Criptografia/SPSATD

MICEI/MSDPA

2006/2007 (Época Normal)

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. 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. Que propriedades se pretendem estabelecer com uma *assinatura digital*? Descreva o processo típico de produção e verificação das assinaturas digitais.

5. 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*)

6. 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