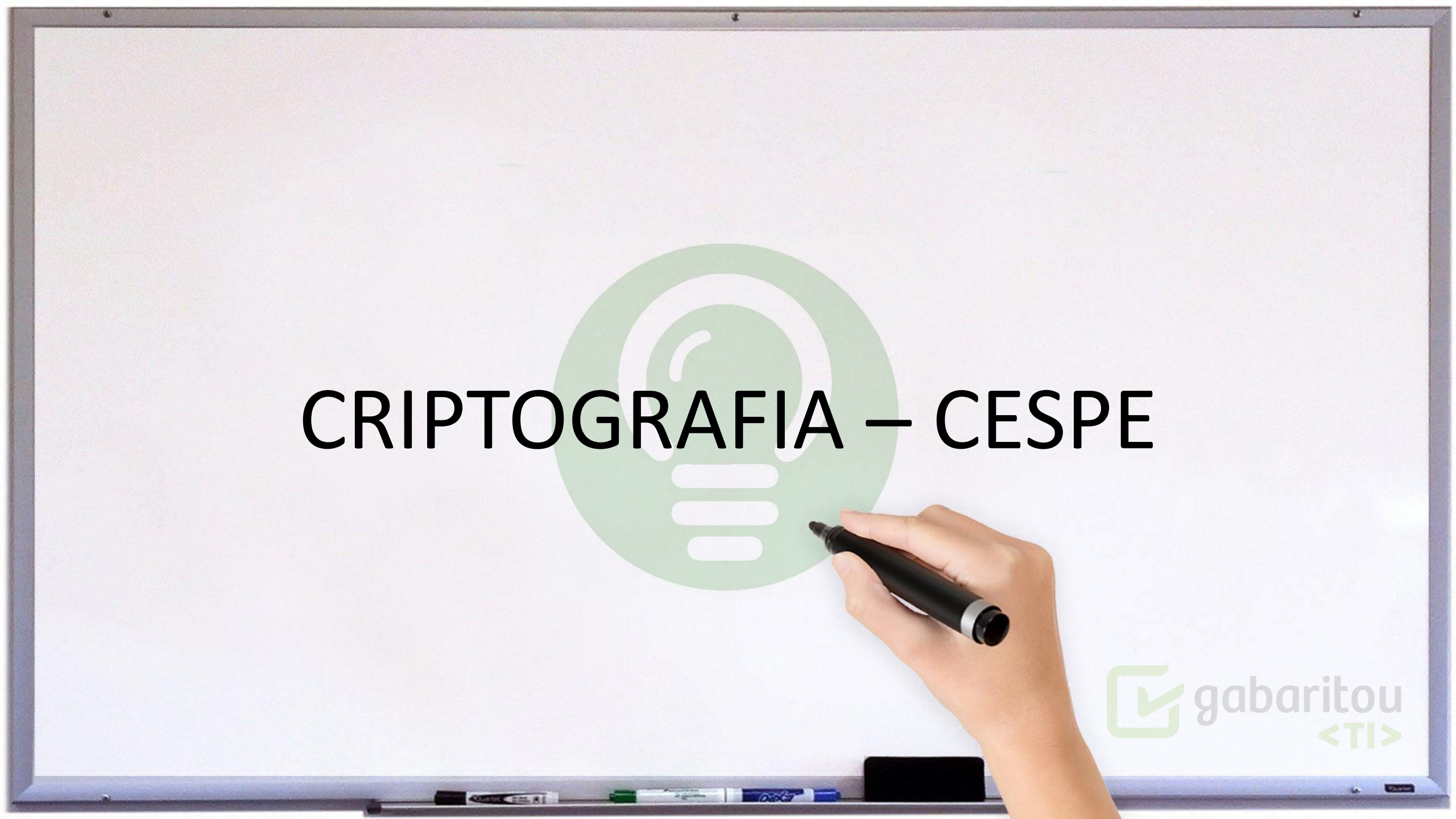
CRIPTOGRAFIA – CESPE



GUSTAVO PINTO VILAR

- ✓ Especialista em Docência do Ensino Superior pela UFRJ
- ✓ Bacharel em Ciência da Computação e Tecnólogo em Processamento de Dados pela ASPER – Associação Paraibana de Ensino Renovado.
- ✓ No serviço público, atuou como Oficial de Cavalaria do Exército Brasileiro, Policial Rodoviário Federal e Papiloscopista Policial Federal.
- ✓ Perito Criminal Federal especialista em Informática Forense, atuando principalmente nas análises de vestígios em crimes cibernéticos.
- ✓ Coautor e revisor da obra Tratado de Computação Forense

1. Acerca das características dos algoritmos criptográficos AES e RSA, julgue os itens que se seguem.

O AES permite que os blocos tenham tamanho, em bits, de 128, 192 ou 256.

C Certo

E Errado

1. Acerca das características dos algoritmos criptográficos AES e RSA, julgue os itens que se seguem.

O AES permite que os blocos tenham tamanho, em bits, de 128, 192 ou 256.

C Certo

E Errado

2. Acerca das características dos algoritmos criptográficos AES e RSA, julgue os itens que se seguem.

Por ser um algoritmo simétrico, o AES utiliza a mesma chave para cifrar e decifrar os dados.

C Certo

E Errado

2. Acerca das características dos algoritmos criptográficos AES e RSA, julgue os itens que se seguem.

Por ser um algoritmo simétrico, o AES utiliza a mesma chave para cifrar e decifrar os dados.

C Certo

E Errado

3. Acerca das características dos algoritmos criptográficos AES e RSA, julgue os itens que se seguem.

O RSA permite a criação de chaves com diversos tamanhos, entre eles, as de 2.048 bits ou 4.096 bits.

C Certo

E Errado

3. Acerca das características dos algoritmos criptográficos AES e RSA, julgue os itens que se seguem.

O RSA permite a criação de chaves com diversos tamanhos, entre eles, as de 2.048 bits ou 4.096 bits.

C Certo

E Errado

4. No que se refere à criptografia, seus conceitos básicos, sistemas simétricos e assimétricos, certificação e assinatura digital, e protocolos criptográficos, assinale a opção correta.

A O único sistema criptográfico matematicamente inviolável é conhecido pelo nome de One Time Pad, e o comprometimento de seu uso ocorre na eventualidade de falhas na geração de chaves aleatórias, na reutilização dessas chaves ou na sua guarda

B No que se refere ao uso de cifradores simétricos, uma cifra de fluxo é mais adequada quando se executa a cifração de arquivos com tamanho limitado, enquanto cifras de bloco são mais adequadas para arquivos de tamanho ilimitado

C O uso de funções oneway, ou de hash criptográfico, é opcional para a construção de assinaturas digitais convencionais

D O protocolo de troca de chaves conhecido como Diffie-Hellman viabiliza a geração de chaves criptográficas assimétricas

E São exemplos de primitivas criptográficas utilizadas na construção de sistemas criptográficos: Standard TLS, IPSec, Kerberos e X.509

4. No que se refere à criptografia, seus conceitos básicos, sistemas simétricos e assimétricos, certificação e assinatura digital, e protocolos criptográficos, assinale a opção correta.

A O único sistema criptográfico matematicamente inviolável é conhecido pelo nome de One Time Pad, e o comprometimento de seu uso ocorre na eventualidade de falhas na geração de chaves aleatórias, na reutilização dessas chaves ou na sua guarda

B No que se refere ao uso de cifradores simétricos, uma cifra de fluxo é mais adequada quando se executa a cifração de arquivos com tamanho limitado, enquanto cifras de bloco são mais adequadas para arquivos de tamanho ilimitado

C O uso de funções oneway, ou de hash criptográfico, é opcional para a construção de assinaturas digitais convencionais

D O protocolo de troca de chaves conhecido como Diffie-Hellman viabiliza a geração de chaves criptográficas assimétricas

E São exemplos de primitivas criptográficas utilizadas na construção de sistemas criptográficos: Standard TLS, IPSec, Kerberos e X.509

5. A propósito de criptografia, assinale a opção correta.

A Há, no envio de email com o hash, garantia de autenticidade, pois ele criptografa a mensagem enviada

B Na criptografia de chave pública, ou assimétrica, a chave utilizada para encriptar mensagens é distribuída livremente, ao passo que a chave privada decripta a mensagem

C São utilizadas, na criptografia simétrica, duas chaves: uma para encriptar e outra para decriptar

D O AES é um algoritmo de criptografia simétrica que usa chaves de 168 bites

E A criptografia, simétrica além de garantir a integridade dos dados, atende plenamente aos demais princípios de segurança como a integridade e a autenticidade, por exemplo

5. A propósito de criptografia, assinale a opção correta.

A Há, no envio de email com o hash, garantia de autenticidade, pois ele criptografa a mensagem enviada

B Na criptografia de chave pública, ou assimétrica, a chave utilizada para encriptar mensagens é distribuída livremente, ao passo que a chave privada decripta a mensagem

C São utilizadas, na criptografia simétrica, duas chaves: uma para encriptar e outra para decriptar

D O AES é um algoritmo de criptografia simétrica que usa chaves de 168 bites

E A criptografia, simétrica além de garantir a integridade dos dados, atende plenamente aos demais princípios de segurança como a integridade e a autenticidade, por exemplo

6. Assinale a opção correta relativamente a criptografia.

A O algoritmo de criptografia AES utiliza quatro estágios diferentes, dois de permutação e dois de substituição

B No modo de operação de cifra de bloco cipher block chaining, o texto claro é tratado em blocos — um bloco por vez — e cada bloco de texto claro é criptografado mediante o uso de uma mesma chave

C Um código gerado por uma função hash para um conjunto de dados pode garantir a sua integridade porque, ao ser calculado novamente sobre o mesmo conjunto de dados, a qualquer tempo, pode determinar, inequivocadamente, se esse conjunto foi alterado ou não

D Esquema de criptografia incondicionalmente seguro significa que o custo para quebrar a cifra é superior ao valor da informação codificada ou que o tempo exigido para quebrar a cifra é superior ao tempo de vida útil da informação

E A criptoanálise, técnica para ataque a um esquema de criptografia convencional, caracteriza-se pela experimentação de cada chave possível em um trecho do texto cifrado, até que se obtenha uma tradução inteligível para texto claro

6. Assinale a opção correta relativamente a criptografia.

A O algoritmo de criptografia AES utiliza quatro estágios diferentes, dois de permutação e dois de substituição

B No modo de operação de cifra de bloco cipher block chaining, o texto claro é tratado em blocos — um bloco por vez — e cada bloco de texto claro é criptografado mediante o uso de uma mesma chave

C Um código gerado por uma função hash para um conjunto de dados pode garantir a sua integridade porque, ao ser calculado novamente sobre o mesmo conjunto de dados, a qualquer tempo, pode determinar, inequivocadamente, se esse conjunto foi alterado ou não

D Esquema de criptografia incondicionalmente seguro significa que o custo para quebrar a cifra é superior ao valor da informação codificada ou que o tempo exigido para quebrar a cifra é superior ao tempo de vida útil da informação

E A criptoanálise, técnica para ataque a um esquema de criptografia convencional, caracteriza-se pela experimentação de cada chave possível em um trecho do texto cifrado, até que se obtenha uma tradução inteligível para texto claro

7. Considere que, em uma rede com muitos usuários, a distribuição das chaves secretas a serem utilizadas na criptografia de documentos seja realizada através da rede com a utilização, de forma automática, de algoritmos. Nessa situação hipotética, a distribuição de chaves não afeta a segurança da rede, mesmo que as comunicações entre os usuários não estejam autenticadas.

C Certo

E Errado

7. Considere que, em uma rede com muitos usuários, a distribuição das chaves secretas a serem utilizadas na criptografia de documentos seja realizada através da rede com a utilização, de forma automática, de algoritmos. Nessa situação hipotética, a distribuição de chaves não afeta a segurança da rede, mesmo que as comunicações entre os usuários não estejam autenticadas.

C Certo

E Errado

8. Se o texto cifrado do texto claro HELLO for ABNZF, então a cifra será monoalfabética.

C Certo

E Errado

8. Se o texto cifrado do texto claro HELLO for ABNZF, então a cifra será monoalfabética.

C Certo

E Errado

9. O comprimento do fluxo de bits, na entrada de uma S-box, é igual ao comprimento do fluxo de bits resultante, na saída da S-box.

C Certo

E Errado

9. O comprimento do fluxo de bits, na entrada de uma S-box, é igual ao comprimento do fluxo de bits resultante, na saída da S-box.

C Certo

E Errado

10. A criptografia de uma chave privada, usada para codificar e decodificar as mensagens, é uma solução para que possam ser distribuídas com segurança as chaves assimétricas.

C Certo

E Errado

10. A criptografia de uma chave privada, usada para codificar e decodificar as mensagens, é uma solução para que possam ser distribuídas com segurança as chaves assimétricas.

C Certo

E Errado

11. Para implementar um sistema de ECM (enterprise content management), do ponto de vista da criptografia, é necessário utilizar infraestrutura interna de chaves públicas, na qual tokens ou smartcards podem ser utilizados para armazenagem e proteção das chaves públicas de cada colaborador.

C Certo

E Errado

11. Para implementar um sistema de ECM (enterprise content management), do ponto de vista da criptografia, é necessário utilizar infraestrutura interna de chaves públicas, na qual tokens ou smartcards podem ser utilizados para armazenagem e proteção das chaves públicas de cada colaborador.

C Certo

E Errado

12. A função criptográfica hash pode ser utilizada para ofuscar senhas em aplicações. O algoritmo md5 é considerado seguro, quando comparado ao SHA-2, devido a sua baixa taxa de colisões e à baixa quantidade de rainbow tables associadas.

Certo

Errado

12. A função criptográfica hash pode ser utilizada para ofuscar senhas em aplicações. O algoritmo md5 é considerado seguro, quando comparado ao SHA-2, devido a sua baixa taxa de colisões e à baixa quantidade de rainbow tables associadas.

Certo

Errado

13. A restrição de endereços IPs de origem, a utilização de chaves criptográfica para autenticação e a mudança da porta padrão, são consideradas boas práticas de segurança quanto ao uso do serviço de SSH.

Certo

Errado

13. A restrição de endereços IPs de origem, a utilização de chaves criptográfica para autenticação e a mudança da porta padrão, são consideradas boas práticas de segurança quanto ao uso do serviço de SSH.

Certo

Errado

14. A partir de uma mensagem criptografada, é possível obter a mensagem aberta, utilizando-se a função UNHASH correspondente à função HASH utilizada na encriptação, uma vez que as funções de encriptação HASH podem ser reversíveis.

Certo

Errado

14. A partir de uma mensagem criptografada, é possível obter a mensagem aberta, utilizando-se a função UNHASH correspondente à função HASH utilizada na encriptação, uma vez que as funções de encriptação HASH podem ser reversíveis.

Certo

Errado

15. A integridade garante que a informação provenha da fonte anunciada e que não seja alvo de alterações ao longo de um processo, ao passo que a autenticidade garante que a informação manipulada mantenha todas as características originais criadas pelo dono da informação.

Certo

Errado

15. A integridade garante que a informação provenha da fonte anunciada e que não seja alvo de alterações ao longo de um processo, ao passo que a autenticidade garante que a informação manipulada mantenha todas as características originais criadas pelo dono da informação.

Certo

Errado

16. O AES (advanced encryption standard) é um algoritmo de criptografia de chave simétrica que criptografa e descriptografa dados por meio de uma chave criptografada e de blocos, cujos tamanhos são de 128, 192 ou 256 bits.

Certo

Errado

16. O AES (advanced encryption standard) é um algoritmo de criptografia de chave simétrica que criptografa e descriptografa dados por meio de uma chave criptografada e de blocos, cujos tamanhos são de 128, 192 ou 256 bits.

Certo

Errado

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

Duas chaves são exigidas ao se utilizarem algoritmos de chave pública. Uma delas, a chave pública, cujos algoritmos são menos robustos que os algoritmos de chave simétrica, é usada para criptografar as mensagens para um usuário que faz uso de uma chave privada para descriptografá-las.

Certo

Errado

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

Duas chaves são exigidas ao se utilizarem algoritmos de chave pública. Uma delas, a chave pública, cujos algoritmos são menos robustos que os algoritmos de chave simétrica, é usada para criptografar as mensagens para um usuário que faz uso de uma chave privada para descriptografá-las.

Certo

Errado

18. A respeito de criptografia e protocolos, julgue os itens a seguir.

O protocolo 3DES possui três chaves criptográficas: a primeira e a segunda criptografam informações; a terceira é usada para descriptografar aquelas.

Certo

Errado

18. A respeito de criptografia e protocolos, julgue os itens a seguir.

O protocolo 3DES possui três chaves criptográficas: a primeira e a segunda criptografam informações; a terceira é usada para descriptografar aquelas.

Certo

Errado

19. Se, em um esquema de criptografia de chave pública, o emissor E criptografar uma mensagem M utilizando a chave pública do receptor R, então, nesse esquema, é oferecida confidencialidade, mas não autenticação.

Certo

Errado

19. Se, em um esquema de criptografia de chave pública, o emissor E criptografar uma mensagem M utilizando a chave pública do receptor R, então, nesse esquema, é oferecida confidencialidade, mas não autenticação.

Certo

Errado

20. 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.

20. 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.

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

Certo

Errado

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

Certo

Errado

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

Certo

Errado

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

Certo

Errado

23. 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.

Certo

Errado

23. 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.

Certo

Errado

24. 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.

Certo

Errado

24. 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.

Certo

Errado

25. Em sistemas de uso prático, são usadas as técnicas simétricas e as assimétricas combinadas.

Certo

Errado

25. Em sistemas de uso prático, são usadas as técnicas simétricas e as assimétricas combinadas.

Certo

Errado

26. A confidencialidade pode ser obtida pelo uso da criptografia simétrica e da assimétrica.

Certo

Errado

26. A confidencialidade pode ser obtida pelo uso da criptografia simétrica e da assimétrica.

Certo

Errado

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

Certo

Errado

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

Certo

Errado

28. A criptografia assimétrica proporciona o não repúdio, não proporcionando, porém, a autenticidade.

Certo

Errado

28. A criptografia assimétrica proporciona o não repúdio, não proporcionando, porém, a autenticidade.

Certo

Errado

29. As funções de resumo criptográfico oferecem garantia probabilística de inforjabilidade.

Certo

Errado

29. As funções de resumo criptográfico oferecem garantia probabilística de inforjabilidade.

Certo

Errado

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

Certo

Errado

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

Certo

Errado

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

Certo

Errado

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

Certo

Errado

32. O algoritmo de criptografia AES (advanced encryption standard) opera em quatro estágios: um de permutação e três de substituição. O estágio de permutação ShiftRows é reversível e os estágios de substituição SubBytes, MixColumns e AddRoundKey são não-reversíveis.

Certo

Errado

32. O algoritmo de criptografia AES (advanced encryption standard) opera em quatro estágios: um de permutação e três de substituição. O estágio de permutação ShiftRows é reversível e os estágios de substituição SubBytes, MixColumns e AddRoundKey são não-reversíveis.

Certo

Errado

33. Para que a criptografia de chave pública seja considerada segura, uma das premissas é que o conhecimento do algoritmo, o conhecimento de uma das chaves e a disponibilidade de amostras de texto cifrado sejam, em conjunto, insuficientes para determinar a outra chave.

Certo

Errado

33. Para que a criptografia de chave pública seja considerada segura, uma das premissas é que o conhecimento do algoritmo, o conhecimento de uma das chaves e a disponibilidade de amostras de texto cifrado sejam, em conjunto, insuficientes para determinar a outra chave.

Certo

Errado

34. 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.

Certo

Errado

34. 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.

Certo

Errado

35. 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.

Certo

Errado

35. 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.

Certo

Errado

36. 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.

Certo

Errado

36. 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.

Certo

Errado

37. 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.

Certo

Errado

37. 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.

Certo

Errado

38. De forma semelhante a assinaturas digitais, o hash pode ser implementado utilizando-se técnicas criptográficas, por meio de pares de chaves relacionadas, em que a chave privada é aplicada para criar a assinatura ou o hash e a chave pública realiza a verificação dessa assinatura.

Certo

Errado

38. De forma semelhante a assinaturas digitais, o hash pode ser implementado utilizando-se técnicas criptográficas, por meio de pares de chaves relacionadas, em que a chave privada é aplicada para criar a assinatura ou o hash e a chave pública realiza a verificação dessa assinatura.

Certo

Errado

39. A criptografia é uma técnica voltada para proteger a confiabilidade das informações, principalmente a criptografia considerada forte, com tamanho de chaves acima de 1.024 bites.

Certo

Errado

39. A criptografia é uma técnica voltada para proteger a confiabilidade das informações, principalmente a criptografia considerada forte, com tamanho de chaves acima de 1.024 bites.

Certo

Errado

40. Na proteção de informações críticas, para a garantia de sua integridade, devem ser utilizados algoritmos de criptografia

Certo

Errado

40. Na proteção de informações críticas, para a garantia de sua integridade, devem ser utilizados algoritmos de criptografia

Certo

Errado

41. 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.

Certo

Errado

41. 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.

Certo

Errado

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

Certo

Errado

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

Certo

Errado

43. 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

Certo

Errado

43. 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

Certo

Errado

44. 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.

Certo

Errado

44. 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.

Certo

Errado

45. 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

Certo

Errado

45. 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

Certo

Errado

46. 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.

Certo

Errado

46. 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.

Certo

Errado

47. A assinatura digital, que é uma unidade de dados originada de uma transformação criptográfica, possibilita que um destinatário da unidade de dados comprove a origem e a integridade dessa unidade e se proteja contra falsificação.

Certo

Errado

47. A assinatura digital, que é uma unidade de dados originada de uma transformação criptográfica, possibilita que um destinatário da unidade de dados comprove a origem e a integridade dessa unidade e se proteja contra falsificação.

Certo

Errado

48. Em uma troca de dados, via Internet, entre dois computadores que estejam utilizando um algoritmo de criptografia assimétrica, antes de trocarem os dados, os usuários deverão compartilhar entre eles a chave, já que ela deve ser a mesma para os dois usuários.

Certo

Errado

48. Em uma troca de dados, via Internet, entre dois computadores que estejam utilizando um algoritmo de criptografia assimétrica, antes de trocarem os dados, os usuários deverão compartilhar entre eles a chave, já que ela deve ser a mesma para os dois usuários.

Certo

Errado

49. 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

Certo

Errado

49. 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

Certo

Errado

50. 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

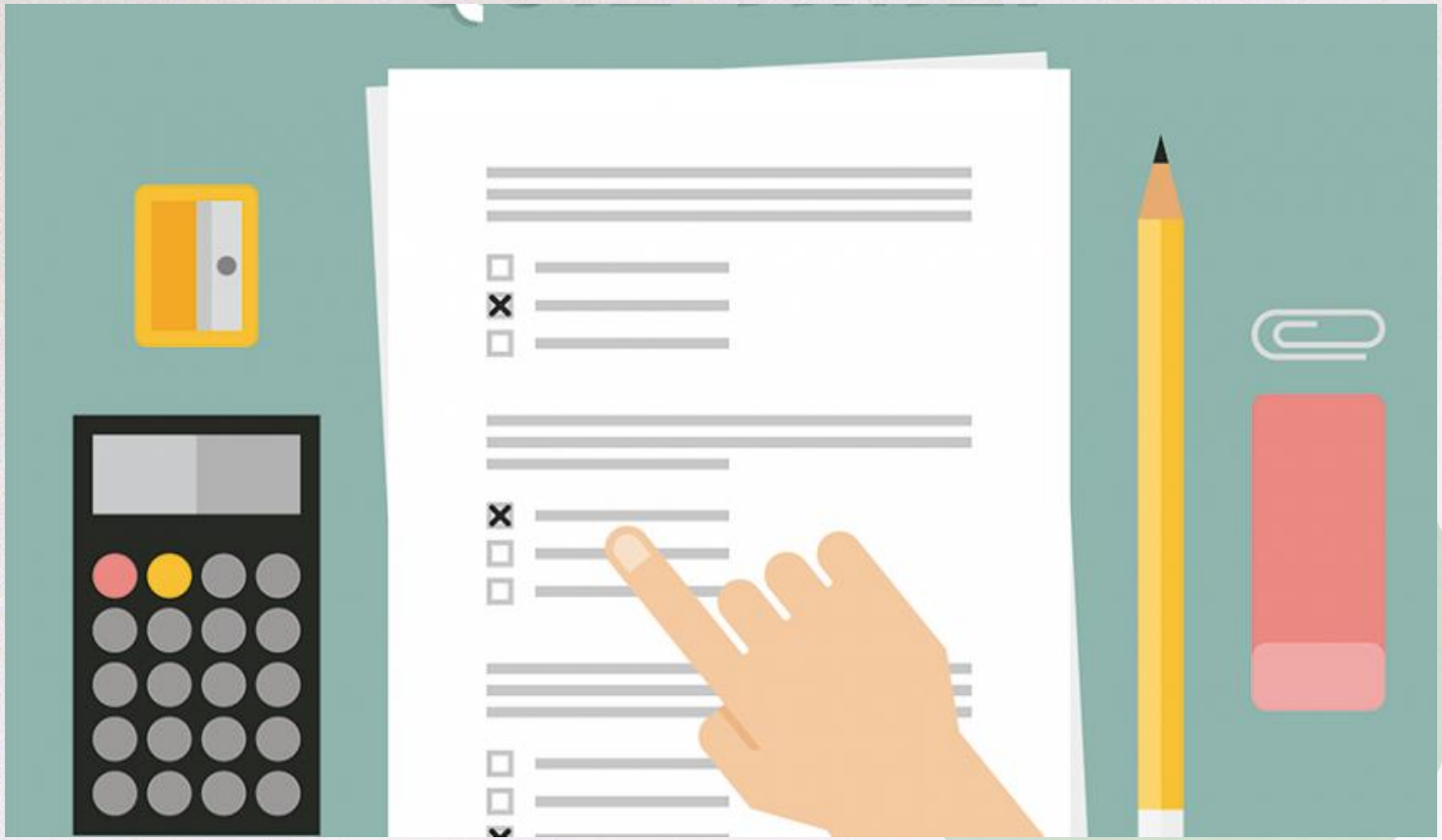
Certo

Errado

50. 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

Certo

Errado



GABARITO

1.	E	18.	E	35.	E
2.	C	19.	C	36.	C
3.	C	20.	B	37.	E
4.	A	21.	E	38.	E
5.	B	22.	C	39.	E
6.	C	23.	C	40.	E
7.	E	24.	C	41.	E
8.	E	25.	C	42.	E
9.	E	26.	C	43.	E
10.	E	27.	E	44.	C
11.	E	28.	E	45.	E
12.	E	29.	C	46.	C
13.	C	30.	C	47.	C
14.	E	31.	E	48.	E
15.	E	32.	E	49.	E
16.	C	33.	C	50.	E
17.	E	34.	C		