Criptografia Aplicada

LESI / LMCC

Exame da 1^a Chamada – 10 de Janeiro 2005

Questão 1 [*Terminologia*]

1. Diga o que entende por "obscurantismo" em criptografia. Explique porque é que este tipo de estratégia de segurança, muito comum na criptografia clássica, é desaconselhada na criptografia moderna. Justifique a sua resposta.

2. Descreva os diferentes ataques que podem ser dirigidos a um algoritmo criptográfico.

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

Criptografia Aplicada

LESI / LMCC

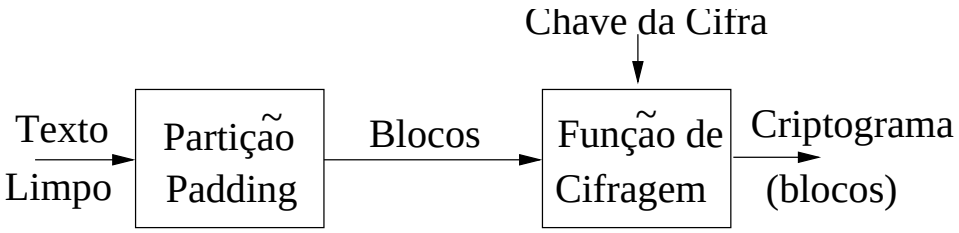
Exame da 1^a Chamada – 10 de Janeiro 2005

Questão 2 [*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.



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

Criptografia Aplicada

LESI / LMCC

Exame da 1^a Chamada – 10 de Janeiro 2005

Questão 3 [*Criptografia Assimétrica*]

1. Descreva o funcionamento de um esquema de cifra híbrido, como utilizado por exemplo nos sistemas de correio electrónico com confidencialidade. Justifique a utilização deste tipo de sistema.

2. No caso de a mensagem ser também assinada, a denominação utilizada é, geralmente, a de "envelope digital". Descreva a sequência de operações para a construção/descodificação de um envelope digital justificando, nomeadamente, a ordem pela qual são efectuadas as operações de cifragem e assinatura.

3. Indique o objectivo do protocolo Diffie-Hellman. Explique, justificando, a diferença entre o protocolo Diffie/Hellman e o protocolo Station-to-Station.

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

Criptografia Aplicada

LESI / LMCC

Exame da 1^a Chamada – 10 de Janeiro 2005

Questão 4 [*Certificados X509*]

1. Descreva a evolução dos certificados de chave pública X509 desde a versão 1 até à versão actual. (Nota: Não é necessário listar e descrever exaustivamente os campos definidos em cada versão. Pretende-se que explique que tipo de informação é possível incluir em cada tipo de certificado e que justifique as alterações introduzidas com as novas versões).

2. Explique a vantagem de incluir a extensão "CRL Distribution Point" num certificado de chave pública referindo-se, nomeadamente ao conceito e à utilização típica de CRLs.

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

Criptografia Aplicada

LESI / LMCC

Exame da 1^a Chamada – 10 de Janeiro 2005

Questão 5 [*Secure Shell (SSH)*]

1. Indique a área de utilização do SSH, e explique, de forma genérica a finalidade de cada uma das suas camadas: Connection, User Authentication e Transport Layer.

2. A negociação dos parâmetros de segurança de uma sessão SSH baseia-se na chamada Host Key. De que tipo de chave se trata? A quem pertence? Porque é que esta chave é tão importante, e de que forma é que funciona como garante da segurança no estabelecimento da sessão?

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