Segurança da Informação – SIN

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

Lista de Exercícios 5

1)[**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
e) assinatura digital presente no certificado e do certifica- do e chave privada da AC

2)[**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.

3)[**FINEP - 2011**] Analise as seguintes afirmações relativas à Autoridade Certificadora (AC):

I. Depois de gerados, os certificados digitais perdem o vínculo com a Autoridade Certificadora (AC) que o emitiu.

II. Uma Autoridade Certificadora (AC) é a entidade responsável por emitir certificados digitais que podem ser para: pessoa, computador, departamento de uma instituição, instituição, etc.

III. Qualquer entidade que tenha a capacidade para gerar uma assinatura digital torna-se uma Autoridade Certificadora (AC), fazendo o papel de "Cartório Eletrônico".

IV. Quando se envia um e-mail importante, pode-se utilizar o certificado digital para assinar "digitalmente"a mensagem, de modo a assegurar ao destinatário a origem do e-mail e que este não foi adulterado entre o envio e o recebimento.

Estão corretos os itens:

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

4)[**Casa da Moeda - 2012**] O Hash Message Authentication Code (HMAC) pode ser utilizado para autenticar mensagens. Esse esquema de autenticação combina o algoritmo de resumo de mensagem com a(o)

a) chave pública
b) chave privada
c) chave secreta
d) assinatura digital
e) certificado digital

5)[**Casa da Moeda - 2012**] A Autoridade Certificadora (AC) é a entidade da Infraestrutura de Chaves Públicas (ICP), que é responsável por emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular. Esses certificados digitais são

considerados à prova de falsificação, pois são

a) assinados digitalmente e unicamente pela AC
b) assinados digitalmente em conjunto pela AC e pelo titular
c) criptografados unicamente pela AC
d) criptografados em conjunto pela AC e pelo titular
e) criptografados e assinados digitalmente em conjunto pela AC e pelo titular

6)[**Casa da Moeda - 2012**] O processo de autenticação de usuários é um método eficaz para proteger o acesso indevido de pessoas a computadores, sistemas operacionais, softwares, redes e ambientes físicos. Um sistema que utiliza um processo de forte autenticação deve verificar algo que o usuário sabe, algo que ele possui e algo que ele é. Para acessar o sistema, nessa ordem de verificação, um usuário legítimo deve fornecer os seguintes itens pessoais:

a) senha pessoal, token com a chave pública e digital
b) senha pessoal, token com o certificado digital e digital
c) senha pessoal, token com a chave privada e digital
d) chave privada, token com a senha pessoal e certificado digital
e) chave pública, token com a senha pessoal e certificado digital

7)[**Fiocruz - 2010**] A respeito do controle de acesso a redes e aplicações, assinale, dentre as alternativas a seguir, a única que contém a ordem correta dos procedimentos lógicos atravessados por um usuário para acessar um recurso:

a) Autenticação, Identificação, Autorização e Auditoria.
b) Identificação, Autenticação, Autorização e Auditoria.
c) Autorização, Identificação, Autenticação e Auditoria.
d) Autorização, Autenticação, Identificação e Auditoria.
e) Bloqueio, Autenticação, Autorização e Auditoria.

8)[**MPU - 2007**] NÃO é um método de reconhecimento utilizado nos mecanismos de autenticação biométrica:

a) assinatura digital.
b) impressão digital.
c) pressionamento de tecla.
d) óptico.
e) facial.

9)[**Petrobrás - 2010**] Analise o texto a seguir. Ato de averiguar a identidade de uma entidade do sistema (por exemplo, usuário, sistema, ponto de rede) e a elegibilidade da entidade para acessar a informação disponível em computadores. Designado para proteção contra atividades fraudulentas no logon, esse ato também pode se referir à verificação da correção de um dado. O texto acima trata do conceito de

a) autenticação.
b) autorização.
c) assinatura digital.
d) certificado digital.
e) função de hash.

10)[**Petrobrás - 2010**] Duas entidades, P e Q, desejam se comunicar por meio de um canal seguro e, para isso, decidem utilizar uma terceira entidade de confiança, X, para a criação deste canal. Ambas as entidades já possuem a chave pública de X e confiariam em uma assinatura dessa entidade. Nesse contexto, considere os seguintes passos executados para a estabelecimento do canal:

1. P requisita a X a chave pública de Q.
2. X pega a chave pública verificada de Q, nos seus bancos de dados, e assina essa chave atestando sua legitimidade.
3. X envia para P a chave junto com a assinatura.
4. P verifica a assinatura de X, certifica-se de que tudo está correto e aceita essa chave de Q como autêntica.
5. P usa sua chave particular para encriptar a chave pública de Q e envia o resultado para Q.
6. Q usa sua chave particular para desencriptar a chave enviada por P.
7. P e Q passam a usar um algoritmo simétrico com a chave enviada por P para trocar as mensagens.

Considerando os objetivos de P e Q e analisando os passos por eles executados, conclui-se que, para atender às necessidades de P e Q

a) os passos descritos estão corretos.
b) o passo 5 deve ser modificado para: P escolhe, aleatoriamente, uma chave de seção e usa a chave pública de Q para encriptar a chave escolhida e envia o resultado para Q.
c) o passo 6 deve ser modificado para: Q usa sua chave pública para desencriptar a chave enviada por P.
d) os passos 1 a 7 devem ser modificados, substituindo-se as referências "chave pública"de Q por sua "chave particular"e "chave particular"de Q, por sua "chave pública".
e) o passo 7 deve ser modificado para: P e Q passam a usar um algoritmo assimétrico com a chave enviada por P para trocar as mensagens.