UNIFACS
Bacharelado em Ciência da Computação
Estrutura de Dados II
Prof. Othon Marcelo Nunes Batista

Atividade para a Segunda Avaliação

1. Quais são as diferenças entre confidencialidade e integridade de mensagem? É possível ter confidencialidade sem integridade? E integridade sem confidencialidade? Justifique as respostas.

2. Cite e explique diferenças entre os sistemas de criptografia de chave simétrica e assimétrica.

3. Suponha que N pessoas queiram se comunicar com cada uma das outras N - 1 pessoas usando criptografia de chaves simétricas. Todas as comunicações entre quaisquer duas pessoas, i e j, são visíveis para todas as outras do grupo de N, e nenhuma outra pessoa desse grupo pode decodificar suas comunicações. O sistema, como um todo, requer quantas chaves? Agora suponha que seja usada criptografia de chave pública. Quantas chaves serão necessárias nesse caso?

4. Você pode decodificar um hash de uma mensagem a fim de obter a mensagem original? Justifique a sua resposta.

5. Suponha que Alice tenha uma mensagem pronta para enviar para qualquer pessoa que lhe pedir. Milhares de pessoas querem ter acesso a mensagem de Alice, mas cada uma quer ter certeza da integridade da mensagem. Nesse contexto, você acha que é mais apropriado um esquema baseado em MAC ou um baseado em assinatura digital? Por quê?

6. O que significa dizer que um documento é verificável e não falsificável?

7. Considere a variação de um algoritmo MAC em que o transmissor envia (m, H(m) + s), sendo H(m) + s a concatenação de H(m) com s. Essa variação é falha? Por quê?

8. De que modo um hash de mensagem criptografado por chave pública proporciona uma assinatura digital melhor do que utilizar a mensagem criptografada com chave pública?

9. Suponha que um intruso tenha uma mensagem criptografada, bem como a versão decodificada dessa mensagem. Que tipo de ataque ele pode elaborar: somente texto cifrado, texto aberto conhecido ou texto aberto escolhido? Justifique a sua resposta.

10. Dê um exemplo prático de algoritmo de criptografia simétrica de fluxo, criptografia simétrica de bloco, criptografia assimétrica e hash.