Segurança da Informação – SIN

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

Lista de Exercícios 1

1) Caracterize as seguintes situações como: **Ataque Passivo** ou **Ataque Ativo**
a) Um usuário lê os emails de outro usuário sem a permissão.
b) Um usuário se passa por outro usuário em uma troca de mensagem.
c) Um usuário interrompe a comunicação de outros dois usuários.

2) Considere os seguintes ataques em um canal de comunicação: fabricação, interrupção, interceptação e modificação de mensagens. Para cada ataque caracterize o serviço de segurança da informação que é violado.

3)[**TRE/GO - 2009**] É um tipo de ataque passivo às transmissões de dados por meio de redes de computadores o de

a) falsidade.
b) negação de serviço.
c) análise de tráfego.
d) repetição.
e) modificação de mensagem.

4) Considere a mensagem cifrada y = OPCMTDUARSOE usando a criptografia de **Permutação** ou **Transposição** com chave de tamanho $|k| = 4$. Considerando que a chave é da forma

$$k = (3, k_2, k_3, k_4),$$

Obtenha o restante da chave $\{k_2, k_3, k_4\}$ e o texto plano x.

5) Dada as cifras $E_k(x)$ criptografe o valor $x = 32$ e a chave $k = 20$. Após criptografar x descreva a função $E_k^{-1}(y)$. Verifique se $E_k^{-1}(E_k(x)) = x$.

a) $E_k(x) = x + k$
b) $E_k(x) = x \cdot k$
c) $E_k(x) = \frac{2}{k} + 5x$
d) $E_k(x) = 2(x + k)$

6) [**INMETRO - 2010**] Com relação aos requisitos de segurança da informação, assinale a opção correta.

a) A integridade é diretamente obtida quando se tem a confidencialidade.
b) A disponibilidade não é afetada pela obtenção da integridade e da confidencialidade.
c) A integridade requer que a informação só seja acessada por quem estiver autorizado.
d) A confidencialidade garante que a informação não será alterada por quem não estiver autorizado.
e) A adição da integridade a um sistema com confidencialidade eleva o seu nível de segurança.

7) [**TRE/GO - 2009**] A capacidade de assegurar a prevenção ao acesso e à manipulação ilegítima da informação, ou ainda, de evitar a interferência indevida na sua operação normal pode ser interpretado como segurança computacional. A figura acima representa os três elementos fundamentais que definem os objetivos de segurança. Nessa figura, os identificadores #1 e #2 correspondem, respectivamente, a

a) confiabilidade e a redundância. A confiabilidade é a garantia de que a informação não é disponibilizada a usuários, programas e processos que não são autorizados.
b) integridade e a confidencialidade. A integridade é um mecanismo de segurança que protege os dados e recursos de serem alterados de forma não autorizada.
c) confidencialidade e a criptografia.
d) confiabilidade e a integridade. Alguns mecanismos de segurança que fornecem a confiabilidade são a criptografia, controle de acesso lógico e físico, protocolos de transmissão, visões de banco de dados e controle de fluxos de tráfego.

8) [**SEFAZ/RJ - 2011**] Segurança da Informação é um tema que se reveste atualmente de alta importância para os negócios. Um de seus aspectos mais relevantes

está associado à capacidade do sistema de permitir que alguns usuários acessem determinadas informações e paralelamente impede que outros, não autorizados, a vejam. O aspecto abordado é denominado

a) Integridade.
b) Privacidade.
c)Confidencialidade.
d)Vulnerabilidade.
e) Disponibilidade.

9) [**TJ/SE - 2009**] Sobre criptologia é INCORRETO afirmar:

a) A decifração é quando se recupera um texto original conhecendo o algoritmo criptográfico.
b) A ocultação de informações pode acontecer de duas formas diferentes: esteganografia e criptografia.
c) Os códigos e as cifras podem ser métodos criptográficos do tipo transposição.
d) A criptoanálise é quando se recupera um texto original sem conhecer o algoritmo criptográfico.
e) A criptologia se ocupa da ocultação de informações e da quebra dos segredos da ocultação.

10) [**MPE/BA - 2011**] Com relação a criptografia simétrica, é correto afirmar:

a) A criptografia de chave simétrica pode manter os dados seguros, mas, se for necessário compartilhar informações confidenciais com outras pessoas, também se deve compartilhar a chave utilizada para criptografar os dados.
b) A criptografia de chave simétrica é um método de codificação que utiliza uma chave pública e uma chave privada para codificar e decodificar a mesma informação.
c) A criptografia de chave simétrica é um método de codificação que utiliza duas chaves públicas para codificar e decodificar a mesma informação.
d) A criptografia de chave simétrica é um método de codificação que utiliza uma chave pública e duas privadas para codificar e decodificar a mesma informação.
e) Os algoritmos de chave simétrica têm como principal característica a possibilidade de utilização de assinatura digital e de certificação digital, sem alteração da chave.

11) [**TRE/RN - 2011**] Com a criptografia simétrica, um requisito fundamental para que duas partes se comuniquem com segurança é

a) que haja um cabeamento adequado que evite invasões.
b) estabelecer comunicação apenas na camada host/rede.
c) a existência de um monitoramento de rede eficaz e online.
d) elas compartilharem duas chaves públicas, porém cada uma em um período diferente do dia.
e) elas compartilharem uma chave secreta.