PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Instituto de Ciências Exatas e Informática
Segurança de Redes de Computadores
Prof. Marco Antonio da Silva Barbosa

Lista de Exercícios de Segurança de Redes de Computadores.

1. Explique com suas palavras o conceito de criptografia.

2. Defina encriptação, decriptação e algoritmo de criptografia.

3. Os objetivos da criptografia são: confidencialidade, integridade, autenticidade e não-repúdio. Explique cada um deles.

4. Cite características, vantagens e desvantagens da criptografia simétrica.

5. Explique porque o algoritmo One Time Pad é dito ser um esquema de cifração perfeita e incondicional. Descreva seu funcionamento.

6. Qual é a diferença entre cifra incondicionalmente segura ou cifra computacionalmente segura.

7. Decifre a mensagem abaixo e descreva:

fnsktwrfynhfrjinxyfshntzitxqnawtxsftifqjnyzwf

(a) Qual cifra foi utilizada na criptografia.
(b) Qual o problema encontrado nesta cifra que facilitou a criptoanalise. Qual melhoria poderia ser aplicada para contornar este problema?
(c) Qual a chave utilizada na criptografia.

8. Usando a cifra Vigenère e a palavra chave coloportus decifre a mensagem abaixo:

cjtrpssxfs

9. Usando a cifra Playfair e a palavra chave portus decifre a mensagem abaixo:

Cngvgsrwpltlcnhpbckfry

10. A segurança em redes pode ser limitada a manter a integridade na transmissão de dados? Caso negativo, quais são os problemas que devem ser abordados?
11. Desenhe e explique o funcionamento do PGP.
12. Quais são os tipos de ataques existentes e quais prejuízos eles podem causar?
13. Cite pelo menos três técnicas de criptoanálise usada e suas características?
14. Cite e explique as técnicas de cifras de criptografia conhecidas.
15. Por que existe a necessidade de adicionar bits de redundância e atualidade nas técnicas de criptografia?
16. Desenhe a estrutura dos algoritmos de chave simétrica? Por qual motivo o 3DES implementa duas passagens de encriptografia e uma de desencriptografia e não as três passagens com encriptografia?

17. Descreva o funcionamento de cada modo de cifra e cite pelo menos uma desvantagem de cada método.
18. Qual é a principal restrição do método de criptografia com chave simétrica?
19. Desenhe e explique a estrutura dos algoritmos de criptografia de chave pública?
20. Classifique o DES, RSA, 3DES e AES em função de qual técnica de criptografia eles utilizam (chave simétrica ou assimétrica)
21. Se Alice deseja enviar uma mensagem com privacidade para Bob utilizando o algoritmo RSA, ela deve criptografar a mensagem utilizando a chave pública de Bob e ele deve descriptografá-la utilizando a sua chave privada. Entretanto, este algoritmo também poderia funcionar na direção contrária. Alice poderia criptografar a mensagem utilizando a sua chave privada e Bob poderia descriptografá-la utilizando a chave pública de Alice. Porque o RSA não é utilizado desta segunda forma?
22. O protocolo "MD5 com Chave" funciona da seguinte forma: Alice envia para Bob

    P + MD5 (P + k)

onde P é o texto original e k é uma chave já compartilhada entre Alice e Bob. Este protocolo provê assinatura digital? Justifique sua resposta.

23. Utilizando o MD5 com assinatura RSA, Alice pode mandar uma mensagem assinada para Bob da seguinte maneira:

    P + D_A(MD5(P))

Se Trudy modificar P, Bob consegue verificar isto. Mas, o que aconteceria se Trudy modificasse P e a assinatura?

24. Suponha que Bob e Alice já compartilham uma chave secreta, mas, mesmo assim, Alice precisa da chave pública de Bob. Explique como Bob poderia enviar sua chave pública para Alice com segurança (integridade).
25. Explique a necessidade de mecanismos de distribuição de chave pública. Porque estes mecanismos são necessários? Qual é a forma mais usual de fazer esta distribuição de forma segura?
26. Para evitar o ataque do homem-do-meio podemos usar os certificados emitidos pelas CA´s. Como isto funciona?
27. Aparentemente os algoritmos de chave assimétrica são mais interessantes que os de chave simétrica, por qual motivo eles não são usados em transmissões de grande volume de dados?
28. O IPsec pode ser utilizado na arquitetura AH e ESP, quais são as diferenças entre os dois? Qual técnica é utilizada por ambos para autenticar os dados transmitidos?
29. Diferencie os modos de operação do IPsec transporte e túnel? Qual dos dois é mais indicado para interligação de uma VPN e porque?
30. Acerca da Criptografia Simétrica de dados, julgue as afirmativas a seguir, se são verdadeiras ou falsas. Justifique as falsas.
    a. Na criptografia simétrica, o emissor e o receptor usam duas instâncias da mesma chave para cifrar e decifrar. Nesse tipo de criptografia, a chave deve ser mantida em segredo e protegida, pois a posse da chave possibilita decifrar mensagens cifradas com essa chave. Esse tipo de criptografia provê autenticação, pois, se duas pessoas usam a mesma chave, há como provar quem enviou cada mensagem.

b. Os sistemas de criptografia simétrica utilizam apenas uma chave, que é usada tanto para cifração quanto para decifração.
c. Uma premissa básica para a segurança dos algoritmos simétricos é a existência de uma forma segura de distribuição e guarda da chave compartilhada entre as partes que vão se comunicar.
d. A segurança de um sistema criptográfico depende, entre outros fatores: do segredo da guarda da chave ou das chaves; da dificuldade em se adivinhar ou tentar uma a uma as possíveis chaves; da dificuldade de se inverter o algoritmo de cifração sem conhecimento da chave; da existência ou não de formas de uma mensagem cifrada ser decifrada sem conhecimento da chave; da possibilidade de se decifrar uma mensagem cifrada conhecendo-se apenas como parte dela é decifrada; da possibilidade de se conhecer e usar propriedades das mensagens em claro para decifrar mensagens cifradas.
e. Atualmente, os sistemas criptográficos utilizados são incondicionalmente seguros por se basearem na dificuldade de resolução de problemas matemáticos específicos ou em limitações na tecnologia computacional vigente.
f. Em geral, um sistema criptográfico impede que dados sejam deletados, ou que o programa que o implementa seja comprometido.
g. 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.
h. 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.
i. O algoritmo DES (Data Encryption Standard) efetua exatamente as mesmas operações durante o processo de cifração e o de decifração. A única diferença percebida entre os dois processos está na ordem de aplicação das chaves parciais (chaves de round).
j. O AES (advanced encryption standard) surgiu com o objetivo de substituir o DES. Um dos principais motivos dessa necessidade de modificação de padrões está no fato de o tamanho do espaço de chaves utilizadas pelo DES (2^{64} possíveis chaves) não ser grande o suficiente, atualmente, para garantir proteção contra ataques do tipo busca por exaustão. O AES, com suas chaves de, no mínimo, 112 bits, aumentou tremendamente a resistência a esse tipo de ataque.
k. O AES (Advanced Encryption Standard) é o atual padrão de cifração de dados do governo norteamericano. Seu algoritmo criptográfico cifra blocos de até 128 bits utilizando, para isso, chaves de 32 bits, 64 bits ou 128 bits.
l. O modo de operação ECB (Electronic Codebook) não é adequado quando o texto em claro possui baixa entropia.
m. No modo CBC, é recomendável que seja escolhido um único vetor de inicialização para a cifração de diversas mensagens.
n. O modo de operação CBC é um dos mais utilizados para criptografar dados. Uma importante característica desse modo é o fato de se poder cifrar ou decifrar qualquer bloco de forma independente dos demais blocos, o que o torna ideal para cifrar arquivos que são acessados aleatoriamente.
o. Para a utilização do modo de operação CBC (Cipher Block Chaning Mode), é necessário que seja criado o que se denomina vetor de inicialização (initialization vector), que evita que mensagens que comecem idênticas gerem

criptogramas com começos idênticos. Um inconveniente desse modo de operação reside na questão da propagação de erros, pois, caso haja um bit errado em um bloco de criptograma a ser decifrado, todos os blocos a partir dali serão decriptografados de forma errada.

p. O algoritmo criptográfico RC4 tem como princípio de funcionamento o segredo criptográfico perfeito, em que a chave criptográfica deve ter o mesmo tamanho que a mensagem. Desse modo, no RC4, a chave de criptografia é a semente de uma sequência pseudo-aleatória que é usada para chavear os bytes cifrados em uma operação linear. A mensagem cifrada pode ser tão longa quanto o período da sequência gerada.

31. Acerca da Criptografia Assimétrica de dados e assinatura digital, julgue as afirmativas a seguir, se são verdadeiras ou falsas. Justifique as falsas.
    a. Na criptografia assimétrica, para garantir a confidencialidade de uma mensagem, quem envia a mensagem deve cifrá-la com a chave privada do destinatário da mensagem. Se a autenticação for o serviço desejado por quem envia a mensagem, este deve cifrá-la com sua chave pública.
    b. Na criptografia assimétrica, dados cifrados usando-se uma chave privada podem ser decifrados usando-se uma chave privada; dados cifrados usando-se uma chave pública podem ser decifrados usando-se uma chave pública; dados cifrados usando-se uma chave privada podem ser decifrados usando-se a correspondente chave pública; dados cifrados usando-se uma chave pública podem ser decifrados usando-se a correspondente chave pública.
    c. Do ponto de vista do custo computacional, os sistemas assimétricos apresentam melhor desempenho que os sistemas simétricos.
    d. Os sistemas de criptografia assimétrica utilizam duas chaves: uma pública, que é usada para cifração; e uma privada, que é usada para decifração.
    e. Em algoritmos de chave assimétrica, é factível a obtenção da chave privada a partir da pública com o uso de técnicas de engenharia reversa.
    f. Se duas cópias de um mesmo arquivo forem cifradas independentemente, uma com um algoritmo simétrico e a outra com um assimétrico, a primeira operação, normalmente, demorará menos que a segunda.
    g. Em geral, um sistema criptográfico impede que dados sejam deletados, ou que o programa que o implementa seja comprometido.
    h. A criptografia assimétrica requer menor esforço computacional que a simétrica.
    i. Tanto a criptografia simétrica quanto a assimétrica oferecem sigilo e integridade.
    j. A criptografia assimétrica utiliza duas chaves, uma pública e outra privada. Quando uma delas é usada para cifrar a outra é usada para decifrar.
    k. Um dos mais utilizados algoritmos de criptografia é o RSA, que se baseia na dificuldade de fatoração de números primos grandes e utiliza, por ser um algoritmo de ciframento assimétrico, um par de chaves (pública e privada) para cada usuário.
    l. 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.
    m. O algoritmo de criptografia assimétrica RSA (Rivest, Shamir e Adleman) tem sua segurança fundamentada na dificuldade de se fatorar números inteiros muito grandes. Além de ser utilizado para criptografar mensagens a serem enviadas por canais inseguros de comunicação, o RSA também pode ser aplicado na criptografia de chaves simétricas que são utilizadas na criptografia simétrica de mensagens.

n. Sistemas criptográficos simétricos AES, DES e RC4 são mais adequados ao estabelecimento de protocolos de não repúdio, quando comparados com algoritmos assimétricos, como RSA.
o. O criptossistema RSA tem por base o problema dos logaritmos discretos.
p. O criptossistema RSA é seguro caso o problema da fatoração de números inteiros seja intratável, ou seja, não exista um algoritmo de fatoração de tempo polinomial.
q. Em um processo de assinatura digital, comumente é gerado um valor condensado (hash) do documento que se deseja assinar e, após isso, esse valor é criptografado utilizando-se chave privada (assimétrica) que somente as partes envolvidas na comunicação desse documento devem conhecer. Dessa forma, ao enviar o documento original e o respectivo valor condensado criptografado, o destinatário poderá validar a assinatura do documento e verificar a sua integridade.
r. Na criptografia simétrica, o emissor e o receptor usam duas instâncias da mesma chave para cifrar e decifrar. Nesse tipo de criptografia, a chave deve ser mantida em segredo e protegida, pois a posse da chave possibilita decifrar mensagens cifradas com essa chave. Esse tipo de criptografia provê autenticação, pois, se duas pessoas usam a mesma chave, há como provar quem enviou cada mensagem.
s. Na criptografia assimétrica, para garantir a confidencialidade de uma mensagem, quem envia a mensagem deve cifrá-la com a chave privada do destinatário da mensagem. Se a autenticação for o serviço desejado por quem envia a mensagem, este deve cifrá-la com sua chave pública.
t. Para criar uma assinatura digital para uma mensagem, pode-se usar uma função hash para calcular um valor a partir do conteúdo da mensagem e criptografar esse valor usando-se a chave pública de quem enviou a mensagem. A partir desse valor é possível, na recepção, verificar por quem a mensagem foi remetida e se a mensagem recebida é diferente da enviada.