Criptografia

Mestrado Integrado em Engenharia Biomédica

2008/2009 (Época Normal)

1. Um aspecto importante na utilização de cifras por blocos é a escolha do "modo de funcionamento".

   (a) Descreva o modo básico ECB (*Electronic Code Book*), assim como os problemas de segurança que lhe estão associados.

   (b) Refira outro(s) modo(s) que permitam ultrapassar esses problemas. Justifique.

2. Relembre o protocolo de acordo de chaves *Diffie-Helman*: (num grupo de ordem p com gerador g)

   - A gera x e envia a B o valor $X = g^x[p]$.
   - B gera y e envia a A o valor $Y = g^y[p]$.
   - A calcula $K = Y^x[p] = g^{x*y}[p]$.
   - B calcula $K = X^y[p] = g^{x*y}[p]$.

   (a) Explique de forma sucinta porque é que um atacante passivo não consegue ficar na posse do segredo acordado.

   (b) No entanto, o protocolo é vulnerável ao ataque *man-in-the-middle*. Em que consiste esse ataque?

3. No que é que consiste um certificado de chave publica X509? Porque motivo é tão importante a utilização desses certificados quando estão envolvidas cifras assimétricas?

4. Suponha que um utilizador A pretende enviar uma mensagem de correio electrónico para B cifrada e assinada. Que certificados estão envolvidos no envio e na recepção dessa mensagem?

5. Que propriedade caracteriza as *funções de hash criptográficas*? Descreva uma aplicação concreta dessa técnica criptográfica.

6. É normal os protocolos de comunicação seguros fazerem uso de uma combinação de técnicas assimétricas e simétricas (e.g. SSL). Porquê? (sugestão: ilustre essa combinação num exemplo concreto – e.g. *envelope digital*)

7. O *framework JCA/JCE*, estudada no âmbito do curso, oferecem 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).