Criptografia Aplicada

LESI / LMCC

Exame da 1^a Chamada – 16 de Janeiro 2004

Questão 1 [*Terminologia*]

1. Desenhe uma árvore hierárquica que reflicta as relações entre os seguintes termos:

cifra por blocos	**chave pública**	**criptograma conhecido**
criptoanálise	**assimétrica**	**chave secreta**
criptografia	**criptologia**	**ataque**
simétrica	**força bruta**	**chave privada**
cifra sequencial	**texto limpo conhecido**	**acordo de chaves**

2. Bruce Schneier afirma num dos seus artigos que na grande maioria dos ataques efectuados na prática os algoritmos criptográficos não são o ponto vulnerável dos sistemas de segurança. Comente esta afirmação dando exemplos.

3. 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:**_____

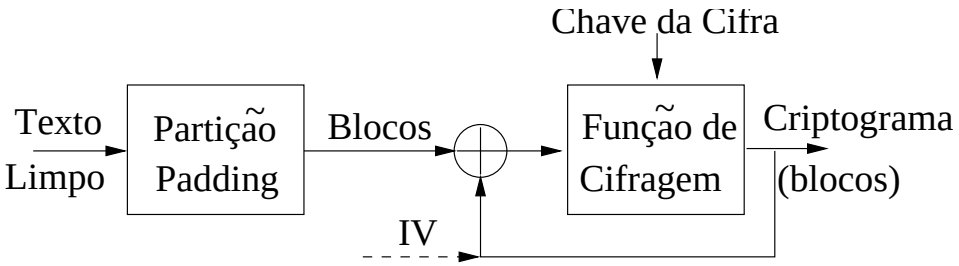
Criptografia Aplicada

LESI / LMCC

Exame da 1^a Chamada – 16 de Janeiro 2004

Questão 2 [*Cifras por blocos*]

1. Explique o porquê da utilização de cifras por blocos.
2. Dê três exemplos de cifras por blocos contextualizando a sua resposta com alguma informação complementar acerca dessas cifras.
3. Descreva as características desejáveis para uma cifra deste tipo.
4. 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 – 16 de Janeiro 2004

Questão 3 [*Distribuição de Chaves*]
Considere o seguinte esquema de distribuição de chaves em que KDS é um *Key Distribution Server*:

1. $Alice \rightarrow Bob : N_c, Alice, Bob, \{N_a, N_c, Alice, Bob\}_{K_{as}}$
2. $Bob \rightarrow KDS : N_c, Alice, Bob, \{N_a, N_c, Alice, Bob\}_{K_{as}}, \{Nb, Nc, Alice, Bob\}_{K_{bs}}$
3. $KDS \rightarrow Bob : N_c, \{N_a, K_{ab}\}_{K_{as}}, \{N_b, K_{ab}\}_{K_{bs}}$
4. $Bob \rightarrow Alice : N_c, \{N_a, K_{ab}\}_{K_{as}}$

Nota: N_a, N_b e N_c são números aleatórios.

1. Explique o funcionamento deste protocolo justificando a inclusão da identificação dos agentes em algumas das mensagens.
2. Justifique a utilização dos números aleatórios.
3. Conhece algum sistema comercial que utilize este tipo de técnica? Identifique-o e descreva-o de forma genérica.

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

Criptografia Aplicada

LESI / LMCC

Exame da 1^a Chamada – 16 de Janeiro 2004

Questão 4 [*Certificados X509*]

1. Considere a seguinte utilização de Certificados de Chave Pública num processo de troca de informação autenticada entre dois utilizadores e.g. e-mail:

   - O emissor da mensagem obtém do receptor o seu Certificado de Chave Pública.
   - Dado o seu desconhecimento da Autoridade de Certificação emissora desse certificado, solicita também ao receptor o certificado dessa CA.
   - O emissor valida os certificados que obteve.
   - O emissor assina digitalmente a mensagem utilizando informação contida no certificado do receptor.
   - O emissor envia a mensagem ao receptor que verifica a assinatura digital.

   Analize este procedimento, primeiro quanto à sua correcção, e posteriormente quanto à sua segurança.

2. O que se alteraria/manteria no caso de se pretender que a informação fosse transferida também com garantias de confidencialidade?

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

Criptografia Aplicada

LESI / LMCC

Exame da 1^a Chamada – 16 de Janeiro 2004

Questão 5 [*Revogação de Certificados X.509*]

1. Explique o que é uma CRL e qual a sua finalidade.

2. A publicação periódica de CRLs coloca algumas limitações ao processo de revogação de certificados. Nomeadamente, confere um carácter discreto à informação nela contida (a informação é actualizada apenas em instantes pré-definidos). Que problemas poderão surgir devido a esta limitação?

3. Sugira um sistema alternativo às CRLs que não padeça desta limitação, e discuta as vantagens/desvantagens dos dois sistemas.

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

Criptografia Aplicada

LESI / LMCC

Exame da 1^a Chamada – 16 de Janeiro 2004

Questão 6 [*Secure Sockets Layer (SSL)*]

1. O sistema SSL baseia-se no conceito de sessão. Explique porque razão este é um modo de funcionamento comum em sistemas com segurança criptográfica.

2. Descreva a forma típica de utilização de Certificados de Chave Pública no estabelecimento de ligações SSL.

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