Criptografia Aplicada

LESI / LMCC

Exame da 1a Chamada – 12 de Janeiro 2007

Questão 1 Recorde o que estudou sobre funções de Hash criptográficas e Message Authentication Codes (MACs).

1. Explique as diferenças entre uma função de Hash criptográfica e um MAC, quer em termos de funcionamento, quer em termos de garantias fornecidas.

2. Porque é que um simples *checksum* (por exemplo um CRC), não pode ser utilizado como função de Hash criptográfica? Dê um exemplo de uma utilização típica de uma função de hash criptográfica que não seria segura com um *checksum* comum.

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

Criptografia Aplicada

LESI / LMCC

Exame da 1a Chamada – 12 de Janeiro 2007

Questão 2

O gerente de um banco leu na Wikipedia que a cifra One-Time-Pad é perfeitamente segura e pretende proteger todas as comunicações nos acessos a Web banking utilizando esta tecnologia.

1. Explique o funcionamento do One-Time-Pad e justifique por palavras suas porque se diz que a sua segurança é perfeita. Como justificaria ao gerente do banco a sua não utilização?

2. Suponha que o gerente do banco ignora a sua recomendação e ainda assim opta pelo One-Time-Pad. Algum tempo depois, é chamado de volta ao banco para resolver o seguinte problema:

   - Um cliente queixa-se de que uma ordem de transferência de uma quantia volumosa foi depositada na conta errada.
   - O gerente garante que a mensagem decifrada pelo banco indicava o número de conta efectivamente creditado.

   Como explicaria ao gerente do banco que a segurança incondicional da cifra One-Time-Pad não elimina a possibilidade deste tipo de ocorrência?

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

Criptografia Aplicada

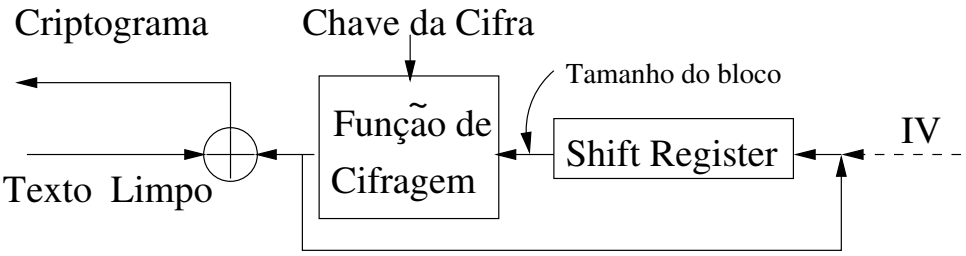
LESI / LMCC

Exame da 1a Chamada – 12 de Janeiro 2007

Questão 3 Considere a utilização de cifras simétricas:

1. 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.

2. 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 1a Chamada – 12 de Janeiro 2007

Questão 4 Recorde o que estudou sobre certificados de chave pública X.509.

1. Em que circunstâncias deve um certificado ser revogado? Descreva o mecanismo previsto na PKI para efectuar esta operação, incluindo a sua utilização típica, e as garantias de segurança que lhe estão subjacentes.

2. A confiança na Autoridade de Certificação é um ingrediente fundamental na utilização de certificados. Admita que A e B confiam na autoridade de certificação CA. Em que condições é que um intruso I, que conhece a chave privada de CA, poderá manipular livremente uma mensagem cifrada e assinada enviada por A para B?

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

Criptografia Aplicada

LESI / LMCC

Exame da 1a Chamada – 12 de Janeiro 2007

Questão 5 Considere o protocolo Secure Sockets Layer (SSL)

1. No estabelecimento de uma sessão SSL são trocados certificados de chave pública. Justifique a sua utilização e descreva-a em função das garantias que permite estabelecer.

2. Suponha que um intruso é bem sucedido a interceptar o certificado do servidor, substituindo-o por outro à sua escolha. Em que condições poderia o intruso beneficiar com esta troca? Que avisos poderia receber o utilizador, se estivesse a estabelecer a ligação utilizando um *browser* (e.g. Internet Explorer, Firefox) comum?

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