Criptografia

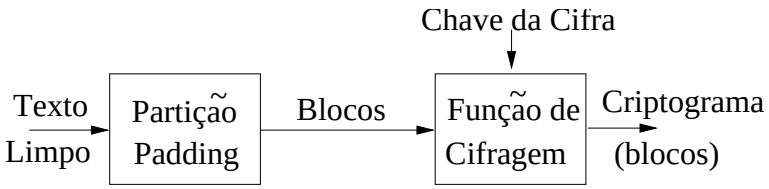
Exame da 2ª Chamada

LECOM — 2005/2006

Duração: 2 horas

Pergunta 1 Considere a utilização de cifras simétricas:

1. Explique o funcionamento e as propriedades de uma cifra simétrica sequencial síncrona. Para que tipo de aplicações recomendaria a sua utilização?
2. Explique porque é que existem diferentes modos de utilização para um determinado algoritmo de cifra por blocos.
3. Considere o seguinte modo de utilização de uma cifra por blocos. Identifique-o, descreva o seu funcionamento, e comente sobre a sua utilidade.



Pergunta 2 Relembre o que aprendeu sobre assinaturas digitais:

1. Para que serve uma assinatura digital? Que propriedades deve assegurar?
2. Explique porque é que na utilização corrente dos algoritmos de assinatura digital se recorre a uma função de hash criptográfica.

Pergunta 3 Os certificados de chave pública são muito utilizados em trocas de mensagens de e-mail.

1. Genéricamente, um certificado é uma prova de que uma determinada parcela de informação x satisfaz uma dada propriedade P. Explique que tipo de informação e que tipo de garantias estão associadas a um certificado de chave pública?
2. Descreva os passos necessários e os agentes envolvidos na emissão de um certificado de chave pública. Que técnicas criptográficas são utilizadas na criação e verificação de um certificado?
3. Considere que um agente A pretende enviar uma mensagem de e-mail cifrada, e assinada a outro agente B. Descreva os certificados envolvidos nesse processo, bem como a sua utilização.

Pergunta 4 Considere o On-line Certificate Status Protocol (OCSP)

1. Identifique a área aplicacional do protocolo OCSP. Explique que tipo de necessidades veio satisfazer, identificando as soluções disponíveis anteriormente e os problemas a elas inerentes.
2. Explique os diferentes tipos de resposta que podem ser dados por um servidor OCSP relativamente a um certificado de chave pública.