Pontifícia Universidade Católica de Minas Gerais
Bacharelado em Ciência da Computação
Redes de Computadores II – 1º Semestre de 2008
Prof. Marco Antonio da Silva Barbosa

1ª Questão
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?

2ª Questão
Desenhe e explique o funcionamento do PGP.

3ª Questão
Quais são os tipos de ataques existentes e quais prejuízos eles podem causar?

4ª Questão
Cite pelo menos três técnicas de criptoanálise usada e suas características?

5ª Questão
Cite e explique as técnicas de cifras de criptografia conhecidas.

6ª Questão
Por que existe a necessidade de adicionar bits de redundância e atualidade nas técnicas de criptografia?

7ª Questão
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?

8ª Questão
Descreva o funcionamento de cada modo de cifra e cite pelo menos uma desvantagem de cada método.

9ª Questão
Qual é a principal restrição do método de criptografia com chave simétrica?

10ª Questão
Desenhe e explique a estrutura dos algoritmos de criptografia de chave pública?

11ª Questão
Classifique o DES, RSA, 3DES e AES em função de qual técnica de criptografia eles utilizam (chave simétrica ou assimétrica)

12ª Questão
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?

13ª Questão
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.

14ª Questão
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?

15ª Questão
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).

16ª Questão
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?

17ª Questão
Para evitar o ataque do homem-do-meio podemos usar os certificados emitidos pelas CA´s. Como isto funciona?

18ª Questão
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?

19ª Questão
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?

20ª Questão
Diferencie os modos de operação do IPsec transporte e túnel? Qual dos dois é mais indicado para interligação de uma VPN e porque?