

**Disciplina: Segurança de Sistemas**

**Profa.: Rejane Cunha Freitas (**rejane.freitas@faculdadecdl.edu.br**)**

**Exercícios de fixação**

1. Suponha que um intruso tenha uma mensagem, bem como a versão cifrada dessa mensagem. Ele pode montar um ataque somente com texto cifrado, um ataque com texto aberto conhecido ou um ataque com texto aberto escolhido?

Apesar de possuir a mensagem, bem como a versão cifrada, ele não possui acesso à chave de criptografia utilizada. Deste modo, ele poderá montar um ataque com texto aberto conhecido.

2. De que maneira uma **hash** fornece um melhor controle de integridade da mensagem do que uma **soma de verificação**?

Os HMACs asseguram a integridade através de um hash com chave, o resultado de um cálculo matemático em uma mensagem utilizando uma função de hash (algoritmo) combinada com uma chave secreta compartilhada.

3.Você pode **decriptografar o hash** de uma mensagem a fim de obter a mensagem original? Explique sua resposta.

Não, pois a criptografia com hash é irreversível, haja vista que ele é usado para verificar se uma determinada informação foi ou não alterada. Logo, o usuário envia informação criptograda, em conjunto com o hash. A pessoa então criptografa e compara o hash que ela gerou com o hash que foi enviada. Se não bater, indica que em algum momento aquele pacote de dados foi alterado.

4. O que significa afirmar que um documento é **verificável,** **não falsificável** e **não repudiável**?

Um documento verificável e não falsificável é quando o destinatário pode provar para alguém que ninguém mais deve ter assinado o documento. Não repudiável é quando o receptor pode levar m, e a assinatura KB(m) à justiça e provar que o autor realmente assinou m.

5. De que modo **um resumo (digest) de mensagem** criptografada por chave pública proporciona uma **assinatura digital melhor** do que utilizar a mensagem criptografada por chave pública?

O resumo da mensagem garante a integridade do documento. Esse resumo é chamado de assinatura digital, que só pode ser descriptografado pelo receptor que possui a chave pública do remetente.

6. Suponha que o certifier.com (**entidade certificadora**) crie um certificado para foo.com (domínio). Tipicamente, todo certificado seria criptografado com a chave pública de certifier.com. Verdadeiro ou falso?

Verdadeiro