Criptografia Aplicada

LESI / LMCC

Exame da 1ª Chamada – 13 de Janeiro 2006

Questão 1 Considere a cifra *One-Time-Pad*.

1. Descreva o seu funcionamento e comente sobre as vantagens e desvantagens da sua utilização na prática.
2. Comente a frase *"A cifra One-Time-Pad é incondicionalmente segura"*. Relacione com o conceito de **ataque por força bruta**.
3. Suponha que se pretende utilizar a cifra *One-Time-Pad* num esquema de cifragem híbrido, tipo **envelope digital**. Descreva em que consistiria esta solução, comentando sobre a sua validade.

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

Criptografia Aplicada

LESI / LMCC

Exame da 1ª Chamada – 13 de Janeiro 2006

Questão 2 Considere o modo de utilização de cifras por blocos *Cipher Block Chaining* (CBC).

1. Descreva o seu funcionamento na cifragem e decifragem.
2. Suponha que se pretende proteger um ficheiro de *log* cifrando-o com base neste modo. Analise a eficiência das seguintes operações:
   - Adicionar uma entrada no início do ficheiro.
   - Adicionar uma entrada no final do ficheiro.
   - Ler uma entrada no início do ficheiro.
   - Ler uma entrada no final do ficheiro.
3. Imagine que o ficheiro de *log* é corrompido por uma falha de *hardware*. Descreva um possível procedimento de recuperação da informação, tendo em conta que o vector de inicialização é sempre armazenado nas posições iniciais do ficheiro (sem qualquer protecção).

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

Criptografia Aplicada

LESI / LMCC

Exame da 1ª Chamada – 13 de Janeiro 2006

Questão 3 Considere a seguinte construção criptográfica que, dados n blocos de texto limpo $(x_1, \ldots, x_n)$, uma cifra por blocos C, uma chave secreta k e um vector de inicialização iv, funciona da seguinte forma:

- $y_0 = iv$
- $y_i = C(x_i \oplus y_{i-1}, k), 1 \leq i \leq n$
- $y_{n+1} = C(y_n, k)$
- Return $(x_1, \ldots, x_n, y_{n+1})$

1. Esta construção implementa que tipo de técnica criptográfica? Descreva o seu modo típico de utilização.
2. Dos quatro requisitos de segurança fundamentais na criptografia, quais deles são garantidos por esta construção? Justifique.
3. Descreva uma construção alternativa que permita satisfazer, pelo menos, os mesmos requisitos de segurança.

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

Criptografia Aplicada

LESI / LMCC

Exame da 1ª Chamada – 13 de Janeiro 2006

Questão 4 Dois utilizadores A e B possuem certificados de chave pública pessoais em hierarquias de certificação disjuntas.

1. Descreva o que entende por **certificado de chave pública** e por **hierarquia de certificação**.
2. Explique de que forma poderão estes utilizadores comunicar com garantias de autenticidade. E se adicionalmente se pretender confidencialidade? Justifique a sua resposta.
3. Suponha que as instituições que gerem estas hierarquias de certificação estão interessadas em facilitar este processo. De que forma o poderiam fazer?

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

Criptografia Aplicada

LESI / LMCC

Exame da 1ª Chamada – 13 de Janeiro 2006

Questão 5 Considere o protocolo 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.

3. Que funcionalidade esperaria encontrar num Cliente/Servidor SSL para lidar com o problema da revogação de certificados de chave pública? Justifique.

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