Segurança da Informação – SIN

Prof. Pedro Carlos da Silva Lara
Instituto Superior de Tecnologia em Ciências da Computação de Petrópolis

Lista de Exercícios 4

Questão 1) [ESAF - CGU 2012] Comparando a criptografia simétrica com a assimétrica, observa-se que

a) a primeira possui o problema do gerenciamento de chaves, ao passo que a segunda possui o problema da complexidade binária.
b) a primeira possui o problema da privacidade da chave universal, ao passo que a segunda possui o problema da criação e distribuição de chaves.
c) a primeira possui o problema da distribuição e gerenciamento de chaves, ao passo que a segunda possui o problema do desempenho.
d) a primeira possui o problema do desempenho em redes sem fio, ao passo que a segunda possui o problema do desempenho em ambientes corporativos.
e) a primeira possui o problema do desempenho, ao passo que a segunda possui o problema da geração de chaves.

Questão 2) [ESAF - CGU 2012] Sobre criptografia, considere:

I. A criptografia simétrica é um tipo de criptografia que usa um par de chaves criptográficas distintas (privada e pública) e matematicamente relacionadas.

II. A criptografia assimétrica é um tipo de criptografia que usa uma chave única para cifrar e decifrar dados.

III. A chave pública está disponível para todos que queiram cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente; a chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.

Está correto o que se afirma em
a) I e II, apenas.
b) I e III, apenas.
c) II e III, apenas.
d) I, II e III.
e) III, apenas.

Questão 3) [TRT-PE 2012] No que tange à segurança, existem duas classes de algoritmos criptográficos, caracterizadas a seguir.

1- utiliza uma mesma chave tanto para cifrar como para decifrar uma mensagem, ou seja, a mesma chave utilizada para "fechar o cadeado" é utilizada para "abrir o cadeado".

2- utiliza chaves distintas, uma para cifrar e "fechar" e outra para decifrar e "abrir", sempre geradas aos pares.

As classes descritas caracterizam algoritmos criptográficos conhecidos, respectivamente, como:
a) absolutos e relativos
b) simétricos e assimétricos
c) de chave pública e de chave secreta
d) de assinatura assimétrica e de assinatura simétrica
e) de cifras de transposição e de cifras de substituição

Questão 4) [MPE - AP 2012] De acordo com o tipo de chave usada, os métodos criptográficos podem ser subdivididos em duas grandes categorias:

a) Autoridade Certificadora (AC) e Autoridade de Registro (AR).
b) criptografia de chave pública e criptografia de chave privada.
c) certificação digital e certificação analógica.
d) assinatura digital e certificado digital.
e) criptografia de chave simétrica e criptografia de chaves assimétricas.

Questão 5) [MPE-PE 2012] É um algoritmo que faz uso intenso das operações de aritmética modular, que se tornou quase um sinônimo de criptografia. Na criptografia com esse algoritmo, uma mensagem (representada por um número inteiro) m é primeiramente elevada à uma potência e usando-se aritmética de módulo n, ou seja, C = me mod n.

O algoritmo citado acima é conhecido como

a) X.509.
b) RSA.
c) AES.
d) DES.
e) RC4.

Questão 6) [TRE-SP 2012] A criptografia assimétrica baseia-se na utilização de duas chaves, sendo uma mantida secreta, enquanto outra pode ser divulgada publicamente.

Com relação ao tema, analise as asserções a seguir.

Maria criptografa a mensagem (texto claro) utilizando-se da chave privada de João. A mensagem cifrada é então enviada a João que a decriptografa utilizando sua chave pública. Como a criptografia assimétrica trabalha com funções matemáticas bidirecionais, João não conseguiria

decriptografar a mensagem usando sua chave privada

PORQUE

Apenas a chave pública permite essa decriptografia, já que é gerada por algoritmos criptográficos assimétricos como o DES, 3DES ou AES e é de conhecimento de ambos os envolvidos na troca de mensagens.

Acerca dessas asserções, é correto afirmar:

a) As duas asserções são proposições verdadeiras, e a segunda é a justificativa correta da primeira.
b) As duas asserções são proposições verdadeiras, mas a segunda não é a justificativa correta da primeira.
c) A primeira asserção é uma proposição falsa, e a segunda, uma proposição verdadeira.
d) A primeira asserção é uma proposição verdadeira, e a segunda, uma proposição falsa.
e) Tanto a primeira quanto a segunda asserções são proposições falsas.

Questão 7) [**BNDES - 2010**] Um usuário mal-intencionado obteve, além do tipo de algoritmo utilizado na criptografia, a chave pública de João, quando este iniciou uma comunicação criptografada (algoritmo assimétrico) com Marcela. De posse dessa chave pública e do algoritmo, o usuário mal-intencionado

a) pode ler o conteúdo das mensagens enviadas de João a Marcela, mas não o inverso.
b) pode ler o conteúdo das mensagens enviadas de Marcela a João, mas não o inverso.
c) não tem acesso ao conteúdo das mensagens de posse desses itens.
d) consegue obter a chave privada a partir de ataques de dicionário.
e) consegue obter a chave privada utilizando ataques de criptoanálise.

Questão 8) [**CGU - 2012**] Com relação ao processo de verificação de assinatura digital, tem-se que o algoritmo de assinatura digital é aplicado sobre a assinatura digital recebida, usando a chave pública do remetente, o que resulta no resumo criptográfico da mensagem; em seguida, o algoritmo de hash é aplicado na mensagem recebida. A assinatura digital é válida se

a) os dois resumos obtidos forem simétricos.
b) os dois certificados digitais forem iguais.
c) o resumo obtido na recepção for o hash do resumo original.
d) os dois resumos obtidos forem iguais.
e) as chaves públicas forem diferentes.

Questão 9) Sobre assinaturas digitais, considere:

I. Consiste na criação de um código, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada.

II. Se José quiser enviar uma mensagem assinada para Maria, ele codificará a mensagem com sua chave pública. Neste processo será gerada uma assinatura digital, que será adicionada à mensagem enviada para Maria. Ao receber a mensagem, Maria utilizará a chave privada de José para decodificar a mensagem.

III. É importante ressaltar que a segurança do método de assinatura digital baseia-se no fato de que a chave pública é conhecida apenas pelo seu dono. Também é importante ressaltar que o fato de assinar uma mensagem não significa gerar uma mensagem sigilosa.

Está correto o que consta em

a) I e III, apenas.
b) I, II e III.
c) II e III, apenas.
d) I, apenas.
e) I e II, apenas.

Questão 10) A assinatura digital é um mecanismo que usa o conceito de chaves públicas para autenticar a origem de um determinado arquivo digital. Considerando que um usuário deseja verificar a validade de uma assinatura $\mathcal{A}$ de um arquivo x, marque a **única** resposta certa:

a) O usuário necessita da chave privada do usuário que assinou. Então ele verifica a assinatura usando o *hash* h do arquivo x. Se forem iguais aceita a assinatura.
b) O usuário necessita da chave pública do usuário que assinou. Assim ele calcula o *hash* h do arquivo x e depois decriptografa a assinatura $\mathcal{A}$ com a chave pública do usuário que assinou gerando um valor h'. Assim ele compara com o hash h com o valor h'. Se $h = h'$ aceita a assinatura. Se forem diferentes a assinatura é inválida.
c) O usuário necessita da chave pública do usuário que assinou. Assim ele tenta decifrar o arquivo x usando chave pública do usuário que assinou o arquivo. Depois de decifrar o aquivo x, ele compara com o hash h.
d) O usuário necessita da chave pública do usuário que assinou. Assim ele calcula o *hash* h do arquivo x e depois criptografa o *hash* h com a sua chave privada. Se for igual a assinatura $\mathcal{A}$ ele aceita a assinatura. Senão, rejeita a assinatura.

Questão 11) [**Perito Criminal Federal - PF (2004)**] Analise as afirmações abaixo:

- Cada uma das chaves pública e privada de um criptossistema RSA são formadas por dois números inteiros denominados expoente e módulo, ambos devendo ser números primos.
- O algoritmo criptográfico DES é uma cifra de substituição que mapeia um bloco de texto claro de 64 bits em um outro bloco de criptograma de 64 bits.
- O DES e o seu sucessor como padrão de criptografia do governo norte-americano, o AES, são cifradores de bloco que obedecem o esquema geral de cifradores de Feistel. Nesses cifradores, os blocos cifrados são divididos em metades (lado esquerdo e lado direito) de

mesmo tamanho, que são processadas independentemente, a cada rodada de cifração. Esse processo faz que apenas metade dos bits do bloco cifrado sofra influência da chave, em cada rodada, introduzindo confusão no processo criptográfico.

- MD5 e SHA-1 são funções de resumo de mensagem (funções hash). Esses algoritmos têm a finalidade de garantir a integridade e a autenticidade para mensagens de tamanho arbitrário.

Assinale a alternativa correta para as respectivas afirmações (**V** verdadeiro e **F** falso).

a) F–V–V–F
b) V–F–V–F
c) F–F–V–V
d) F–V–F–F
e) V–V–F–F

Questão 12) [Analista de Suporte – Finep 2011] Um certificado de chave pública (certificado digital) é um conjunto de dados à prova de falsificação e que atesta a associação de uma chave pública a um usuário final. Essa associação é garantida pela Autoridade Certificadora (AC) que emite o certificado digital após a confirmação da identidade do usuário. Com relação ao certificado emitido por uma AC, sua integridade e autenticidade são conferidas APENAS de posse da
a) assinatura digital presente no certificado.
b) assinatura digital presente no certificado e da chave pública da AC.
c) assinatura digital presente no certificado e da chave privada da AC.
d) assinatura digital presente no certificado e das chaves pública e privada da AC

Questão 13) [INMETRO - 2010] 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.

Questão 14) [TJ-MG 2012] Um certifcado digital para servidor web é uma credencial que identifca uma entidade e pretende criar um canal criptográfco seguro entre o navegador do usuário e o servidor da entidade. São características de um certifcado digital para servidor web, EXCETO:
a) Utiliza criptografa simétrica e assimétrica.
b) Composto por um par de chaves (chave pública e chave privada) assinado por uma autoridade certifcadora.
c) Proporciona disponibilidade, integridade, confdencialidade e autenticidade.
d) Habilita a comunicação através de https entre o navegador e o servidor web.

Questão 15) [TRE-CE 2012] No processo de assinatura digital, após gerar o ...I.., ele deve ser criptografado através de um sistema de ...II... , para garantir a ...III..... e a ...IV.... . O autor da mensagem deve usar sua ...V... para assinar a mensagem e armazenar o ...VI..... criptografado junto à mensagem original.

As lacunas I, II, III, IV, V e VI são preenchidas correta e respectivamente por

a) hash, chave pública, autenticação, irretratabilidade, chave privada e hash
b) digest, criptografia, confidencialidade, autenticidade, chave privada e digest
c) resumo, encriptação, autenticidade, integridade, chave privada e resumo
d) algoritmo, embaralhamento, irretratabilidade, integridade, chave privada e hash
e) hash, chave privada, autenticação, irretratabilidade, chave pública e hash

Questão 16) Descreva o algoritmo MAC-CBC. Explique também o processo de verificação.