Criptografia e Segurança da Informação

LESI

2008/2009 (Época Normal)

1. O *modo de operação* é um aspecto crucial na segurança da utilização de uma cifra por blocos.
   (a) Descreva um cenário onde a escolha inapropriada do modo de operação da cifra compromete a segurança. Justifique.
   (b) Como é que, nesse mesmo cenário, a escolha de um modo mais apropriado permitiria ultrapassar essas falhas de segurança? Justifique.
2. Caracterize os conceitos de *adversário activo* e *adversário passivo*. Forneça um exemplo de uma técnica considerada segura perante um tipo de adversário, e insegura perante o outro. Justifique.
3. Explique as diferenças entre uma função de Hash criptográfica e um MAC, quer em termos de funcionamento, quer em termos das garantias fornecidas.
4. A confiança na Autoridade de Certificação (CA) é um ingrediente fundamental na utilização de certificados X509. Admita que A e B confiam na autoridade de certificação CA mas um intruso I dispõe da chave privada da CA. Em que medida pode I manipular/comprometer uma mensagem de *email* cifrada e assinada enviada por A para B? Justifique (considerando diferente cenários, se achar conveniente).
5. O *framework JCA/JCE*, estudada no âmbito do curso, oferece ao programador Java uma API apropriada para o desenvolvimento de aplicações criptográficas.
   (a) As *Engines Classes* disponibilizam aos programadores "serviços" criptográficos. Forneça exemplos de 4 dessas classes, indicando a respectiva funcionalidade.
   (b) Para uma das classes referida na alínea anterior, apresente o "padrão típico" de utilização (i.e. a sequência de métodos invocados numa utilização típica).

1.6 + 1.6 + 1.6 + 1.6 + 2 + 1.1 + .5