



CHAVES E CRIPTOGRAFIA – ESAF

01 - **(ESAF - Auditor-Fiscal da Receita Federal do Brasil - AFRFB - 2005)** O processo de cifragem e decifragem são realizados com o uso de algoritmos com funções matemáticas que protegem a informação quanto à sua integridade, autenticidade e sigilo. Quanto aos algoritmos utilizados nos processos de cifragem, decifragem e assinatura digital é correto afirmar que

- a) o uso da assinatura digital garante o sigilo da mensagem independentemente do tipo de chave utilizada.
- b) os algoritmos RSA para assinatura digital fazem o uso de chave simétrica.
- c) os algoritmos de chave simétrica têm como principal característica a possibilidade de utilização de assinatura digital e de certificação digital, sem alteração da chave.
- d) a criptografia de chave simétrica tem como característica a utilização de uma mesma chave secreta para a codificação e decodificação dos dados.
- e) a assinatura digital é obtida com a aplicação do algoritmo de Hash sobre a chave pública do usuário que deseja assinar digitalmente uma mensagem.

02 - **(ESAF - Auditor-Fiscal do Trabalho - 2006)** Analise as seguintes afirmações relacionadas a conceitos básicos de Internet, protocolos TCP/IP e Segurança da Informação.

- I. A assinatura digital é o processo de manter mensagens e dados em segurança, permitindo e assegurando a confidencialidade. Quando utilizam apenas chaves privadas, as assinaturas digitais são usadas para fornecer serviços de integridade de dados, autenticação e não repúdio.
- II. Um algoritmo de criptografia simétrica requer que uma chave secreta seja usada na criptografia e uma chave pública diferente e complementar da secreta, utilizada no processo anterior, seja utilizada na decriptografia. Devido à sua baixa velocidade, a criptografia simétrica é usada quando o emissor de uma mensagem precisa criptografar pequenas quantidades de dados. A criptografia simétrica também é chamada criptografia de chave pública.
- III. Na Internet, O UDP (User Datagram Protocol) é um protocolo de transporte que presta um serviço de comunicação não orientado a conexão e sem garantia de entrega. Portanto, as aplicações que utilizam este tipo de protocolo devem ser as responsáveis pela recuperação dos dados perdidos.
- IV. Os servidores de diretório responsáveis por prover informações como nomes e endereços das máquinas são normalmente chamados servidores de nomes. Na Internet, os serviços de nomes usado é o Domain Name System (DNS). O DNS apresenta uma arquitetura cliente/servidor, podendo envolver vários servidores DNS na resposta a uma consulta.

Indique a opção que contenha todas as afirmações verdadeiras.

- a) I e II b) III e IV c) II e III d) I e III e) II e IV

03 - **(ESAF - Ministério do Planejamento, Orçamento e Gestão - 2006)** Uma assinatura digital é um meio pelo qual

- a) o gerador de uma mensagem, de um arquivo ou de outras informações codificadas digitalmente vincula sua identidade às informações.
- b) os servidores de e-mail substituem uma mensagem pelo equivalente codificado.
- c) os servidores de páginas da Web identificam o endereço IP do site de destino.
- d) os servidores de páginas da Web identificam o endereço IP do site de origem.
- e) os Firewalls utilizam para garantir o repúdio da informação.

04 - **(ESAF - Ministério do Planejamento, Orçamento e Gestão - 2006)** Quanto aos conceitos básicos de Segurança da Informação é correto afirmar que a criptografia simétrica

- a) usa um algoritmo de criptografia que requer que a mesma chave secreta seja usada na criptografia e na decriptografia.
- b) é um método de criptografia no qual duas chaves diferentes são usadas: uma chave pública para criptografar dados e uma chave particular para decriptografá-los.
- c) é um método de criptografia no qual duas chaves diferentes são usadas: uma chave particular para criptografar dados e uma chave pública para decriptografá-los.
- d) é o processo de gravação de partes de um arquivo em setores contíguos de um disco rígido a fim de aumentar a segurança da informação.
- e) é o resultado de tamanho fixo, também chamado de síntese da mensagem, obtido pela aplicação de uma função matemática unidirecional a uma quantidade de dados arbitrária.

05 - **(ESAF - Técnico da Receita Federal - TRF - 2005)** Analise as seguintes afirmações relacionadas à criptografia.

- I. A criptografia de chave simétrica pode manter os dados seguros, mas se for necessário compartilhar informações secretas com outras pessoas, também deve-se compartilhar a chave utilizada para criptografar os dados.
- II. Com algoritmos de chave simétrica, os dados assinados pela chave pública podem ser verificados pela chave privada.
- III. Com algoritmos RSA, os dados encriptados pela chave pública devem ser decriptados pela chave privada.
- IV. Com algoritmos RSA, os dados assinados pela chave privada são verificados apenas pela mesma chave privada.

Indique a opção que contenha todas as afirmações verdadeiras.

- a) I e II b) II e III c) III e IV d) I e III e) II e IV

GABARITO

01 - D 02 - B 03 - A 04 - A 05 - D