Criptografia Aplicada

LESI / LMCC

Teste intermédio – 12 de Novembro 2007

Questão 1 Considere os diferentes modos de operação das cifras por blocos.

1. Explique porque é que o modo ECB só deve ser utilizado para mensagens que não necessitem de mais do que um bloco.

2. Comente a seguinte afirmação: *mesmo quando utilizado para cifrar mensagens com um único bloco, o modo ECB é vulnerável ao ataque "codebook"*. Comente em particular se é (ou não) relevante a escolha do procedimento de *padding*.

3. Explique porque é que o modo CBC (*cipher block chaining*) ultrapassa as limitações apontadas.

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

Criptografia Aplicada

LESI / LMCC

Teste intermédio – 12 de Novembro 2007

Questão 2 Considere uma cifra sequêncial síncrona (e.g. RC4).

1. Explique o princípio geral de funcionamento dessa cifra.
2. Porque motivo se recomenda que as chaves sejam utilizadas uma única vez? Ilustre com um ataque que tire partido da repetição da utilização da chave.

Questão 3 Considere que um utilizador de um sistema multi-utilizador pretende garantir que o conteúdo de uma directoria não é alterado por outro utilizador do sistema (em particular, pelo administrador). Sugira uma solução baseada em técnicas criptográficas que lhe forneça essa garantia.

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

Criptografia Aplicada

LESI / LMCC

Teste intermédio – 12 de Novembro 2007

Questão 4 Considere o protocolo de acordo de chaves *Diffie-Hellman*.

1. Descreve resumidamente o seu funcionamento e os aspectos de segurança relativamente a um adversário passivo e activo respectivamente.

2. Na codificação desse protocolo no *framework JCA/JCE* estão envolvidas várias classes. Explique, de forma sucinta, o papel exercido por cada uma dessas classes.

3. Para uma das classes referidas na alínea anterior (à sua escolha), descreva o respectivo padrão de utilização (i.e. as linhas de código correspondentes).

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