicioso.

~~[63] A colisão de hashes ocorre quando duas entradas de mensagens idênticas resultam em dois valores diversos de message digest ou hash, e pode decorrer, por exemplo, de exploração do tipo força bruta (ataque de dicionário).~~

[64] O algoritmo AES, em relação ao DES, seu antecessor, apresenta as seguintes vantagens: maior tamanho de blocos, uso de chaves de tamanho variável e variabilidade do número de rounds.

5. Considerando que as técnicas associadas à criptografia são comumente empregadas para se atingir requisitos de segurança, julgue os itens a seguir.

[76] Em sistemas de uso prático, são usadas as técnicas simétricas e as assimétricas combinadas.

[77] A confidencialidade pode ser obtida pelo uso da criptografia simétrica e da assimétrica.

[78] Em conjunto com as funções de resumo criptográfico (hash), a criptografia simétrica proporciona autenticidade.

[79] A criptografia assimétrica proporciona o não repúdio, não proporcionando, porém, a autenticidade.

[80] As funções de resumo criptográfico oferecem garantia probabilística de inforjabilidade

5. Considerando que as técnicas associadas à criptografia são comumente empregadas para se atingir requisitos de segurança, julgue os itens a seguir.

[76] Em sistemas de uso prático, são usadas as técnicas simétricas e as assimétricas combinadas.

[77] A confidencialidade pode ser obtida pelo uso da criptografia simétrica e da assimétrica.

~~[78] Em conjunto com as funções de resumo criptográfico (hash), a criptografia simétrica proporciona autenticidade.~~

~~[79] A criptografia assimétrica proporciona o não repúdio, não proporcionando, porém, a autenticidade.~~

[80] As funções de resumo criptográfico oferecem garantia probabilística de inforjabilidade

6. Acerca de controle de acesso e certificação digital, julgue os itens a seguir.

[75] Em uma PKI (public key infrastructure), utiliza-se uma solução mista de troca de conteúdo encriptado, em que são manejadas soluções de criptografia simétrica, criptografia assimétrica e funções hash, para se garantir a disponibilidade das informações.

6. Acerca de controle de acesso e certificação digital, julgue os itens a seguir.

~~[75] Em uma PKI (public key infrastructure), utiliza-se uma solução mista de troca de conteúdo encriptado, em que são manejadas soluções de criptografia simétrica, criptografia assimétrica e funções hash, para se garantir a disponibilidade das informações.~~

7. A respeito de segurança da informação, julgue os seguintes itens.

[91] A criptografia hash é one-way, pois, uma vez obtido um valor hash h para uma string x, é computacionalmente impossível encontrar um valor de x que gere o hash h.

[93] RSA é um algoritmo simétrico que pode utilizar qualquer uma das suas duas chaves relacionadas para criptografar textos ou mensagens, sendo a outra chave utilizada para decriptografar.

7. A respeito de segurança da informação, julgue os seguintes itens.

[91] A criptografia hash é one-way, pois, uma vez obtido um valor hash h para uma string x, é computacionalmente impossível encontrar um valor de x que gere o hash h.

~~[93] RSA é um algoritmo simétrico que pode utilizar qualquer uma das suas duas chaves relacionadas para criptografar textos ou mensagens, sendo a outra chave utilizada para decriptografar.~~

8. Acerca da criptografia de chave simétrica, assinale a opção correta.

A. O padrão de criptografia DES (Digital Encryption Standard) utiliza exclusivamente o método de cifragem de fluxo, por considerá-lo mais seguro.

B. Mesmo não conhecendo a chave, um invasor pode descobrir uma mensagem ao examinar o texto cifrado e, assim, identificar algumas combinações.

C. Não há a necessidade de que a chave para criptografar seja a mesma para decriptografar, o essencial é que ela tenha a mesma quantidade de bytes para que se mantenha a simetria.

D. Na criptografia por chave simétrica, um usuário, ao usar um algoritmo para criptografar e um outro diferente para decriptografar, obterá um resultado válido.

E. O método de ataque conhecido como força bruta é ineficaz para a descoberta da chave utilizada nesse tipo de criptografia.

8. Acerca da criptografia de chave simétrica, assinale a opção correta.

~~A. O padrão de criptografia DES (Digital Encryption Standard) utiliza exclusivamente o método de cifragem de fluxo, por considerá-lo mais seguro.~~

B. Mesmo não conhecendo a chave, um invasor pode descobrir uma mensagem ao examinar o texto cifrado e, assim, identificar algumas combinações.

~~C. Não há a necessidade de que a chave para criptografar seja a mesma para decriptografar, o essencial é que ela tenha a mesma quantidade de bytes para que se mantenha a simetria.~~

~~D. Na criptografia por chave simétrica, um usuário, ao usar um algoritmo para criptografar e um outro diferente para decriptografar, obterá um resultado válido.~~

~~E. O método de ataque conhecido como força bruta é ineficaz para a descoberta da chave utilizada nesse tipo de criptografia.~~

9. Acerca de criptografia e da infraestrutura de chave pública, julgue os itens subsecutivos.

[95] A técnica de criptografia de chave única utiliza a mesma chave para criptografar e descriptografar uma mensagem.

9. Acerca de criptografia e da infraestrutura de chave pública, julgue os itens subsecutivos.

[95] A técnica de criptografia de chave única utiliza a mesma chave para criptografar e descriptografar uma mensagem.

10. No que se refere à segurança da informação, julgue os itens a seguir.

[51] Para averiguar a integridade de um arquivo de computador a ser transmitido por um meio inseguro, pode-se gerar um hash antes da transmissão e verificar o hash após a transmissão.

[54] A utilização de algoritmos de criptografia garante a disponibilidade e a autenticidade de informações em ambientes de tecnologia da informação.

[55] A lentidão e a paralisação do funcionamento de um sítio de comércio eletrônico que provê transações para venda de produtos é considerado incidente que viola a confidencialidade das informações do sítio.

10. No que se refere à segurança da informação, julgue os itens a seguir.

[51] Para averiguar a integridade de um arquivo de computador a ser transmitido por um meio inseguro, pode-se gerar um hash antes da transmissão e verificar o hash após a transmissão.

~~[54] A utilização de algoritmos de criptografia garante a disponibilidade e a autenticidade de informações em ambientes de tecnologia da informação.~~

~~[55] A lentidão e a paralisação do funcionamento de um sítio de comércio eletrônico que provê transações para venda de produtos é considerado incidente que viola a confidencialidade das informações do sítio.~~

GABARITO

1. C, E, C
2. C, C, E
3. C, E
4. C, E, C, C
5. C, C, E, E, C
6. E
7. C, E
8. B
9. C
10. C, E, E

Segunda Bateria de Questões Com Resolução Assistida

Criptografia Simétrica e Assimétrica

1. A respeito de criptografia, julgue os próximos itens.

[92] Os algoritmos de criptografia simétricos apresentam menor desempenho que os algoritmos assimétricos.

[93] A criptologia incorpora estudos e conhecimentos das áreas de criptografia e criptoanálise.

[94] No RSA (Rivest-Shamir-Adleman), o texto claro é criptografado em blocos com valor binário limitado.

1. A respeito de criptografia, julgue os próximos itens.

~~[92] Os algoritmos de criptografia simétricos apresentam menor desempenho que os algoritmos assimétricos.~~

[93] A criptologia incorpora estudos e conhecimentos das áreas de criptografia e criptoanálise.

[94] No RSA (Rivest-Shamir-Adleman), o texto claro é criptografado em blocos com valor binário limitado.

2. A respeito de certificação digital, julgue os itens seguintes.

[90] O algoritmo RSA gera chaves públicas de tamanho fixo e limitado a 2.048 bits

2. A respeito de certificação digital, julgue os itens seguintes.

~~[90] O algoritmo RSA gera chaves públicas de tamanho fixo e limitado a 2.048 bits~~

3. Julgue os próximos itens, relativos à segurança da informação.

[76] Para evitar o acesso de terceiros não confiáveis aos dados, pode-se utilizar a criptografia simétrica, técnica que confere confidencialidade às informações.

3. Julgue os próximos itens, relativos à segurança da informação.

[76] Para evitar o acesso de terceiros não confiáveis aos dados, pode-se utilizar a criptografia simétrica, técnica que confere confidencialidade às informações.

4. Acerca de criptografias simétrica e assimétrica em uma sessão TLS, julgue os itens subsecutivos.

[117] O RC4 é um algoritmo simétrico suportado tanto no TLS 1.2 quanto no SSL 3.0.

[118] No TLS 1.2, a função SHA-256 foi substituída pelo MD5-SHA-1.

4. Acerca de criptografias simétrica e assimétrica em uma sessão TLS, julgue os itens subsecutivos.

[117] O RC4 é um algoritmo simétrico suportado tanto no TLS 1.2 quanto no SSL 3.0.

~~[118] No TLS 1.2, a função SHA-256 foi substituída pelo MD5-SHA-1.~~

5. Julgue os itens a seguir, a respeito de criptografia.

[115] O algoritmo de criptografia MD5 (Message-Digest Algorithm 5) é um método que transforma uma palavra em um código criptografado único, ou seja, não é possível que duas strings diferentes produzam o mesmo hash.

[117] Criptografia de chave simétrica, que também é conhecida como criptografia de chave pública, utiliza chaves distintas para codificar e decodificar as informações. Uma dessas chaves é pública e a outra é do gerador da criptografia..

5. Julgue os itens a seguir, a respeito de criptografia.

~~[115] O algoritmo de criptografia MD5 (Message-Digest Algorithm 5) é um método que transforma uma palavra em um código criptografado único, ou seja, não é possível que duas strings diferentes produzam o mesmo hash.~~

~~[117] Criptografia de chave simétrica, que também é conhecida como criptografia de chave pública, utiliza chaves distintas para codificar e decodificar as informações. Uma dessas chaves é pública e a outra é do gerador da criptografia..~~

6. Criptografia é uma técnica matemática capaz de transformar uma informação da sua forma original para outra forma totalmente ilegível, a partir da qual um processo inverso pode voltar a recuperar a informação para seu formato original. Acerca dessas informações, assinale a opção correta.

A. A técnica criptográfica garante os atributos de autenticidade, integridade, confidencialidade, disponibilidade e não repúdio da informação.

B. Os algoritmos de chaves simétricas e assimétricas são as categorias básicas de algoritmos criptográficos, sendo os de chaves assimétricas a base conceitual da certificação digital.

C. Os algoritmos RSA e as curvas elípticas são exemplos de algoritmos criptográficos com base em chaves simétricas.

D. Os algoritmos DES e AES são exemplos de algoritmos criptográficos com base em chaves assimétricas.

E. Quando criptografada, a informação passa a ter a garantia de nível máximo de proteção

6. Criptografia é uma técnica matemática capaz de transformar uma informação da sua forma original para outra forma totalmente ilegível, a partir da qual um processo inverso pode voltar a recuperar a informação para seu formato original. Acerca dessas informações, assinale a opção correta.

A. ~~A técnica criptográfica garante os atributos de autenticidade, integridade, confidencialidade, disponibilidade e não repúdio da informação.~~

B. Os algoritmos de chaves simétricas e assimétricas são as categorias básicas de algoritmos criptográficos, sendo os de chaves assimétricas a base conceitual da certificação digital.

C. ~~Os algoritmos RSA e as curvas elípticas são exemplos de algoritmos criptográficos com base em chaves simétricas.~~

D. ~~Os algoritmos DES e AES são exemplos de algoritmos criptográficos com base em chaves assimétricas.~~

E. ~~Quando criptografada, a informação passa a ter a garantia de nível máximo de proteção~~

7. Julgue os próximos itens, acerca de segurança da informação.

[91] Um exemplo da utilização de criptografia contra ataques à confidencialidade é a criptografia de enlace, em que cada enlace de comunicação vulnerável é equipado nas duas extremidades com um dispositivo de criptografia, protegendo o tráfego em todos os enlaces de comunicações

7. Julgue os próximos itens, acerca de segurança da informação.

[91] Um exemplo da utilização de criptografia contra ataques à confidencialidade é a criptografia de enlace, em que cada enlace de comunicação vulnerável é equipado nas duas extremidades com um dispositivo de criptografia, protegendo o tráfego em todos os enlaces de comunicações

8. Julgue os próximos itens, relativos à criptografia.

[116] Na criptografia assimétrica, as chaves pública e privada têm as funções de cifração e decifração, respectivamente.

[117] Se um remetente cifra uma mensagem com sua chave privada e, a seguir, cifra o resultado novamente com a chave pública do destinatário, apenas este último poderá recuperar a mensagem e somente se dispuser da chave pública do remetente.

[118] A criptografia simétrica provê confidencialidade, integridade, autenticidade e não repúdio.

[120] São modos de operação seguros para cifras simétricas ECB, CBC e CTR.

8. Julgue os próximos itens, relativos à criptografia.

~~[116] Na criptografia assimétrica, as chaves pública e privada têm as funções de cifração e decifração, respectivamente.~~

[117] Se um remetente cifra uma mensagem com sua chave privada e, a seguir, cifra o resultado novamente com a chave pública do destinatário, apenas este último poderá recuperar a mensagem e somente se dispuser da chave pública do remetente.

~~[118] A criptografia simétrica provê confidencialidade, integridade, autenticidade e não repúdio.~~

~~[120] São modos de operação seguros para cifras simétricas ECB, CBC e CTR~~.

9. Uma empresa cuja matriz está localizada em Brasília possui três filiais localizadas em outras cidades do Brasil. As atribuições da matriz incluem analisar todas as propostas de negócio e autorizar os valores finais da negociação, além de analisar a documentação dos clientes para a liberação do crédito. Como atende a clientes em cidades onde não possui pontos de atendimento, a empresa recebe as propostas e documentos dos clientes eletronicamente e fecha contratos à distância. Os clientes também podem ser atendidos nas filiais, caso em que elas se responsabilizam pela recepção dos documentos e pelo seu envio, por meio eletrônico, para a matriz.

Com base nessa situação hipotética, julgue os seguintes itens.

[78] Para garantir o não repúdio de transações feitas com um grupo de quatro clientes corporativos, deve-se implementar uma solução baseada em algoritmo simétrico de criptografia.

[79] Para garantir o sigilo dos dados trocados entre as filiais utilizando-se algoritmos de criptografia simétrica, é necessário que as chaves criptográficas sejam aleatoriamente definidas a cada transação.

[80] A garantia de autenticidade dos documentos enviados à matriz pelas filiais pode ser obtida utilizando-se um algoritmo de criptografia simétrica.

9. Uma empresa cuja matriz está localizada em Brasília possui três filiais localizadas em outras cidades do Brasil. As atribuições da matriz incluem analisar todas as propostas de negócio e autorizar os valores finais da negociação, além de analisar a documentação dos clientes para a liberação do crédito. Como atende a clientes em cidades onde não possui pontos de atendimento, a empresa recebe as propostas e documentos dos clientes eletronicamente e fecha contratos à distância. Os clientes também podem ser atendidos nas filiais, caso em que elas se responsabilizam pela recepção dos documentos e pelo seu envio, por meio eletrônico, para a matriz.

Com base nessa situação hipotética, julgue os seguintes itens.

~~[78] Para garantir o não repúdio de transações feitas com um grupo de quatro clientes corporativos, deve-se implementar uma solução baseada em algoritmo simétrico de criptografia.~~

~~[79] Para garantir o sigilo dos dados trocados entre as filiais utilizando-se algoritmos de criptografia simétrica, é necessário que as chaves criptográficas sejam aleatoriamente definidas a cada transação.~~

[80] A garantia de autenticidade dos documentos enviados à matriz pelas filiais pode ser obtida utilizando-se um algoritmo de criptografia simétrica.

10. Com relação aos sistemas de criptografia e suas aplicações, julgue os itens subsecutivos.

[83] Se um usuário assina uma mensagem com sua própria chave pública e a envia, o destinatário será capaz de verificar a autenticidade e a integridade da mensagem.

[84] Em sistemas de criptografia assimétrica existem duas chaves com funções complementares que devem ser mantidas em segredo.

[85] Se um usuário cifra uma mensagem com a chave pública do destinatário e depois cifra novamente com sua própria chave privada, apenas o destinatário será capaz de recuperar a mensagem em claro.

10. Com relação aos sistemas de criptografia e suas aplicações, julgue os itens subsecutivos.

~~[83] Se um usuário assina uma mensagem com sua própria chave pública e a envia, o destinatário será capaz de verificar a autenticidade e a integridade da mensagem.~~

~~[84] Em sistemas de criptografia assimétrica existem duas chaves com funções complementares que devem ser mantidas em segredo.~~

[85] Se um usuário cifra uma mensagem com a chave pública do destinatário e depois cifra novamente com sua própria chave privada, apenas o destinatário será capaz de recuperar a mensagem em claro.

GABARITO

1. E, C, C
2. E
3. C
4. C, E
5. E, E
6. B
7. C
8. E, C, E, E
9. E, E, C
10. E, E, C

Terceira Bateria de Questões Com Resolução Assistida

Criptografia Simétrica e Assimétrica

1. Julgue os itens seguintes, acerca de criptografia e algoritmos de criptografia.

[74] Para o algoritmo RSA, chaves de 1024 bits são consideradas inseguras.

[75] Em função da colisão de MD5, utilizada no algoritmo AES para criptografia assimétrica, chaves de 128 bits não são recomendadas em aplicações com criptografia assimétrica.

[76] Por meio da assinatura digital, é possível verificar a propriedade da autenticidade de determinada informação.

1. Julgue os itens seguintes, acerca de criptografia e algoritmos de criptografia.

~~[74] Para o algoritmo RSA, chaves de 1024 bits são consideradas inseguras.~~

~~[75] Em função da colisão de MD5, utilizada no algoritmo AES para criptografia assimétrica, chaves de 128 bits não são recomendadas em aplicações com criptografia assimétrica~~.

[76] Por meio da assinatura digital, é possível verificar a propriedade da autenticidade de determinada informação.

2. Julgue os próximos itens a respeito de segurança da informação.

[51] Na criptografia simétrica, são geradas duas chaves criptográficas, uma privada e outra pública, para que um arquivo seja transferido, entre dois computadores, de forma criptografada.

[52] O hash poderá auxiliar na verificação da integridade de um arquivo transferido de um computador para outro.

[53] Assinatura digital é um mecanismo capaz de garantir a autenticidade e a integridade de um arquivo transferido via Internet.

[54] Considere que um arquivo que esteja sendo transferido entre dois usuários tenha sido interceptado e seu conteúdo tenha sido visualizado e encaminhado a outros usuários. Nessa situação, caracterizou-se a ocorrência do comprometimento da integridade do arquivo.

[55] Se um sítio da web sofrer comprometimento devido a problemas de hardware no servidor, impossibilitando a visualização do conteúdo pelos usuários, esse fato poderá ser considerado como comprometimento da disponibilidade do serviço.

2. Julgue os próximos itens a respeito de segurança da informação.

~~[51] Na criptografia simétrica, são geradas duas chaves criptográficas, uma privada e outra pública, para que um arquivo seja transferido, entre dois computadores, de forma criptografada.~~

[52] O hash poderá auxiliar na verificação da integridade de um arquivo transferido de um computador para outro.

[53] Assinatura digital é um mecanismo capaz de garantir a autenticidade e a integridade de um arquivo transferido via Internet.

~~[54] Considere que um arquivo que esteja sendo transferido entre dois usuários tenha sido interceptado e seu conteúdo tenha sido visualizado e encaminhado a outros usuários. Nessa situação, caracterizou-se a ocorrência do comprometimento da integridade do arquivo.~~

[55] Se um sítio da web sofrer comprometimento devido a problemas de hardware no servidor, impossibilitando a visualização do conteúdo pelos usuários, esse fato poderá ser considerado como comprometimento da disponibilidade do serviço.

3. Acerca dos algoritmos de criptografia simétricos e dos algoritmos de criptografia assimétricos, julgue os próximos itens.

[92] Em algoritmos assimétricos, as chaves são matematicamente independentes e a fatoração dos dados permite obter a relação de independência.

[93] O algoritmo RSA define que, para cada iteração de passagem da cifra de bloco, a chave do bloco seja dependente do bloco anterior. Esse algoritmo também define que a chave seja de 56 bits.

[94] O algoritmo AES, que é simétrico, opera com cifra de blocos de tamanho fixo e chaves com tamanhos variados de 128, 192 ou 256 bits.

3. Acerca dos algoritmos de criptografia simétricos e dos algoritmos de criptografia assimétricos, julgue os próximos itens.

~~[92] Em algoritmos assimétricos, as chaves são matematicamente independentes e a fatoração dos dados permite obter a relação de independência.~~

~~[93] O algoritmo RSA define que, para cada iteração de passagem da cifra de bloco, a chave do bloco seja dependente do bloco anterior. Esse algoritmo também define que a chave seja de 56 bits.~~

[94] O algoritmo AES, que é simétrico, opera com cifra de blocos de tamanho fixo e chaves com tamanhos variados de 128, 192 ou 256 bits.

4. Com relação às funções de hash, à assinatura digital e aos certificados digitais, julgue os itens a seguir.

[115] Uma função de hash não linear é aquela em que uma mensagem de determinado tamanho, que utiliza salt bit, deve passar por uma função e gerar uma saída de tamanho aleatório.

4. Com relação às funções de hash, à assinatura digital e aos certificados digitais, julgue os itens a seguir.

~~[115] Uma função de hash não linear é aquela em que uma mensagem de determinado tamanho, que utiliza salt bit, deve passar por uma função e gerar uma saída de tamanho aleatório.~~

5. No que se refere à criptografia, julgue os itens que se seguem.

[109] Enquanto a criptografia simétrica utiliza a mesma chave para cifração e decifração, a assimétrica utiliza uma chave exclusiva para cifração e outra exclusiva para decifração.

[110] A cifra AES usa um tamanho de bloco fixo de 128 bits e pode operar usando chaves com tamanho de 128, 192 ou 256 bits.

5. No que se refere à criptografia, julgue os itens que se seguem.

~~[109] Enquanto a criptografia simétrica utiliza a mesma chave para cifração e decifração, a assimétrica utiliza uma chave exclusiva para cifração e outra exclusiva para decifração.~~

[110] A cifra AES usa um tamanho de bloco fixo de 128 bits e pode operar usando chaves com tamanho de 128, 192 ou 256 bits.

6. Acerca dos algoritmos de criptografia e de compressão de arquivos de dados, julgue os seguintes itens.

[116] A compressão de dados antes da encriptação geralmente aumenta a segurança do sistema, por reduzir a redundância na mensagem, dificultando a criptoanálise.

[117] Esquemas de criptografia de chave pública também são conhecidos como de criptografia simétrica, pois possuem apenas uma chave, tanto para encriptação quanto para desencriptação.

6. Acerca dos algoritmos de criptografia e de compressão de arquivos de dados, julgue os seguintes itens.

[116] A compressão de dados antes da encriptação geralmente aumenta a segurança do sistema, por reduzir a redundância na mensagem, dificultando a criptoanálise.

~~[117] Esquemas de criptografia de chave pública também são conhecidos como de criptografia simétrica, pois possuem apenas uma chave, tanto para encriptação quanto para desencriptação.~~

7. A respeito de criptografia, julgue os itens subsequentes.

[102] Modos de operação de cifra de bloco permitem cifrar mensagens de tamanhos arbitrários com a utilização de algoritmos de cifragem de blocos, que trabalham com blocos de tamanho fixo. Os modos de operação existentes asseguram a confidencialidade e a integridade da mensagem cifrada, embora nem todos possam ser utilizados para autenticação.

[103] A confidencialidade e a integridade de uma comunicação são garantidas com o uso de criptografia tanto simétrica quanto assimétrica. No entanto, para garantir autenticidade e irretratabilidade, é necessário o uso combinado desses dois tipos de criptografia

7. A respeito de criptografia, julgue os itens subsequentes.

~~[102] Modos de operação de cifra de bloco permitem cifrar mensagens de tamanhos arbitrários com a utilização de algoritmos de cifragem de blocos, que trabalham com blocos de tamanho fixo. Os modos de operação existentes asseguram a confidencialidade e a integridade da mensagem cifrada, embora nem todos possam ser utilizados para autenticação.~~

~~[103] A confidencialidade e a integridade de uma comunicação são garantidas com o uso de criptografia tanto simétrica quanto assimétrica. No entanto, para garantir autenticidade e irretratabilidade, é necessário o uso combinado desses dois tipos de criptografia~~

8. Julgue os itens a seguir, a respeito de certificação digital e algoritmos RSA, AES e RC4.

[106] Embora o algoritmo RSA satisfaça aos requisitos necessários para prover assinatura digital, ele é utilizado, por questões de desempenho, em conjunto com funções de hashes criptográficos, como SHA-1.

8. Julgue os itens a seguir, a respeito de certificação digital e algoritmos RSA, AES e RC4.

[106] Embora o algoritmo RSA satisfaça aos requisitos necessários para prover assinatura digital, ele é utilizado, por questões de desempenho, em conjunto com funções de hashes criptográficos, como SHA-1.

9. A respeito de hashes criptográficos, julgue os itens que se seguem.

[107] SHA-1 e MD-5 são exemplos de hashes criptográficos largamente utilizados na Internet. O MD-5 tem sido substituído pelo SHA-1 pelo fato de este gerar um hash maior e ser o único à prova de colisões.

[108] O SHA-1, comumente usado em protocolos de segurança, como TLS, SSH e IPSec, também é utilizado por alguns sistemas de controle de versão como Git e Mercurial para garantir a integridade das revisões.

9. A respeito de hashes criptográficos, julgue os itens que se seguem.

~~[107] SHA-1 e MD-5 são exemplos de hashes criptográficos largamente utilizados na Internet. O MD-5 tem sido substituído pelo SHA-1 pelo fato de este gerar um hash maior e ser o único à prova de colisões.~~

[108] O SHA-1, comumente usado em protocolos de segurança, como TLS, SSH e IPSec, também é utilizado por alguns sistemas de controle de versão como Git e Mercurial para garantir a integridade das revisões.

10. Julgue os itens a seguir, referentes à criptografia e assinatura e certificação digitais.

[67] Uma assinatura digital consiste na cifração do resumo criptográfico de uma mensagem ou arquivo, com o uso da chave privada de quem assina.

10. Julgue os itens a seguir, referentes à criptografia e assinatura e certificação digitais.

[67] Uma assinatura digital consiste na cifração do resumo criptográfico de uma mensagem ou arquivo, com o uso da chave privada de quem assina.

GABARITO

1. E, E, C
2. E, C, C, E, C
3. E, E, C
4. E
5. E, C
6. C, E
7. E, E
8. C
9. E, C
10. C

Quarta Bateria de Questões Com Resolução Assistida

Criptografia Simétrica e Assimétrica

1. Acerca de criptografia e detecção de intrusão, julgue os itens subsequentes.

[116] Em uma mensagem criptografada por uma cifra de bloco, a alteração de qualquer bit da mensagem cifrada impede a sua correta decodificação, daquele ponto da mensagem em diante.

1. Acerca de criptografia e detecção de intrusão, julgue os itens subsequentes.

~~[116] Em uma mensagem criptografada por uma cifra de bloco, a alteração de qualquer bit da mensagem cifrada impede a sua correta decodificação, daquele ponto da mensagem em diante.~~

2. No que se refere à criptografia, julgue os itens a seguir

[77] Na cifra de Playfair, o algoritmo de criptografia utiliza m letras de texto claro sucessivas e as substitui por m letras de texto cifrado. Essa substituição é determinada por m equações lineares, em que cada caractere recebe um valor numérico (a = 0, b = 1, ... z = 50).

[78] A criptoanálise, baseada nas propriedades do algoritmo de criptografia, e a força bruta, que compreende a tentativa de quebra de todas as chaves possíveis, constituem tipos de ataque a um algoritmo de criptografia.

2. No que se refere à criptografia, julgue os itens a seguir

~~[77] Na cifra de Playfair, o algoritmo de criptografia utiliza m letras de texto claro sucessivas e as substitui por m letras de texto cifrado. Essa substituição é determinada por m equações lineares, em que cada caractere recebe um valor numérico (a = 0, b = 1, ... z = 50).~~

[78] A criptoanálise, baseada nas propriedades do algoritmo de criptografia, e a força bruta, que compreende a tentativa de quebra de todas as chaves possíveis, constituem tipos de ataque a um algoritmo de criptografia.

3. Em relação à criptografia, julgue os próximos itens.

[109] Uma chave criptográfica, utilizada para manter a confidencialidade de uma informação, é enviada ao destinatário para que ele possa visualizar a informação criptografada. A chave é a mesma para o remetente e para o destinatário. Esse tipo de criptografia é, portanto, considerado assimétrico.

[110] Para executar cópias de segurança de servidores de rede, é possível utilizar hash criptográfico a fim de validar a integridade de um ou mais arquivos.

[111] A assinatura digital permite atestar a autenticidade e a integridade de uma informação, quando apenas o proprietário da informação conhece a chave privada. Assim, a verificação da assinatura é feita por meio da chave privada.

3. Em relação à criptografia, julgue os próximos itens.

~~[109] Uma chave criptográfica, utilizada para manter a confidencialidade de uma informação, é enviada ao destinatário para que ele possa visualizar a informação criptografada. A chave é a mesma para o remetente e para o destinatário. Esse tipo de criptografia é, portanto, considerado assimétrico.~~

[110] Para executar cópias de segurança de servidores de rede, é possível utilizar hash criptográfico a fim de validar a integridade de um ou mais arquivos.

~~[111] A assinatura digital permite atestar a autenticidade e a integridade de uma informação, quando apenas o proprietário da informação conhece a chave privada. Assim, a verificação da assinatura é feita por meio da chave privada.~~

4. Com relação à certificação digital, julgue os itens que se seguem.

[117] Na criptografia de chave pública assimétrica, são utilizadas duas chaves diferentes: uma chave privada confidencial, para criptografar os dados, e outra chave pública, para decriptografar os dados, a qual é distribuída para os destinatários.

4. Com relação à certificação digital, julgue os itens que se seguem.

~~[117] Na criptografia de chave pública assimétrica, são utilizadas duas chaves diferentes: uma chave privada confidencial, para criptografar os dados, e outra chave pública, para decriptografar os dados, a qual é distribuída para os destinatários.~~

5. Julgue os próximos itens, relativos aos conceitos sobre criptografias, algoritmos simétricos e assimétricos de criptografia.

[101] O algoritmo RSA, baseado na construção de chaves públicas e privadas, utiliza números primos, e, quanto maior for o número primo escolhido, mais seguro será o algoritmo.

[102] A técnica utilizada para esconder uma mensagem secreta dentro de uma maior, de modo que não se possa discernir a presença ou o conteúdo da mensagem oculta é denominada estenografia.

[103] O DES (data encryption standard) triplo utiliza, exatamente, por três vezes o algoritmo DES, além de uma mesma chave de 56 bits para criptografar mensagens.

5. Julgue os próximos itens, relativos aos conceitos sobre criptografias, algoritmos simétricos e assimétricos de criptografia.

[101] O algoritmo RSA, baseado na construção de chaves públicas e privadas, utiliza números primos, e, quanto maior for o número primo escolhido, mais seguro será o algoritmo.

~~[102] A técnica utilizada para esconder uma mensagem secreta dentro de uma maior, de modo que não se possa discernir a presença ou o conteúdo da mensagem oculta é denominada estenografia.~~

~~[103] O DES (data encryption standard) triplo utiliza, exatamente, por três vezes o algoritmo DES, além de uma mesma chave de 56 bits para criptografar mensagens.~~

6. Julgue os itens que se seguem, relativos à criptografia simétrica e assimétrica.

[140] Na realização de cifra por blocos em criptografia simétrica, cada bloco de determinado tamanho deve ser cifrado separadamente, assim como o conjunto de operações matemáticas envolvendo a chave deve ser repetido a cada bloco. Para que esse processo de cifra possa ser considerado seguro, deve ser empregada uma chave de 12 bits em cada bloco.

[141] Em criptografia assimétrica, o tamanho da chave é um parâmetro secundário para a confidencialidade; o principal parâmetro consiste no emprego do algoritmo RSA, que é resistente a ataques do tipo MEN IN THE MIDDLE, e na confiança na autoridade certificadora

6. Julgue os itens que se seguem, relativos à criptografia simétrica e assimétrica.

~~[140] Na realização de cifra por blocos em criptografia simétrica, cada bloco de determinado tamanho deve ser cifrado separadamente, assim como o conjunto de operações matemáticas envolvendo a chave deve ser repetido a cada bloco. Para que esse processo de cifra possa ser considerado seguro, deve ser empregada uma chave de 12 bits em cada bloco.~~

~~[141] Em criptografia assimétrica, o tamanho da chave é um parâmetro secundário para a confidencialidade; o principal parâmetro consiste no emprego do algoritmo RSA, que é resistente a ataques do tipo MEN IN THE MIDDLE, e na confiança na autoridade certificadora~~

7. A respeito de sistemas de criptografia e tipos de criptografia utilizados em sistemas de segurança de rede, julgue os itens a seguir.

[68] A criptografia simétrica é específica para conexões de rede não monitoradas. Uma desvantagem dessa técnica de criptografia é o fato de que, por meio de um ataque de CBC (cypher block chaining), um atacante pode extrair dados legíveis de uma conexão de rede interceptada.

[69] Se um usuário A quiser enviar uma mensagem cifrada unicamente para um usuário B, sem que outros usuários sejam capazes de decifrá-la, um mecanismo de cifra adequado nesse caso envolverá o uso de criptografia de chave pública ou assimétrica.

[70] O algoritmo AES (advanced encryption standard) permite, entre outras funcionalidades, a utilização de cifras assimétricas durante o uso de uma sessão SSL/TLS

7. A respeito de sistemas de criptografia e tipos de criptografia utilizados em sistemas de segurança de rede, julgue os itens a seguir.

~~[68] A criptografia simétrica é específica para conexões de rede não monitoradas. Uma desvantagem dessa técnica de criptografia é o fato de que, por meio de um ataque de CBC (cypher block chaining), um atacante pode extrair dados legíveis de uma conexão de rede interceptada.~~

[69] Se um usuário A quiser enviar uma mensagem cifrada unicamente para um usuário B, sem que outros usuários sejam capazes de decifrá-la, um mecanismo de cifra adequado nesse caso envolverá o uso de criptografia de chave pública ou assimétrica.

~~[70] O algoritmo AES (advanced encryption standard) permite, entre outras funcionalidades, a utilização de cifras assimétricas durante o uso de uma sessão SSL/TLS~~

8. Com relação a criptografia, certificação digital e assinatura digital, julgue os itens subsequentes.

[69] Em criptografia simétrica, quando são usadas funções cypher block chaining, cada bloco cifrado depende dos blocos anteriormente cifrados.

8. Com relação a criptografia, certificação digital e assinatura digital, julgue os itens subsequentes.

[69] Em criptografia simétrica, quando são usadas funções cypher block chaining, cada bloco cifrado depende dos blocos anteriormente cifrados.

9. A respeito de criptografia, julgue os itens seguintes.

[66] Em um sistema assimétrico, garante-se a autenticidade da mensagem quando uma mensagem é cifrada duas vezes: primeiro, com a chave pública do autor e, depois, com a chave pública do destinatário.

[67] Nos sistemas simétricos, as partes compartilham uma chave secreta, utilizada tanto na cifração quanto na decifração.

[68] Uma assinatura digital consiste na cifração de um arquivo digital e do seu resumo criptográfico com uma chave privada.

[70] Se, em um sistema assimétrico, uma mensagem for cifrada duas vezes, primeiro com a chave privada do autor e, depois, com a chave pública do destinatário, garante-se que somente o destinatário conseguirá abrir a mensagem e que só o fará se dispuser da chave pública do autor.

9. A respeito de criptografia, julgue os itens seguintes.

~~[66] Em um sistema assimétrico, garante-se a autenticidade da mensagem quando uma mensagem é cifrada duas vezes: primeiro, com a chave pública do autor e, depois, com a chave pública do destinatário.~~

[67] Nos sistemas simétricos, as partes compartilham uma chave secreta, utilizada tanto na cifração quanto na decifração.

~~[68] Uma assinatura digital consiste na cifração de um arquivo digital e do seu resumo criptográfico com uma chave privada.~~

[70] Se, em um sistema assimétrico, uma mensagem for cifrada duas vezes, primeiro com a chave privada do autor e, depois, com a chave pública do destinatário, garante-se que somente o destinatário conseguirá abrir a mensagem e que só o fará se dispuser da chave pública do autor.

10. Com relação à criptografia e suas aplicações, julgue os itens.

[118] Alto nível de segurança das mensagens que trafegam em uma VPN é obtido pela cifração dessas mensagens, sem a necessidade de mecanismos de garantia de integridade.

[119] A criptografia simétrica difere da assimétrica por utilizar uma chave compartilhada entre as partes, que é usada tanto na cifração, quanto na decifração.

[121] Uma assinatura digital consiste na cifração do resumo criptográfico de um arquivo digital com uma chave pública.

10. Com relação à criptografia e suas aplicações, julgue os itens.

~~[118] Alto nível de segurança das mensagens que trafegam em uma VPN é obtido pela cifração dessas mensagens, sem a necessidade de mecanismos de garantia de integridade.~~

[119] A criptografia simétrica difere da assimétrica por utilizar uma chave compartilhada entre as partes, que é usada tanto na cifração, quanto na decifração.

~~[121] Uma assinatura digital consiste na cifração do resumo criptográfico de um arquivo digital com uma chave pública.~~

GABARITO

1. E
2. E, C
3. E, C, E
4. E
5. C, E, E
6. E, E
7. E, C, C
8. C
9. E, C, E, C
10. E, C, E

Quinta Bateria de Questões Com Resolução Assistida

Criptografia Simétrica e Assimétrica

1. Os Correios pretendem oferecer uma nova modalidade de prestação de serviços cuja contratação pode ser feita por qualquer cliente, via Internet. No momento da contratação, o cliente informa os seus dados pessoais e bancários, que serão enviados a um de dois bancos conveniados habilitados a efetuar o débito em sua conta corrente, no valor do contrato.

Considerando essa situação, julgue os itens subsequentes.

[105] A assinatura digital é suficiente para garantir o não repúdio e o sigilo dos dados que deverão transitar entre os computadores do cliente e o dos Correios.

[106] É possível ter a integridade dos dados transitados nas duas comunicações utilizando algoritmos simétricos.

[107] O uso do algoritmo criptográfico AES é suficiente para garantir o sigilo das informações enviadas pelos Correios aos bancos conveniados.

1. Os Correios pretendem oferecer uma nova modalidade de prestação de serviços cuja contratação pode ser feita por qualquer cliente, via Internet. No momento da contratação, o cliente informa os seus dados pessoais e bancários, que serão enviados a um de dois bancos conveniados habilitados a efetuar o débito em sua conta corrente, no valor do contrato.

Considerando essa situação, julgue os itens subsequentes.

~~[105] A assinatura digital é suficiente para garantir o não repúdio e o sigilo dos dados que deverão transitar entre os computadores do cliente e o dos Correios.~~

[106] É possível ter a integridade dos dados transitados nas duas comunicações utilizando algoritmos simétricos.

~~[107] O uso do algoritmo criptográfico AES é suficiente para garantir o sigilo das informações enviadas pelos Correios aos bancos conveniados.~~

2. Julgue os itens seguintes, a respeito de certificação digital e assinatura digital

[108] Para conferir a autenticidade de um certificado digital, é necessário utilizar o certificado digital da autoridade certificadora que o emitiu. Esse certificado pode ser emitido por outra autoridade certificadora ou pode ser autoassinado.

[109] Para assinar digitalmente um documento eletrônico, um usuário deve utilizar a chave que consta no seu certificado digital.

2. Julgue os itens seguintes, a respeito de certificação digital e assinatura digital

[108] Para conferir a autenticidade de um certificado digital, é necessário utilizar o certificado digital da autoridade certificadora que o emitiu. Esse certificado pode ser emitido por outra autoridade certificadora ou pode ser autoassinado.

[109] Para assinar digitalmente um documento eletrônico, um usuário deve utilizar a chave que consta no seu certificado digital.

3. Com relação aos sistemas de criptografia, assinale a opção correta.

A. MD5 é um algoritmo de criptografia utilizado para a verificação de integridade de arquivos que são obtidos na Internet por meio de download.

B. DES é embasado no tempo necessário para que uma chave secreta seja descoberta, em função do comprimento da chave, por isso, além de ser inviolável, é um dos algoritmos de criptografia mais confiáveis.

C. SHA é um algoritmo que gera um resumo de mensagem que varia de tamanho em função do tamanho da própria mensagem.

D. O algoritmo AES, uma variação do DES, utiliza o conceito de chaves simétricas.

E. As aplicações de chave pública não permitem autenticação de usuários, pois são destinadas para uso apenas de órgãos do governo

3. Com relação aos sistemas de criptografia, assinale a opção correta.

A. MD5 é um algoritmo de criptografia utilizado para a verificação de integridade de arquivos que são obtidos na Internet por meio de download.

B. DES é embasado no tempo necessário para que uma chave secreta seja descoberta, em função do comprimento da chave, por isso, além de ser inviolável, é um dos algoritmos de criptografia mais confiáveis.

C. SHA é um algoritmo que gera um resumo de mensagem que varia de tamanho em função do tamanho da própria mensagem.

D. O algoritmo AES, uma variação do DES, utiliza o conceito de chaves simétricas.

E. As aplicações de chave pública não permitem autenticação de usuários, pois são destinadas para uso apenas de órgãos do governo

4. A respeito de criptografia simétrica e assimétrica, assinale a opção correta.

A. Simetria de chaves significa que as partes têm a mesma chave para cifrar e decifrar uma mensagem.

B. A ciência da criptografia se divide em duas grandes vertentes: a criptografia de chave privada ou assimétrica e a criptografia de chave pública ou simétrica.

C. O sistema criptográfico DES opera com um bloco de 64 bits, em que, a cada 8 bits, se agrega um bit de paridade, razão por que, na prática, a chave tem somente 56 bits.

D. Privacidade e integridade são as únicas questões de segurança que requerem o uso de criptografia.

E. Classifica-se a criptografia de chave simétrica em duas famílias: criptografia simétrica de blocos (block cipher) e criptografia simétrica de via (stream cipher).

4. A respeito de criptografia simétrica e assimétrica, assinale a opção correta.

A. Simetria de chaves significa que as partes têm a mesma chave para cifrar e decifrar uma mensagem.

B. A ciência da criptografia se divide em duas grandes vertentes: a criptografia de chave privada ou assimétrica e a criptografia de chave pública ou simétrica.

C. O sistema criptográfico DES opera com um bloco de 64 bits, em que, a cada 8 bits, se agrega um bit de paridade, razão por que, na prática, a chave tem somente 56 bits.

D. Privacidade e integridade são as únicas questões de segurança que requerem o uso de criptografia.

E. Classifica-se a criptografia de chave simétrica em duas famílias: criptografia simétrica de blocos (block cipher) e criptografia simétrica de via (stream cipher).

5. Com relação aos sistemas criptográficos, assinale a opção correta.

A. Com os sistemas simétricos, consegue-se obter confidencialidade, integridade e disponibilidade.

B. Com os sistemas assimétricos, consegue-se obter confidencialidade, integridade, autenticidade e não repúdio.

C. O sistema RSA, com ou sem curvas elípticas, tem por base o problema do logaritmo discreto.

D. AES e 3DES são cifras simétricas que têm por base a malha de Feistel.

E. O 3DES consiste de três rodadas consecutivas do DES em que a mesma chave de 64 bits é usada.

5. Com relação aos sistemas criptográficos, assinale a opção correta.

A. Com os sistemas simétricos, consegue-se obter confidencialidade, integridade e disponibilidade.

B. Com os sistemas assimétricos, consegue-se obter confidencialidade, integridade, autenticidade e não repúdio.

C. O sistema RSA, com ou sem curvas elípticas, tem por base o problema do logaritmo discreto.

D. AES e 3DES são cifras simétricas que têm por base a malha de Feistel.

E. O 3DES consiste de três rodadas consecutivas do DES em que a mesma chave de 64 bits é usada.

6. Acerca de segurança da informação e criptografia, julgue os itens seguintes

[96] A técnica de segurança de informação denominada assinatura digital permite ao receptor verificar a integridade da mensagem e a identidade do transmissor.

[97] A adição de uma assinatura digital a uma mensagem pode ser efetuada pelo seu transmissor, por meio da adição, à mensagem cifrada, de um hash (da mensagem original em claro) cifrado com sua chave privada.

[98] A distribuição de chaves é mais simples e segura na utilização de um sistema criptográfico simétrico ou de chave secreta que na utilização de um sistema criptográfico assimétrico ou de chave pública.

[99] Sistemas criptográficos assimétricos ou de chave pública oferecem melhor desempenho na cifração e decifração de mensagens que sistemas criptográficos simétricos.

[100] Considerando-se que, em um sistema de criptografia assimétrico - ou de chave pública -, um usuário A deseje enviar, de forma segura, uma mensagem a um usuário B, é correto afirmar que o usuário A deverá cifrar a mensagem com sua chave privada e o usuário B, ao receber a mensagem, deverá decifrá-la com a chave pública de A.

6. Acerca de segurança da informação e criptografia, julgue os itens seguintes

[96] A técnica de segurança de informação denominada assinatura digital permite ao receptor verificar a integridade da mensagem e a identidade do transmissor.

[97] A adição de uma assinatura digital a uma mensagem pode ser efetuada pelo seu transmissor, por meio da adição, à mensagem cifrada, de um hash (da mensagem original em claro) cifrado com sua chave privada.

~~[98] A distribuição de chaves é mais simples e segura na utilização de um sistema criptográfico simétrico ou de chave secreta que na utilização de um sistema criptográfico assimétrico ou de chave pública.~~

~~[99] Sistemas criptográficos assimétricos ou de chave pública oferecem melhor desempenho na cifração e decifração de mensagens que sistemas criptográficos simétricos.~~

~~[100] Considerando-se que, em um sistema de criptografia assimétrico - ou de chave pública -, um usuário A deseje enviar, de forma segura, uma mensagem a um usuário B, é correto afirmar que o usuário A deverá cifrar a mensagem com sua chave privada e o usuário B, ao receber a mensagem, deverá decifrá-la com a chave pública de A.~~

7. A respeito do estabelecimento de um sistema de gestão da segurança, julgue os itens seguintes.

[106] Uma das desvantagens decorrentes do uso de mecanismos de criptografia assimétricos, relativamente à criptografia simétrica, consiste no aumento do custo computacional para produzir uma mensagem cifrada com igual resistência a ataques.

7. A respeito do estabelecimento de um sistema de gestão da segurança, julgue os itens seguintes.

[106] Uma das desvantagens decorrentes do uso de mecanismos de criptografia assimétricos, relativamente à criptografia simétrica, consiste no aumento do custo computacional para produzir uma mensagem cifrada com igual resistência a ataques.

8. Com relação a sistemas criptográficos, assinaturas e certificados digitais, julgue os itens subsecutivos

[107] AES é uma cifra de bloco simétrica, com blocos de 128 bits e chaves de 128, 192 e 256 bits, e RSA é um sistema assimétrico que tem por base a fatoração de grandes números inteiros.

[109] Uma assinatura digital confere autenticidade, integridade e sigilo a uma mensagem.

[110] Os sistemas assimétricos usam duas chaves com funções complementares: se uma é usada para cifração, a outra é usada na decifração; além disso, uma delas deve ser mantida secreta, enquanto a outra pode ser pública.

8. Com relação a sistemas criptográficos, assinaturas e certificados digitais, julgue os itens subsecutivos

[107] AES é uma cifra de bloco simétrica, com blocos de 128 bits e chaves de 128, 192 e 256 bits, e RSA é um sistema assimétrico que tem por base a fatoração de grandes números inteiros.

~~[109] Uma assinatura digital confere autenticidade, integridade e sigilo a uma mensagem.~~

[110] Os sistemas assimétricos usam duas chaves com funções complementares: se uma é usada para cifração, a outra é usada na decifração; além disso, uma delas deve ser mantida secreta, enquanto a outra pode ser pública.

9. No que se refere à criptografia, assinale a opção correta.

A. Nos sistemas simétricos, os modos de operação ECB e CBC são seguros.

B. O esforço computacional necessário para cifração e decifração é idêntico para sistemas simétricos e assimétricos.

C. Confidencialidade e integridade são obtidas apenas nos sistemas assimétricos.

D. Autenticidade e não repúdio são obtidos nos sistemas simétricos.

E. Nos sistemas assimétricos, cada usuário utiliza duas chaves: uma que deve ser mantida secreta e a outra que é pública.

9. No que se refere à criptografia, assinale a opção correta.

A. Nos sistemas simétricos, os modos de operação ECB e CBC são seguros.

B. O esforço computacional necessário para cifração e decifração é idêntico para sistemas simétricos e assimétricos.

C. Confidencialidade e integridade são obtidas apenas nos sistemas assimétricos.

D. Autenticidade e não repúdio são obtidos nos sistemas simétricos.

E. Nos sistemas assimétricos, cada usuário utiliza duas chaves: uma que deve ser mantida secreta e a outra que é pública.

10. A assinatura digital consiste na cifração

A. do resumo criptográfico da mensagem (hash) com a chave pública do autor.

B. da mensagem com a chave privada do autor.

C. do resumo criptográfico da mensagem (hash) com a chave privada do autor.

D. da mensagem com a chave pública do autor.

E. da mensagem e do seu resumo criptográfico (hash) com a chave pública do autor.

10. A assinatura digital consiste na cifração

A. do resumo criptográfico da mensagem (hash) com a chave pública do autor.

B. da mensagem com a chave privada do autor.

C. do resumo criptográfico da mensagem (hash) com a chave privada do autor.

D. da mensagem com a chave pública do autor.

E. da mensagem e do seu resumo criptográfico (hash) com a chave pública do autor.

GABARITO

1. E, C, E
2. C, E
3. A
4. A
5. B
6. C, C, E, E, E
7. C
8. C, E, C
9. E
10. C

Sexta Bateria de Questões Com Resolução Assistida

Criptografia Simétrica e Assimétrica

1. Com relação à assinatura e certificação digitais, é correto afirmar que

A. uma assinatura digital confere apenas autenticidade a uma mensagem.

B. uma assinatura digital, que é apensa a uma mensagem, consiste na cifração do seu hash usando a chave pública do autor.

C. se uma mensagem é cifrada duas vezes seguidas, usando a chave privada do remetente na primeira e a pública do destinatário na segunda, garante-se que a mensagem de fato partiu do remetente e que só será aberta pelo destinatário.

D. se uma mensagem é cifrada duas vezes seguidas, usando a chave pública do destinatário na primeira e a pública do remetente na segunda, garante-se que a mensagem de fato partiu do remetente e que só será aberta pelo destinatário.

E. se uma mensagem é cifrada duas vezes seguidas, usando a chave pública do remetente na primeira e a pública do destinatário na segunda, garante-se que a mensagem de fato partiu do remetente e que só será aberta pelo destinatário.

1. Com relação à assinatura e certificação digitais, é correto afirmar que

A. uma assinatura digital confere apenas autenticidade a uma mensagem.

B. uma assinatura digital, que é apensa a uma mensagem, consiste na cifração do seu hash usando a chave pública do autor.

C. se uma mensagem é cifrada duas vezes seguidas, usando a chave privada do remetente na primeira e a pública do destinatário na segunda, garante-se que a mensagem de fato partiu do remetente e que só será aberta pelo destinatário.

D. se uma mensagem é cifrada duas vezes seguidas, usando a chave pública do destinatário na primeira e a pública do remetente na segunda, garante-se que a mensagem de fato partiu do remetente e que só será aberta pelo destinatário.

E. se uma mensagem é cifrada duas vezes seguidas, usando a chave pública do remetente na primeira e a pública do destinatário na segunda, garante-se que a mensagem de fato partiu do remetente e que só será aberta pelo destinatário.

2. Julgue os itens que se seguem, relativos a sistemas de criptografia e suas aplicações.

[106] O algoritmo de criptografia RSA (Rivest, Shamir e Adleman) é embasado no conceito de chave simétrica.

[107] Um algoritmo de criptografia eficiente impede que uma mensagem que trafega em uma rede de comunicação seja decodificada ou apagada por intrusos.

2. Julgue os itens que se seguem, relativos a sistemas de criptografia e suas aplicações.

~~[106] O algoritmo de criptografia RSA (Rivest, Shamir e Adleman) é embasado no conceito de chave simétrica.~~

~~[107] Um algoritmo de criptografia eficiente impede que uma mensagem que trafega em uma rede de comunicação seja decodificada ou apagada por intrusos.~~

3. Julgue os próximos itens, relativos a vulnerabilidades e ataques a sistemas computacionais, bem como à proteção oferecida pela criptografia para a segurança da informação

[111] As técnicas usadas para verificar a integridade de dados contra dano acidental, tais como os checksums, podem por si só ser usadas para garantir a integridade dos dados contra mudanças intencionais.

[112] O esquema de criptografia data encryption standard (DES) duplo é vulnerável a ataque do tipo meet-in-the-middle (encontro no meio).

[113] Em criptossistemas de chave pública, o algoritmo de Rivest, Shamir e Adleman (RSA) é adequado para a implementação de criptografia/decriptografia, assinatura digital e troca de chave.

[114] Considere que João criptografe uma mensagem com a chave pública de Pedro. Nessa situação hipotética, a mensagem não poderá ser facilmente decriptografada por terceiros sem a chave privada de Pedro; uma mensagem criptografada com a chave privada de Pedro não poderia, da mesma forma, ser decriptografada facilmente por João sem a chave pública de Pedro.

3. Julgue os próximos itens, relativos a vulnerabilidades e ataques a sistemas computacionais, bem como à proteção oferecida pela criptografia para a segurança da informação

~~[111] As técnicas usadas para verificar a integridade de dados contra dano acidental, tais como os checksums, podem por si só ser usadas para garantir a integridade dos dados contra mudanças intencionais.~~

[112] O esquema de criptografia data encryption standard (DES) duplo é vulnerável a ataque do tipo meet-in-the-middle (encontro no meio).

[113] Em criptossistemas de chave pública, o algoritmo de Rivest, Shamir e Adleman (RSA) é adequado para a implementação de criptografia/decriptografia, assinatura digital e troca de chave.

[114] Considere que João criptografe uma mensagem com a chave pública de Pedro. Nessa situação hipotética, a mensagem não poderá ser facilmente decriptografada por terceiros sem a chave privada de Pedro; uma mensagem criptografada com a chave privada de Pedro não poderia, da mesma forma, ser decriptografada facilmente por João sem a chave pública de Pedro.

4. Considere que, em determinada empresa, o funcionário Haroldo precise passar informações confidenciais para o seu chefe, Júlio. Para maior segurança, os dados são transmitidos criptografados pela rede da empresa. Rogério, outro funcionário da empresa, está tentando indevidamente interceptar as informações trocadas entre Haroldo e Júlio. Com base nessa situação hipotética, julgue os itens, acerca de configurações e do emprego dos sistemas de criptografia.

[87] Considere que Haroldo e Júlio se comuniquem utilizando um sistema de criptografia de chave pública, sem assinatura digital. Nesse caso, se Rogério, passando-se por Haroldo, enviar uma mensagem criptografada para Júlio, este pode não ter como saber que a mensagem não foi enviada por Haroldo.

[88] Mesmo que Haroldo e Júlio coloquem normalmente os seus nomes no corpo das mensagens trocadas entre eles, esse procedimento não facilita o deciframento não autorizado das mensagens, já que os dados são criptografados.

[89] Caso Haroldo utilize assinatura digital em suas mensagens, Júlio pode comprovar se uma mensagem supostamente enviada por Haroldo partiu realmente dele. Além disso, caso Haroldo resolva negar que tenha enviado dada mensagem, tendo ele efetivamente a enviado, Júlio pode provar que a mensagem é de fato de Haroldo.

4. Considere que, em determinada empresa, o funcionário Haroldo precise passar informações confidenciais para o seu chefe, Júlio. Para maior segurança, os dados são transmitidos criptografados pela rede da empresa. Rogério, outro funcionário da empresa, está tentando indevidamente interceptar as informações trocadas entre Haroldo e Júlio. Com base nessa situação hipotética, julgue os itens, acerca de configurações e do emprego dos sistemas de criptografia.

[87] Considere que Haroldo e Júlio se comuniquem utilizando um sistema de criptografia de chave pública, sem assinatura digital. Nesse caso, se Rogério, passando-se por Haroldo, enviar uma mensagem criptografada para Júlio, este pode não ter como saber que a mensagem não foi enviada por Haroldo.

~~[88] Mesmo que Haroldo e Júlio coloquem normalmente os seus nomes no corpo das mensagens trocadas entre eles, esse procedimento não facilita o deciframento não autorizado das mensagens, já que os dados são criptografados.~~

[89] Caso Haroldo utilize assinatura digital em suas mensagens, Júlio pode comprovar se uma mensagem supostamente enviada por Haroldo partiu realmente dele. Além disso, caso Haroldo resolva negar que tenha enviado dada mensagem, tendo ele efetivamente a enviado, Júlio pode provar que a mensagem é de fato de Haroldo.

5. Julgue os próximos itens, relativos à segurança da informação.

[140] Em processos de autenticação de mensagens, um digest MDC (modification detection code) utiliza uma função hash sem chaves. Se for assinado, o digest permite verificar a integridade de mensagem, além de sua autenticação, e não repúdio.

[141] Em sistemas criptográficos de chave pública, curva elíptica consiste na implementação de algoritmos de chave pública já existentes que proveem sistemas criptográficos com chaves de maior tamanho que os algoritmos de chaves simétricas.

[142] Para que o conteúdo de uma mensagem criptografada seja decifrado apenas pelo seu verdadeiro destinatário, é necessário que ela seja assinada digitalmente.

5. Julgue os próximos itens, relativos à segurança da informação.

[140] Em processos de autenticação de mensagens, um digest MDC (modification detection code) utiliza uma função hash sem chaves. Se for assinado, o digest permite verificar a integridade de mensagem, além de sua autenticação, e não repúdio.

~~[141] Em sistemas criptográficos de chave pública, curva elíptica consiste na implementação de algoritmos de chave pública já existentes que proveem sistemas criptográficos com chaves de maior tamanho que os algoritmos de chaves simétricas.~~

~~[142] Para que o conteúdo de uma mensagem criptografada seja decifrado apenas pelo seu verdadeiro destinatário, é necessário que ela seja assinada digitalmente.~~

GABARITO

1.C

2.E, E

3.E, C, C, C

4.C, E, C

5.C, E, E

Sétima Bateria de Questões Com Resolução Assistida

Criptografia Simétrica e Assimétrica

1. Com relação à segurança da informação, julgue os itens seguintes.

[139] Assumindo que as assinaturas não possam ser forjadas, os esquemas de criptografia de chaves públicas permitem que mensagens criptografadas sejam assinadas de tal modo que o recipiente possa ter certeza de que a mensagem originou-se com a pessoa que alega tê-la feito.

[140] Abordagens básicas de criptografia de dados incluem a substituição e a permutação. A substituição ocorre na situação em que, para cada caractere de um texto simples, verifica-se a substituição desse caractere por um outro texto cifrado. A permutação ocorre quando caracteres de texto simples são reformulados em alguma sequência diferente da original.

[141] Considere a situação na qual os usuários camuflam-se como o próprio SGBD, por exemplo, removendo fisicamente parte do banco de dados, grampeando uma linha de comunicação e processando um programa que atravesse as defesas do sistema operacional. Nessa situação, estão caracterizadas ameaças de segurança que podem ser eficazmente combatidas com criptografia de dados.

1. Com relação à segurança da informação, julgue os itens seguintes.

[139] Assumindo que as assinaturas não possam ser forjadas, os esquemas de criptografia de chaves públicas permitem que mensagens criptografadas sejam assinadas de tal modo que o recipiente possa ter certeza de que a mensagem originou-se com a pessoa que alega tê-la feito.

[140] Abordagens básicas de criptografia de dados incluem a substituição e a permutação. A substituição ocorre na situação em que, para cada caractere de um texto simples, verifica-se a substituição desse caractere por um outro texto cifrado. A permutação ocorre quando caracteres de texto simples são reformulados em alguma sequência diferente da original.

[141] Considere a situação na qual os usuários camuflam-se como o próprio SGBD, por exemplo, removendo fisicamente parte do banco de dados, grampeando uma linha de comunicação e processando um programa que atravesse as defesas do sistema operacional. Nessa situação, estão caracterizadas ameaças de segurança que podem ser eficazmente combatidas com criptografia de dados.

2. Acerca de protocolos e algoritmos de criptografia e certificação digital, julgue os itens a seguir.

[104] Protocolos de criptografia simétrica usados em redes abertas só possuem expectativa de uso eficiente e eficaz se forem combinados com um protocolo de gerenciamento de chaves como o IKE (Internet key exchange).

2. Acerca de protocolos e algoritmos de criptografia e certificação digital, julgue os itens a seguir.

[104] Protocolos de criptografia simétrica usados em redes abertas só possuem expectativa de uso eficiente e eficaz se forem combinados com um protocolo de gerenciamento de chaves como o IKE (Internet key exchange).

3. Com relação à segurança de redes, julgue os itens que se seguem.

[102] É possível atingir confidencialidade e integridade com o uso de sistemas criptográficos simétricos.

[103] É possível obter autenticação e não repúdio, além de confidencialidade e integridade, por meio dos sistemas criptográficos assimétricos.

3. Com relação à segurança de redes, julgue os itens que se seguem.

[102] É possível atingir confidencialidade e integridade com o uso de sistemas criptográficos simétricos.

[103] É possível obter autenticação e não repúdio, além de confidencialidade e integridade, por meio dos sistemas criptográficos assimétricos.

4. Acerca dos sistemas criptográficos, julgue os itens.

[106] Enquanto uma cifra de bloco atua em um bit ou byte do fluxo de dados por vez, uma cifra de fluxo atua sobre um conjunto de caracteres de texto em claro, que são tratados como um todo e usados para produzir um criptograma de igual comprimento.

[107] Nos sistemas simétricos, os usuários usam a mesma chave para cifrar e decifrar mensagens, enquanto nos sistemas assimétricos mais de uma chave é usada.

[108] Em um sistema de chaves assimétricas, cada usuário tem um par de chaves, sendo que uma delas é mantida secreta e a outra é pública.

[109] Nos sistemas assimétricos, as chaves são escolhidas de forma que se uma mensagem é cifrada usando uma das chaves, o criptograma correspondente é decifrado utilizando a outra chave do par.

4. Acerca dos sistemas criptográficos, julgue os itens.

~~[106] Enquanto uma cifra de bloco atua em um bit ou byte do fluxo de dados por vez, uma cifra de fluxo atua sobre um conjunto de caracteres de texto em claro, que são tratados como um todo e usados para produzir um criptograma de igual comprimento.~~

[107] Nos sistemas simétricos, os usuários usam a mesma chave para cifrar e decifrar mensagens, enquanto nos sistemas assimétricos mais de uma chave é usada.

[108] Em um sistema de chaves assimétricas, cada usuário tem um par de chaves, sendo que uma delas é mantida secreta e a outra é pública.

[109] Nos sistemas assimétricos, as chaves são escolhidas de forma que se uma mensagem é cifrada usando uma das chaves, o criptograma correspondente é decifrado utilizando a outra chave do par.

5. Com relação às cifras criptográficas, julgue os itens seguintes.

[110] O padrão DES, que utiliza chave de 64 bits, não é mais recomendado, considerando a sua vulnerabilidade a ataques de força bruta.

[111] O padrão 2DES consiste em duas rodadas consecutivas do DES, com duas chaves distintas de 56 bits, tendo assim uma chave equivalente a 112 bits.

[112] O padrão 3DES com duas chaves consiste em três rodadas consecutivas do DES, com chaves distintas de 56 bits, sendo que a primeira e a última usam a mesma chave, tendo assim uma chave equivalente a 112 bits.

[113] O padrão AES define uma cifra na qual os comprimentos do bloco e da chave podem ser especificados independentemente para 128 bits, 192 bits ou 256 bits. Os três tamanhos de chave determinam vários parâmetros da cifra, como número de rodadas, e podem ser usados limitando o bloco a 128 bits

5. Com relação às cifras criptográficas, julgue os itens seguintes.

~~[110] O padrão DES, que utiliza chave de 64 bits, não é mais recomendado, considerando a sua vulnerabilidade a ataques de força bruta.~~

~~[111] O padrão 2DES consiste em duas rodadas consecutivas do DES, com duas chaves distintas de 56 bits, tendo assim uma chave equivalente a 112 bits.~~

[112] O padrão 3DES com duas chaves consiste em três rodadas consecutivas do DES, com chaves distintas de 56 bits, sendo que a primeira e a última usam a mesma chave, tendo assim uma chave equivalente a 112 bits.

[113] O padrão AES define uma cifra na qual os comprimentos do bloco e da chave podem ser especificados independentemente para 128 bits, 192 bits ou 256 bits. Os três tamanhos de chave determinam vários parâmetros da cifra, como número de rodadas, e podem ser usados limitando o bloco a 128 bits

GABARITO

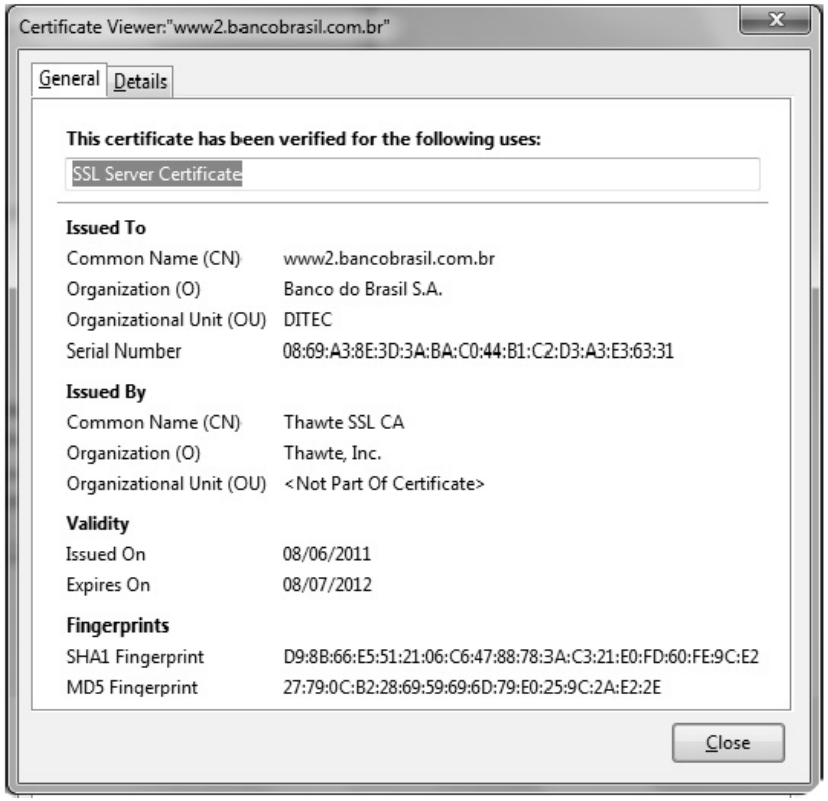
1. C, C, C
2. C
3. C, C
4. E, C, C, C
5. E, E, C, C

Oitava Bateria de Questões Com Resolução Assistida

Criptografia – Certificação Digital

1. Julgue os próximos itens, relativos à criptografia.

A figura acima ilustra o certificado digital de Internet banking do sítio do Banco do Brasil. Considerando esse certificado, julgue os itens a seguir.



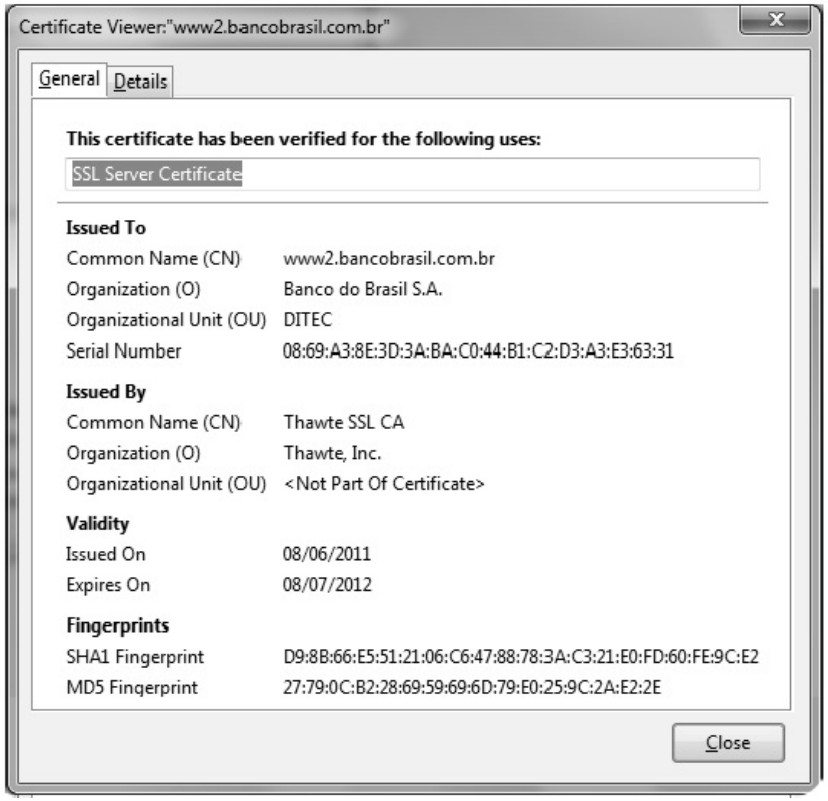
[80] Os campos CN, O, OU são comuns em certificados digitais. Além desses campos, outros campos adicionais podem ser utilizados, desde que sejam observadas as devidas restrições de uso dos campos.

[81] A assinatura digital produzida mediante o uso do algoritmo MD5 gera uma saída de 16 bytes.

[82] Assinaturas SHA1 para certificados de 1.024 bits terminam com a sequência hexadecimal 9C:E2. Portanto, a chave pública do certificado mostrado na figura é de 1.024 bits.

1. Julgue os próximos itens, relativos à criptografia.

A figura acima ilustra o certificado digital de Internet banking do sítio do Banco do Brasil. Considerando esse certificado, julgue os itens a seguir.



[80] Os campos CN, O, OU são comuns em certificados digitais. Além desses campos, outros campos adicionais podem ser utilizados, desde que sejam observadas as devidas restrições de uso dos campos.

[81] A assinatura digital produzida mediante o uso do algoritmo MD5 gera uma saída de 16 bytes.

~~[82] Assinaturas SHA1 para certificados de 1.024 bits terminam com a sequência hexadecimal 9C:E2. Portanto, a chave pública do certificado mostrado na figura é de 1.024 bits.~~

2. Com relação a criptografia, certificação digital e assinatura digital, julgue os itens subsequentes.

[70] Um certificado digital possui, além da chave pública do proprietário do certificado, a assinatura digital da autoridade certificadora que o assinou.

2. Com relação a criptografia, certificação digital e assinatura digital, julgue os itens subsequentes.

[70] Um certificado digital possui, além da chave pública do proprietário do certificado, a assinatura digital da autoridade certificadora que o assinou.

3. A respeito de criptografia, julgue os itens seguintes.

[69] Um certificado digital consiste na cifração do resumo criptográfico de uma chave privada com a chave pública de uma autoridade certificadora.

3. A respeito de criptografia, julgue os itens seguintes.

~~[69] Um certificado digital consiste na cifração do resumo criptográfico de uma chave privada com a chave pública de uma autoridade certificadora.~~

4. Com relação à criptografia e suas aplicações, julgue os itens.

[122] Um certificado digital consiste na cifração do resumo criptográfico de uma chave pública com a chave privada de uma autoridade certificadora.

4. Com relação à criptografia e suas aplicações, julgue os itens.

[122] Um certificado digital consiste na cifração do resumo criptográfico de uma chave pública com a chave privada de uma autoridade certificadora.

5. Com relação a certificação digital e infraestrutura de chaves públicas, julgue os itens que se seguem

[102] A Infraestrutura de Chave Pública Brasil (ICP-Brasil) emite certificados, autentica-os e possui uma autoridade certificadora que faz manutenção dos certificados durante o ciclo de vida destes, apesar de não ser uma entidade reconhecida pela legislação brasileira.

5. Com relação a certificação digital e infraestrutura de chaves públicas, julgue os itens que se seguem

~~[102] A Infraestrutura de Chave Pública Brasil (ICP-Brasil) emite certificados, autentica-os e possui uma autoridade certificadora que faz manutenção dos certificados durante o ciclo de vida destes, apesar de não ser uma entidade reconhecida pela legislação brasileira.~~

6. A respeito de certificação digital, assinale a opção correta.

A. A lista de certificados revogados, mantida pelas autoridades de registro, contém o histórico de quantas vezes um certificado foi renovado e a informação quanto à sua validade ou não.

B. A ICP-Brasil é uma entidade máxima da infraestrutura que emite certificados aos usuários do governo e também para organizações que prestam serviço para a União.

C. Para exercerem a função de emissoras de certificado, as autoridades certificadoras não precisam estar vinculadas à ICPBrasil.

D. Ao se assinar uma mensagem com uma assinatura digital, pode-se utilizar uma chave pública para o envio e usar uma chave privada para o recebimento da mensagem.

E. A assinatura digital tem como finalidade principal a garantia da integridade e da origem da mensagem.

6. A respeito de certificação digital, assinale a opção correta.

A. A lista de certificados revogados, mantida pelas autoridades de registro, contém o histórico de quantas vezes um certificado foi renovado e a informação quanto à sua validade ou não.

B. A ICP-Brasil é uma entidade máxima da infraestrutura que emite certificados aos usuários do governo e também para organizações que prestam serviço para a União.

C. Para exercerem a função de emissoras de certificado, as autoridades certificadoras não precisam estar vinculadas à ICPBrasil.

D. Ao se assinar uma mensagem com uma assinatura digital, pode-se utilizar uma chave pública para o envio e usar uma chave privada para o recebimento da mensagem.

E. A assinatura digital tem como finalidade principal a garantia da integridade e da origem da mensagem.

7. Considere que, em determinada empresa, o funcionário Haroldo precise passar informações confidenciais para o seu chefe, Júlio. Para maior segurança, os dados são transmitidos criptografados pela rede da empresa. Rogério, outro funcionário da empresa, está tentando indevidamente interceptar as informações trocadas entre Haroldo e Júlio. Com base nessa situação hipotética, julgue os itens, acerca de configurações e do emprego dos sistemas de criptografia.

[90] Caso Júlio tenha obtido um certificado digital de uma autoridade certificadora, ele deve proteger esse certificado e mantê-lo em sigilo.

7. Considere que, em determinada empresa, o funcionário Haroldo precise passar informações confidenciais para o seu chefe, Júlio. Para maior segurança, os dados são transmitidos criptografados pela rede da empresa. Rogério, outro funcionário da empresa, está tentando indevidamente interceptar as informações trocadas entre Haroldo e Júlio. Com base nessa situação hipotética, julgue os itens, acerca de configurações e do emprego dos sistemas de criptografia.

~~[90] Caso Júlio tenha obtido um certificado digital de uma autoridade certificadora, ele deve proteger esse certificado e mantê-lo em sigilo.~~

8. Acerca de protocolos e algoritmos de criptografia e certificação digital, julgue os itens a seguir.

[105] Constituem elementos dos sistemas de assinatura e certificação digital em uso atual na Internet e web: capacidade de instalação de novos certificados digitais nos browsers, aderentes ao formato X.509; uso de protocolos de hash criptográfico que sejam resilientes a ataques de dicionário; e uso combinado de criptografia assimétrica e simétrica.

8. Acerca de protocolos e algoritmos de criptografia e certificação digital, julgue os itens a seguir.

[105] Constituem elementos dos sistemas de assinatura e certificação digital em uso atual na Internet e web: capacidade de instalação de novos certificados digitais nos browsers, aderentes ao formato X.509; uso de protocolos de hash criptográfico que sejam resilientes a ataques de dicionário; e uso combinado de criptografia assimétrica e simétrica.

9. Com relação à segurança de redes, julgue os itens que se seguem.

[105] Um certificado digital é a assinatura digital de uma chave pública, cifrada com a chave pública da autoridade certificadora.

9. Com relação à segurança de redes, julgue os itens que se seguem.

[105] Um certificado digital é a assinatura digital de uma chave pública, cifrada com a chave pública da autoridade certificadora.

1O. Com relação à segurança de redes, julgue os itens que se seguem.

[116] Um certificado digital é a chave pública de um usuário assinada por uma autoridade certificadora confiável.

1O. Com relação à segurança de redes, julgue os itens que se seguem.

[116] Um certificado digital é a chave pública de um usuário assinada por uma autoridade certificadora confiável.

GABARITO

1. C, C, E
2. C
3. E
4. C
5. E
6. E
7. E
8. C
9. E
10. C

Nona Bateria de Questões
Com Resolução Assistida

Criptografia – Certificação Digital

1. Julgue os próximos itens, relativos à criptografia.

[119] Na verificação de uma assinatura digital de uma mensagem, a primeira é decifrada com a chave pública do remetente e comparada ao resumo criptográfico da segunda.

1. Julgue os próximos itens, relativos à criptografia.

[119] Na verificação de uma assinatura digital de uma mensagem, a primeira é decifrada com a chave pública do remetente e comparada ao resumo criptográfico da segunda.

2. Uma empresa cuja matriz está localizada em Brasília possui três filiais localizadas em outras cidades do Brasil. As atribuições da matriz incluem analisar todas as propostas de negócio e autorizar os valores finais da negociação, além de analisar a documentação dos clientes para a liberação do crédito. Como atende a clientes em cidades onde não possui pontos de atendimento, a empresa recebe as propostas e documentos dos clientes eletronicamente e fecha contratos à distância. Os clientes também podem ser atendidos nas filiais, caso em que elas se responsabilizam pela recepção dos documentos e pelo seu envio, por meio eletrônico, para a matriz.

Com base nessa situação hipotética, julgue os seguintes itens.

[81] O uso de certificados autoassinados para assinar eletronicamente os documentos digitais enviados pelos clientes às filiais é suficiente para garantir a autoria do envio desses documentos

2. Uma empresa cuja matriz está localizada em Brasília possui três filiais localizadas em outras cidades do Brasil. As atribuições da matriz incluem analisar todas as propostas de negócio e autorizar os valores finais da negociação, além de analisar a documentação dos clientes para a liberação do crédito. Como atende a clientes em cidades onde não possui pontos de atendimento, a empresa recebe as propostas e documentos dos clientes eletronicamente e fecha contratos à distância. Os clientes também podem ser atendidos nas filiais, caso em que elas se responsabilizam pela recepção dos documentos e pelo seu envio, por meio eletrônico, para a matriz.

Com base nessa situação hipotética, julgue os seguintes itens.

~~[81] O uso de certificados autoassinados para assinar eletronicamente os documentos digitais enviados pelos clientes às filiais é suficiente para garantir a autoria do envio desses documentos~~

3. A Autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz) é a primeira autoridade da cadeia de certificação. No que se refere à ICP-Brasil, julgue os itens subsequentes.

[95] A emissão da lista de certificados revogados (LCR) é responsabilidade da AC-Raiz da ICP-Brasil.

[96] O comitê gestor da ICP-Brasil verifica se as autoridades certificadoras atuam em conformidade com as diretrizes e as normas técnicas estabelecidas.

[97] A estrutura da ICP-Brasil não prevê o uso de autoridades de registro e utiliza autoridades certificadoras assinadas pela chave pública da própria ICP-Brasil.

3. A Autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz) é a primeira autoridade da cadeia de certificação. No que se refere à ICP-Brasil, julgue os itens subsequentes.

[95] A emissão da lista de certificados revogados (LCR) é responsabilidade da AC-Raiz da ICP-Brasil.

~~[96] O comitê gestor da ICP-Brasil verifica se as autoridades certificadoras atuam em conformidade com as diretrizes e as normas técnicas estabelecidas.~~

~~[97] A estrutura da ICP-Brasil não prevê o uso de autoridades de registro e utiliza autoridades certificadoras assinadas pela chave pública da própria ICP-Brasil.~~

4. Com relação às funções de hash, à assinatura digital e aos certificados digitais, julgue os itens a seguir.

[114] Um certificado digital padrão X.509 contém, entre outros dados, a versão, o número serial e o tipo de algoritmo criptográfico utilizado pela autoridade certificadora.

[116] Se a veracidade do emissor de uma mensagem estiver garantida e sua assinatura puder ser verificada publicamente, o emissor deverá assinar a mensagem com sua chave privada.

4. Com relação às funções de hash, à assinatura digital e aos certificados digitais, julgue os itens a seguir.

[114] Um certificado digital padrão X.509 contém, entre outros dados, a versão, o número serial e o tipo de algoritmo criptográfico utilizado pela autoridade certificadora.

[116] Se a veracidade do emissor de uma mensagem estiver garantida e sua assinatura puder ser verificada publicamente, o emissor deverá assinar a mensagem com sua chave privada.

5. No que diz respeito ao funcionamento da ICP-Brasil, julgue os itens que se seguem.

[118] Compete à AC-Raiz da ICP-Brasil emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente inferior a ela.

[119] Recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes, são responsabilidades de uma autoridade de registro vinculada à AC-Raiz da ICP-Brasil.

5. No que diz respeito ao funcionamento da ICP-Brasil, julgue os itens que se seguem.

[118] Compete à AC-Raiz da ICP-Brasil emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente inferior a ela.

[119] Recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes, são responsabilidades de uma autoridade de registro vinculada à AC-Raiz da ICP-Brasil.

6. Julgue os itens a seguir, a respeito de certificação digital e algoritmos RSA, AES e RC4.

[104] Ao acessar um sítio seguro na Internet e receber o certificado digital do servidor, o navegador do cliente faz uma consulta à autoridade certificadora que assinou aquele certificado para verificar, por exemplo, se o certificado é válido ou não está revogado. Essa verificação é feita com o uso do protocolo OCSP (Online Certificate Status Protocol).

6. Julgue os itens a seguir, a respeito de certificação digital e algoritmos RSA, AES e RC4.

[104] Ao acessar um sítio seguro na Internet e receber o certificado digital do servidor, o navegador do cliente faz uma consulta à autoridade certificadora que assinou aquele certificado para verificar, por exemplo, se o certificado é válido ou não está revogado. Essa verificação é feita com o uso do protocolo OCSP (Online Certificate Status Protocol).

7. Julgue os itens a seguir, referentes à criptografia e assinatura e certificação digitais.

[66] Um certificado digital consiste na cifração do resumo criptográfico de uma chave pública com a utilização da chave privada de uma autoridade certificadora.

7. Julgue os itens a seguir, referentes à criptografia e assinatura e certificação digitais.

[66] Um certificado digital consiste na cifração do resumo criptográfico de uma chave pública com a utilização da chave privada de uma autoridade certificadora.

8. Em relação à criptografia, julgue os próximos itens.

[112] Certificado digital é um tipo de registro eletrônico, com chave pública, que contém dados capazes de identificar uma entidade. Além disso, é validado por outra entidade e pode ser emitido para pessoas físicas e jurídicas.

8. Em relação à criptografia, julgue os próximos itens.

[112] Certificado digital é um tipo de registro eletrônico, com chave pública, que contém dados capazes de identificar uma entidade. Além disso, é validado por outra entidade e pode ser emitido para pessoas físicas e jurídicas.

9. Com relação à certificação digital, julgue os itens que se seguem.

[114] As autoridades de registro, que se devem vincular a uma autoridade certificadora, recebem, validam, verificam e encaminham as solicitações de emissão e de revogação dos certificados digitais para as autoridades certificadoras.

[115] Um requisito para uma entidade tornar-se uma autoridade de registro é ser uma entidade jurídica, não podendo as pessoas físicas tornarem-se autoridades de registro.

[116] A Infraestrutura de Chaves Públicas do Brasil compõe-se de duas categorias de certificados digitais: A, destinada a atividades sigilosas, e S, destinada à autenticação e identificação.

9. Com relação à certificação digital, julgue os itens que se seguem.

[114] As autoridades de registro, que se devem vincular a uma autoridade certificadora, recebem, validam, verificam e encaminham as solicitações de emissão e de revogação dos certificados digitais para as autoridades certificadoras.

[115] Um requisito para uma entidade tornar-se uma autoridade de registro é ser uma entidade jurídica, não podendo as pessoas físicas tornarem-se autoridades de registro.

~~[116] A Infraestrutura de Chaves Públicas do Brasil compõe-se de duas categorias de certificados digitais: A, destinada a atividades sigilosas, e S, destinada à autenticação e identificação.~~

10. Acerca de certificação digital, julgue os próximos itens.

[104] A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para a identificação virtual do cidadão no Brasil, conforme os padrões e normas estipulados pela CERTISIGN, à qual se subordina hierarquicamente em nível mundial.

[105] Assim como pessoas físicas, as micro e pequenas empresas também podem comprovar sua identidade no meio virtual, realizar transações comerciais e financeiras com validade jurídica, participar de pregões eletrônicos e trocar mensagens no mundo virtual com segurança e agilidade com o e-CPF Simples.

10. Acerca de certificação digital, julgue os próximos itens.

~~[104] A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para a identificação virtual do cidadão no Brasil, conforme os padrões e normas estipulados pela CERTISIGN, à qual se subordina hierarquicamente em nível mundial.~~

[105] Assim como pessoas físicas, as micro e pequenas empresas também podem comprovar sua identidade no meio virtual, realizar transações comerciais e financeiras com validade jurídica, participar de pregões eletrônicos e trocar mensagens no mundo virtual com segurança e agilidade com o e-CPF Simples.

GABARITO

1. C
2. E
3. C, E, E
4. C, C
5. C, C
6. E
7. C
8. C
9. C, C, E
10. E, C

Décima Bateria de Questões Com Resolução Assistida

Criptografia – Certificação Digital

1. No que diz respeito aos fundamentos de criptografia e certificação digital, julgue os itens subsecutivos. Nesse contexto, considere que a sigla AC, sempre que utilizada, se refira a autoridade certificadora.

[93] Para a obtenção da chave pública de uma AC, utiliza-se um esquema de gerenciamento de chaves públicas, denominado infraestrutura de chaves públicas (ICP). No Brasil, a ICP-Brasil é organizada de forma hierárquica, em que uma AC raiz certifica outras ACs e, posteriormente, estas, bem como a AC raiz, emitem certificados para os usuários finais.

[94] Cada certificado digital emitido por uma AC é específico para determinado usuário final e pode ser revogado a qualquer momento pela respectiva AC.

1. No que diz respeito aos fundamentos de criptografia e certificação digital, julgue os itens subsecutivos. Nesse contexto, considere que a sigla AC, sempre que utilizada, se refira a autoridade certificadora.

~~[93] Para a obtenção da chave pública de uma AC, utiliza-se um esquema de gerenciamento de chaves públicas, denominado infraestrutura de chaves públicas (ICP). No Brasil, a ICP-Brasil é organizada de forma hierárquica, em que uma AC raiz certifica outras ACs e, posteriormente, estas, bem como a AC raiz, emitem certificados para os usuários finais.~~

[94] Cada certificado digital emitido por uma AC é específico para determinado usuário final e pode ser revogado a qualquer momento pela respectiva AC.

2. Acerca da infraestrutura de chaves públicas ICP-Brasil, julgue o item abaixo.

[98] A assinatura eletrônica vinculada a um certificado emitido no âmbito da ICP-Brasil tem função específica e restrita de determinar a não violação do conteúdo de um documento assinado eletronicamente, e não conduz à presunção de autenticidade do emissor do documento subscrito.

2. Acerca da infraestrutura de chaves públicas ICP-Brasil, julgue o item abaixo.

~~[98] A assinatura eletrônica vinculada a um certificado emitido no âmbito da ICP-Brasil tem função específica e restrita de determinar a não violação do conteúdo de um documento assinado eletronicamente, e não conduz à presunção de autenticidade do emissor do documento subscrito.~~

3. Acerca dos conceitos de segurança de redes, criptografia e certificação digital, julgue os itens seguintes.

[96] No certificado padrão X.509, o campo Encrypted identifica o algoritmo usado para a assinatura do certificado.

[99] Na ICP-Brasil, embora a assinatura digital possua autenticidade, integridade, confiabilidade e não repúdio, ela não garante sigilo ao documento eletrônico.

[100] O padrão PKCS#7, utilizado no algoritmo Diffie-Hellman, descreve uma sintaxe genérica para dados que podem ser submetidos a funções criptográficas, como assinatura e envelopagem digital, sendo utilizado na ICP-Brasil como formato para a entrega dos certificados digitais aos seus titulares.

3. Acerca dos conceitos de segurança de redes, criptografia e certificação digital, julgue os itens seguintes.

~~[96] No certificado padrão X.509, o campo Encrypted identifica o algoritmo usado para a assinatura do certificado.~~

[99] Na ICP-Brasil, embora a assinatura digital possua autenticidade, integridade, confiabilidade e não repúdio, ela não garante sigilo ao documento eletrônico.

~~[100] O padrão PKCS#7, utilizado no algoritmo Diffie-Hellman, descreve uma sintaxe genérica para dados que podem ser submetidos a funções criptográficas, como assinatura e envelopagem digital, sendo utilizado na ICP-Brasil como formato para a entrega dos certificados digitais aos seus titulares.~~

4. Com relação a PKI e certificação digital, julgue os itens que se seguem.

[74] Se uma autoridade certificadora estiver instalada e em funcionamento, a lista de certificados revogados (LCR) deverá ficar criptografada para não expor as chaves privadas.

[75] Certificação cruzada é uma forma de criar uma cadeia de confiança entre uma autoridade certificadora e outras autoridades certificadoras.

4. Com relação a PKI e certificação digital, julgue os itens que se seguem.

~~[74] Se uma autoridade certificadora estiver instalada e em funcionamento, a lista de certificados revogados (LCR) deverá ficar criptografada para não expor as chaves privadas.~~

[75] Certificação cruzada é uma forma de criar uma cadeia de confiança entre uma autoridade certificadora e outras autoridades certificadoras.

5. Julgue os próximos itens, que se referem à certificação digital.

[89] Um certificado digital consiste na cifração do resumo criptográfico de uma chave pública, usando-se a chave privada de uma autoridade certificadora raiz.

[90] A verificação de um certificado digital é feita mediante a decifração, com a chave pública da autoridade certificadora que o assinou, do resumo criptográfico cifrado (que nele consta) e a confrontação deste com o cálculo do resumo da chave pública a que se refere o certificado.

[91] Um certificado comum autoassinado é, em princípio, menos seguro que um certificado assinado por outra autoridade certificadora.

[92] Os certificados mutuamente assinados são mais seguros que os assinados por uma terceira autoridade certificadora.

5. Julgue os próximos itens, que se referem à certificação digital.

[89] Um certificado digital consiste na cifração do resumo criptográfico de uma chave pública, usando-se a chave privada de uma autoridade certificadora raiz.

~~[90] A verificação de um certificado digital é feita mediante a decifração, com a chave pública da autoridade certificadora que o assinou, do resumo criptográfico cifrado (que nele consta) e a confrontação deste com o cálculo do resumo da chave pública a que se refere o certificado.~~

[91] Um certificado comum autoassinado é, em princípio, menos seguro que um certificado assinado por outra autoridade certificadora.

~~[92] Os certificados mutuamente assinados são mais seguros que os assinados por uma terceira autoridade certificadora.~~

6. Acerca de criptografia e da infraestrutura de chave pública, julgue os itens subsecutivos.

[94] A assinatura digital é gerada por criptografia assimétrica mediante a utilização de uma chave pública para codificar a mensagem.

[96] A lista de certificados revogados (LCR) de uma infraestrutura de chaves públicas deve ser emitida pela autoridade certificadora, que também é responsável por emitir e gerenciar certificados digitais.

6. Acerca de criptografia e da infraestrutura de chave pública, julgue os itens subsecutivos.

~~[94] A assinatura digital é gerada por criptografia assimétrica mediante a utilização de uma chave pública para codificar a mensagem.~~

[96] A lista de certificados revogados (LCR) de uma infraestrutura de chaves públicas deve ser emitida pela autoridade certificadora, que também é responsável por emitir e gerenciar certificados digitais.

7. A respeito de certificação digital, julgue os itens seguintes.

[89] Ao utilizar um certificado digital de 2.048 bits, tanto a chave privada quanto a chave pública terão 1024 bits, que somadas geram o certificado de 2048 bits.

7. A respeito de certificação digital, julgue os itens seguintes.

~~[89] Ao utilizar um certificado digital de 2.048 bits, tanto a chave privada quanto a chave pública terão 1024 bits, que somadas geram o certificado de 2048 bits.~~

8. A propósito de segurança de redes e certificação digital, julgue os itens subsecutivos.

[120] A assinatura digital garante a confidencialidade da transmissão da informação.

8. A propósito de segurança de redes e certificação digital, julgue os itens subsecutivos.

~~[120] A assinatura digital garante a confidencialidade da transmissão da informação.~~

9. Julgue os itens a seguir, a respeito de criptografia.

[116] Na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), a autoridade de registro é uma entidade na qual os usuários de serviços de Carimbo do Tempo confiam para emitir certificado para provar a sua existência em determinado período.

9. Julgue os itens a seguir, a respeito de criptografia.

~~[116] Na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), a autoridade de registro é uma entidade na qual os usuários de serviços de Carimbo do Tempo confiam para emitir certificado para provar a sua existência em determinado período.~~

10. A respeito de fundamentos de assinatura digital e certificado digital, julgue os itens subsequentes.

[93] A autoridade certificadora é responsável por divulgar informações caso o certificado por ela emitido não seja mais confiável.

[94] O uso de assinatura digital objetiva comprovar a autenticidade e a integridade de uma informação, sendo a integridade garantida mediante a codificação de todo o conteúdo referente à assinatura.

10. A respeito de fundamentos de assinatura digital e certificado digital, julgue os itens subsequentes.

[93] A autoridade certificadora é responsável por divulgar informações caso o certificado por ela emitido não seja mais confiável.

~~[94] O uso de assinatura digital objetiva comprovar a autenticidade e a integridade de uma informação, sendo a integridade garantida mediante a codificação de todo o conteúdo referente à assinatura.~~

GABARITO

1. E, C
2. E
3. E, C, E
4. E, C
5. C, E, C, E
6. E, C
7. E
8. E
9. E
10. C, E