Sistemas Distribuídos - UCSAL
Professor : **Marco Antônio C. Câmara -** 3ª Lista de Exercícios

Aluno(a) : _____

(fonte : Aval.Segurança Informação UCSAL 2013-1)

1ª Questão : Em um computador pessoal de sua residência, um usuário instala um software (A)ntivírus e um software de (B)ackup, além de garantir a a(T)ualização frequente do Sistema Operacional e utilizar a autenticação dos usuários autorizados através de nome de usuário e (S)enha.

Com base no seu conhecimento dos pilares da Segurança da Informação (*Confidencialidade, Integridade, Disponibilidade, Autenticidade e Não-Repúdio*), que recursos você associaria a cada um dos pilares listados abaixo? (é possível que existam pilares não associados a nenhum recurso, ou pilares associados a mais de um recurso.

Confidencialidade: ( ) ( ) ( ) ( ) Integridade: ( ) ( ) ( ) ( )

Disponibilidade: ( ) ( ) ( ) ( ) Autenticidade: ( ) ( ) ( ) ( )

Não-Repúdio: ( ) ( ) ( ) ( )

(fonte : Lista Professor Alisson Cleiton- internet)

2ª Questão : Analise as seguintes afirmações relacionadas à criptografia, e indique, ao final, a opção que contenha todas as afirmações verdadeiras:

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

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

(fonte : Lista de Exercícios Segurança de Redes UCSAL 2011-2)

3ª Questão : Associe cada uma das afirmativas aos algoritmos de (S)ubstituição, (T)ransposição, (C)have Pública/Privada. Podem existir associações de até dois algoritmos a cada afirmativa. Caso a afirmativa não se ajuste a nenhum dos algoritmos, assinale a mesma com a letra (X):
( ) Pelo menos parte da chave deve ser de conhecimento exclusivo de uma partes envolvidas na comunicação;
( ) Não ocorre troca dos caracteres utilizados na mensagem cifrada;
( ) A quebra da cifra envolve a análise de frequência de ocorrência de caracteres no alfabeto da linguagem utilizada;
( ) Quanto maior a chave, mais seguro;
( ) A chave tipicamente é numérica;
( ) Também chamada de cifra de César;
( ) Criada nos últimos 100 anos.

(fonte : 2ª Avaliação Segurança de Redes 2011-2)

( ) **4ª Questão :** Utilizando o seu conhecimento sobre os métodos de criptografia estudados, escreva ao lado a soma das alternativas corretas. **Cada alternativa falsa considerada correta anula uma alternativa correta que tenha sido considerada. Portanto, não considere como certas alternativas duvidosas.**

(01) Um algoritmo de criptografia simétrico pode ser implementado de forma segura se não houver compartilhamento da chave pelo emissor e receptor.
(02) Um algoritmo de criptografia precisa se preocupar em garantir a atualidade das mensagens principalmente pelo surgimento, a cada dia, de novas técnicas de decriptografia.
(04) Algoritmos baseados na cifra de César normalmente são quebrados com base na análise da frequência de ocorrência de caracteres no alfabeto da linguagem e tipo de mensagem utilizada.
(08) A criptografia por transposição envolve a troca dos caracteres da mensagem original pelos caracteres correspondentes com base no código ASCII utilizado.
(16) Embora tenha ocorrido grande evolução dos algoritmos de criptografia nas últimas décadas, principalmente devido ao surgimento dos computadores, a criptografia já era utilizada a séculos por diversas civilizações.
(32) A cifra de César básica tem como chave um número inteiro.
(64) Nos algoritmos assimétricos, cada dispositivo possui duas diferentes chaves.

(fonte : Lista de Exercícios Segurança de Redes UCSAL 2011-2)

5ª Questão : Com base no seu conhecimento sobre o algoritmo de criptografia RSA, responda:

a) Qual a complexidade numérica envolvida em uma possível tentativa de decriptografia deste método?
b) Supondo ser possível executar o procedimento do item anterior, existe alguma outra dificuldade envolvida na decriptografia? Qual é?
c) Sendo o método numérico, que procedimento pode ser realizado para criptografar uma sequência alfanumérica?
d) Qual o papel da "entidade certificadora" neste método?

(fonte : Lista de Exercícios Segurança de Redes UCSAL 2011-2)

6ª Questão: Explique a diferença entre entre um algoritmo de "Criptografia Simétrico" e "Criptografia Assimétrica":

(fonte : Lista de Exercícios Segurança de Redes UCSAL 2011-2)

7ª Questão: O nome da minha empresa é XYZ Informática, situada na Av. Tancredo Neves em Salvador. Qual será o possível nome do meu domínio: (*as perguntas abaixo podem ter mais de uma resposta correta, uma única resposta correta ou nenhuma resposta correta*)

a) ( ) WWW.XYZ.COM.BR
b) ( ) XYZ.COM.BR
c) ( ) XYZ.BR
d) ( ) XYZ.INF.BR

(fonte : 1ª Avaliação Segurança de Redes 2011-2)

8ª Questão : Com base nos conhecimentos adquiridos em sala de aula, cada um dos 3 pilares básicos da segurança da informação – (C)onfidencialidade, (I)ntegridade e (D)isponibilidade - podem ser aplicados em 3 pontos específicos. Associe as letras acima aos pontos onde os pilares tipicamente são aplicados (é admissível a marcação de mais de uma letra por alternativa):

a) Usuário (C) (I) (D)

b) Serviço (C) (I) (D)

c) Tráfego (C) (I) (D)

(fonte : 1ª Avaliação Segurança de Redes 2011-2)

( ) **9ª Questão :** Utilizando o seu conhecimento sobre os controles tipicamente aplicáveis em um ambiente distribuído visando a Segurança da Informação, escreva ao lado a soma das alternativas corretas. **Cada alternativa falsa considerada correta anula uma alternativa correta que tenha sido considerada. Portanto, não considere alternativas duvidosas.**

(01) Os IDSs (*Intrusion Detection Systems*) analisam o tráfego da rede, localizando padrões anormais ou suspeitos, permitindo assim detectar riscos de intrusão.
(02) Normalmente os IDS são instalados apenas na fronteira entre a rede local e a Internet.
(04) Mecanismos de Controle de Conteúdo (*Content Filtering*) permitem determinar regras para liberação de páginas WEB para grupos de usuários.
(08) A criptografia de tráfego, que atua basicamente sobre a Integridade e a Confidencialidade da informação, aumenta a segurança na utilização de meios físicos públicos para envio de mensagens privadas.
(16) A biometria é uma das técnicas utilizadas na construção de sistemas de autenticação forte.
(32) A utilização de *firewalls* pode eliminar a necessidade de sistemas de autenticação.
(64) A diferença fundamental entre o IDS (*Intrusion Detection Systems*) e o IPS (*Intrusion Prevention Systems*) é que o segundo é capaz de atuar sobre o problema, bloqueando determinados eventos.

( ) **10a Questão :** Com base no seu conhecimento sobre a primitiva de requisição/resposta *doOperation* na invocação remota de processos estudados em Sistemas Distribuídos, escreva ao lado a soma das alternativas corretas. **Cada alternativa falsa considerada correta anula uma alternativa correta que tenha sido considerada. Portanto, não considere alternativas duvidosas**.

(01) É bloqueado durante a execução remota do processo no servidor.
(02) É executado no servidor.
(04) Implementa a devolução da mensagem de resposta do servidor após a execução remota do processo.
(08) Implementa o envio da mensagem de requisição de execução remota do processo.
(16) Se comunica com a primitiva *getRequest*.