Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 30 de Janeiro 2004

Questão 1 [*Autenticação*]

1. Explique os conceitos de **autenticação de origem de mensagens** e **integridade**. Um destes conceitos implica o outro. Identifique esta implicação, justificando.

2. A distinção entre **autenticação de origem de mensagens** e **identificação** é algo subtil. Estabeleça esta distinção dando exemplos de aplicações em que cada uma destas garantias seja necessária, e de técnicas criptográficas que possam ser utilizadas para as implementar.

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

Criptografia Aplicada

LESI / LMCC

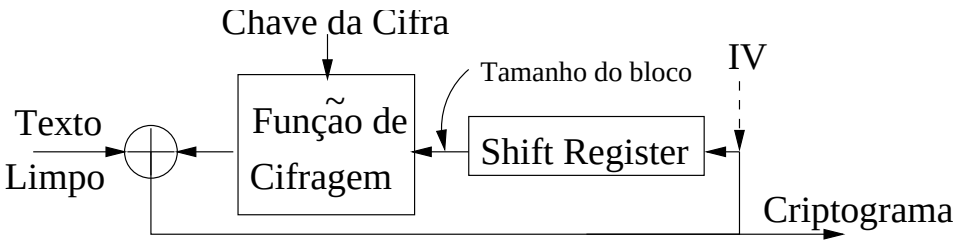
Exame da 2^a Chamada – 30 de Janeiro 2004

Questão 2 [*Cifras sequenciais*]

1. Explique, em termos genéricos, o funcionamento de uma cifra sequencial. Em que tipo de aplicações são utilizadas as cifras deste tipo? Dê um exemplo de uma cifra deste tipo.

2. Distinga as cifras síncronas das cifras auto-sincronizáveis.

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 – 30 de Janeiro 2004

Questão 3 [*Criptografia de Chave Pública*]
Considere as seguintes funções:

$$y = f(x, k_a) \tag{1}$$

$$z = g(y, k_b) \tag{2}$$

1. Que características devem possuir estas funções para que possam ser consideradas um esquema de cifra assimétrica. Explique a sua utilização neste contexto.

2. Que características devem possuir estas funções para que possam ser consideradas um esquema de assinaturas digitais. Explique a sua utilização neste contexto.

3. Baseado nas suas respostas às alíneas anteriores, que propriedade deverá ter um esquema de cifra assimétrica para que possa ser adaptado para um esquema de assinaturas digitais. Conhece alguma cifra assimétrica com esta característica?

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

Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 30 de Janeiro 2004

Questão 4 [*Acordo de chaves*]
Considere o protocolo Station-to-Station. Este protocolo é uma versão alargada do protocolo Diffie-Hellmann em que os parâmetros públicos trocados entre os interlocutores são assinados digitalmente.

1. Explique, em termos gerais, os objectivos e o funcionamento do protocolo Diffie-Hellmann. Note que para o fazer não é necessário explicitar os cálculos matemáticos envolvidos, mas sim descrever o propósito de cada passo executado, e quem o executa.

2. Explique o porquê da extensão implementada no protocolo Station-to-Station.

3. Suponha que o sistema de certificação digital utilizado para suportar o esquema de assinaturas digitais é comprometido: um intruso passa a conhecer a chave privada da autoridade de certificação. Explique as implicações desta brecha de segurança para:

   (a) Acordos de chave a serem estabelecidos no futuro.

   (b) Acordos de chave estabelecidos no passado e dos quais um intruso possua um registo.

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

Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 30 de Janeiro 2004

Questão 5 [*Public Key infrastructure*]

1. Diga o que entende por Public Key Infrastructure e enumere os principais componentes numa infrastrutura deste tipo.

2. Considere um processo de emissão de um Certificado de Chave Pública em que o pedido de certificado é efectuado via Web, sem contacto directo entre a Autoridade de Registo e o futuro Titular. Que problemas de segurança poderão advir desta implementação simplificada?

3. Explique o processo de validação de um Certificado de Chave Pública. Refira-se, nomeadamente, aos conceitos de *Hierarquia de Certificação*, *Cadeia de Certificação* e *Autoridade de Certificação de raiz*.

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

Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 30 de Janeiro 2004

Questão 6 [Aplicações Correntes da Criptografia]
Considere o sistema PGP (Pretty Good Privacy).

1. Descreva o processo de troca de uma mensagem cifrada entre dois utilizadores. Que denominação genérica se dá a essa técnica?

2. O PGP permite gerar assinaturas digitais anexadas a documentos, ou como documentos isolados. Discuta a utilidade desta funcionalidade.

3. Descreva as diversas formas de validar uma chave pública no sistema PGP.

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