Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 28 de Janeiro 2005

Questão 1 [*Terminologia*]

1. O objectivo da criptografia é assegurar que os intervenientes numa troca de informação tenham garantias de que os requisitos de segurança foram satisfeitos. Descreva os diferentes tipos de requisitos de segurança que podem estar associados a uma troca de informação apontando, onde achar relevante, as relações que existem entre alguns desses requisitos. Dê exemplos práticos de cenários em que esses requisitos possam estar envolvidos.

2. Discuta as diferentes formas de quantificar a segurança de um algoritmo criptográfico. Relacione a sua resposta com os conceitos de **segurança incondicional** e **força bruta**.

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

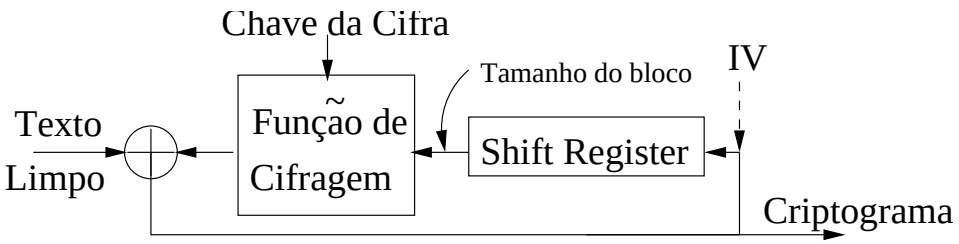
Exame da 2^a Chamada – 28 de Janeiro 2005

Questão 2 [*Cifras Simétricas*]

1. Dê três exemplos de cifras simétricas complementando a sua resposta com alguma informação contextual acerca dessas cifras.

2. Defina "padding" e explique a sua inclusão quando se utiliza uma cifra por blocos. Dê um exemplo de um algoritmo de "padding" explicando o seu funcionamento.

3. Considere o seguinte modo de utilização de uma cifra por blocos. Identifique-o, descreva o seu funcionamento, e comente sobre a sua utilidade.



Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 28 de Janeiro 2005

Questão 3 [*Autenticação e Identificação*]

1. Descreva as duas classes de algoritmos de autenticação de origem de mensagens que estudou, explicando a família de técnicas críptográficas a que pertencem (simétricas/assimétricas), a forma típica de utilização, e as principais diferenças relativamente às garantias de segurança que permitem obter.

2. Explique o princípio do conhecimento zero num protocolo de identificação. Qual o mecanismo básico em que se baseiam todos os protocolos de conhecimento zero? Dê um exemplo de um protocolo que seja estritamente de conhecimento zero, não necessariamente um protocolo criptográfico.

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 28 de Janeiro 2005

Questão 4 [*Certificados X509*]

1. Distinga uma extensão "critical" de uma extensão "non-critical". Indique um exemplo de utilização de uma extensão "critical", com base por exemplo na extensão "Key Usage".

2. Explique o conceito de "Certificate Policy" descrevendo a sua importante no contexto das PKIs. O que é um "Certification Practice Statement"

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 28 de Janeiro 2005

Questão 5 [*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.

3. Comente os requisitos de autenticação impostos pelo protocolo para pedidos e respostas OCSP, e a forma como são assegurados.

Nome:_____ **Número:**_____ **Curso:**_____