Criptografia

Mestrado Integrado em Engenharia Biomédica

2008/2009 (Época Recurso)

1. As cifras simétricas podem ser classificadas como *sequenciais* ou *por blocos*.
   (a) Descreva de forma sucinta cada um desses tipos de cifra.
   (b) O que é que, do ponto de vista de utilização, distingue esses tipos de cifras. Forneça exemplos de aplicações onde seja adequado cada um deles.
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.
3. 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.
4. O certificados X509 são provavelmente o aspecto mais visível da utilização da criptografia nas utilizações correntes (correio electrónico, etc.).
   (a) Que problema pretendem resolver? No que é que consistem? E porque é que permitem ultrapassar as dificuldades apontadas?
   (b) O que é uma CRL? Quais os problemas associados e que cuidados são requeridos na sua utilização?
5. 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).
6. O framework JCA/JCE, estudado no âmbito do curso, disponibiliza ao programador acesso a funcionalidades criptográficas.
   (a) Que características destaca desse *framework*? (em particular nas opções de desenho e arquitectura).
   (b) A tecnologia criptográfica é caracterizada por uma constante evolução (em termos de algorítmos, nos tamanhos recomendados dos segredos, etc.). Não quer isso dizer que o framework está condenado a, também ele, ficar ultrapassado? Justifique.