



Iniciado em segunda, 19 set 2022, 16:16

Estado Finalizada

Concluída em segunda, 19 set 2022, 17:26

Tempo 1 hora 9 minutos

Empregado

Avallar 10,0 de um máximo de 10,0(100%)

Questão 1

Correto

Atingiu 0,5 de 0,5

Marcar questão

Considere um grupo de N pessoas que se comunicam entre si usando criptografia simétrica. Todas as comunicações entre quaisquer duas pessoas do grupo também são visíveis para as demais. Nenhuma outra pessoa fora deste grupo pode decifrar as mensagens trocadas. Com base nisto, analise as afirmações abaixo e marque a alternativa correta.

- I - O sistema como um todo requer o uso de apenas duas chaves.
- II - Se a criptografia utilizada fosse assimétrica, seriam necessários N pares de chaves (pública e privada).
- III - Neste sistema não há problema com a distribuição das chaves, já que as pessoas são conhecidas.

Escolha uma opção:

- a. Todas as afirmações são verdadeiras.
- b. Somente II e III são falsas.
- c. Somente I e II são falsas.
- d. Somente I e III são falsas.
- e. Todas as afirmações são falsas.

A resposta correta é: Somente I e III são falsas.

Questão 2

Completo

Atingiu 0,5 de 0,5

Remover marcação

Um aluno entra no computador do laboratório e digita o seguinte endereço no browser: <http://ohio.infoway.vista.edu/chamex.html>. Explique como o servidor DNS do laboratório consegue descobrir o endereço IP da máquina que contém o arquivo chamex.html. Na resposta, apontar os hosts DNS envolvidos e explicar passo a passo como ocorre a resolução de endereços nesse caso.

Quando um cliente (browser) insere um endereço de nomes para ser resolvido para um IP, a primeira coisa que esse cliente faz é encaminhar o nome (<http://ohio.infoway.vista.edu/chamex.html>) para o DNS Server. O DNS server - que vai resolver o nome para um IP - sabe onde está o host DNS chamado **root**, que é o primeiro na árvore de resolução de DNS.

Assim, o DNS Server começa a perguntar para cada host DNS uma parte do nome a ser resolvido. Esse processo é de trás pra frente (da direita para a esquerda). Portanto, o DNS Server pergunta ao DNS host **root** qual o endereço do DNS host **edu**. Então, o DNS host **root** responde para o DNS Server onde está localizado o DNS host **edu**.

Em seguida, o DNS Server pergunta ao DNS host **edu** onde é que está o DNS host **vista**. Então, o DNS host **edu** responde para o DNS Server onde está localizado o DNS host **vista**. Depois, o DNS Server pergunta ao DNS host **vista** qual o endereço do DNS host **infoway**. Então, o DNS host **vista** responde para o DNS Server onde está localizado o DNS host **infoway**.

Logo após, o DNS Server pergunta ao DNS host **infoway** onde está o DNS host **ohio**. Então, o DNS host **infoway** responde para o DNS Server onde está localizado o DNS host **ohio**.

Por fim, é no IP do DNS host **ohio** em que a página **chamex.html** vai estar armazenada. Com isso, usando o protocolo HTTP do cabeçalho da URL, transfere-se a página **chamex.html** do servidor **ohio.infoway.vista.edu** para o browser do aluno que acessou o endereço em seu computador do laboratório.

Passo a passo:

1. Azul
2. Laranja
3. Roxo
4. Verde
5. Rosa
6. Vermelho

Comentário:

Questão 3

Correto

Atingiu 0,5 de 0,5

Marcar questão

Folha de São Paulo - 14/02/2008 - 11h33

Petrobras confirma furto de informações sigilosas

"A Petrobras confirmou nesta quinta-feira que dados sobre pesquisas sísmicas, que podem incluir a descoberta de petróleo e gás, foram furtados de um container da empresa. Segundo a estatal, as informações eram sigilosas e relevantes. A Petrobras informou apenas que o furto foi feito de uma empresa terceirizada prestadora de serviços, mas não citou nomes. Segundo fontes ouvidas pela Folha Online, o container era transportado pela norte-americana Halliburton.

Segundo a Petrobras, o furto ocorreu no início deste mês e a investigação está sob sigilo. Uma missão especial da Polícia Federal no Rio, em conexão direta com o comando da PF em Brasília, estária no caso.

Na ocasião do crime, o container da Halliburton se dirigia a Macaé (RJ), rumo à base de operações da estatal na Bacia de Campos, transportando equipamentos, quando ocorreu o furto dos dados, que estariam em um disco rígido e computadores portáteis.

A estatal não informou detalhes sobre o conteúdo dos dados roubados, nem se continham números sobre o megacampo de Tupi, na Bacia de Santos. A Petrobras também evitou comentar detalhes do furto, mas disse que possui cópias das informações."

De acordo com o texto acima, marque a opção correta.

Escolha uma opção:

- a. O roubo das informações caracterizou um ataque ao serviço de disponibilidade da Petrobrás.
- b. Pelo texto acima, fica claro que os computadores portáteis da Petrobrás permitem o acesso de pessoas não autorizadas.
- c. A integridade dos dados das pesquisas feitas pela Petrobrás foi atingida neste roubo.
- d. Uma forma da Petrobrás garantir a confidencialidade dos dados, seria a utilização de mecanismos de criptografia.
- e. De acordo com o exposto, pode-se concluir que o transporte dos equipamentos da Petrobrás não apresenta vulnerabilidades.

A resposta correta é: Uma forma da Petrobrás garantir a confidencialidade dos dados, seria a utilização de mecanismos de criptografia.

Questão 4

Correto

Atingiu 0,5 de 0,5

Marcar questão

De acordo com as características do algoritmo DES, analise as afirmações abaixo e assinale a opção correta.

I - As tabelas de permutação (P-boxes) são utilizadas para se fazer transposições entre os bits de um bloco, onde algumas delas são voltadas para expansão e outras utilizadas para se fazer contracção.
II - Apesar da chave ser 64 bits, apenas 56 deles são utilizados e ela não sofre mudanças durante todo o processo de encriptação.
III - Em cada uma das 16 rodadas do algoritmo, a chave sofre uma adição de 1 ou 2 bits, dependendo da rodada.

Escolha uma opção:

- a. Somente I e III são verdadeiras.
- b. Somente II é verdadeira.
- c. Todas as afirmações são verdadeiras.
- d. Somente II e III são falsas.
- e. Todas as afirmações são falsas.

A resposta correta é: Somente II e III são falsas.

Navegação do questionário

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18				

Mostrar uma página por vez

Terminar revisão

