Criptografia Aplicada

LESI / LMCC

Teste final – 23 de Janeiro de 2008

Questão 1

1. As técnicas assimétricas são normalmente utilizadas em conjugação com técnicas simétricas. Porquê? Ilustre com um exemplo concreto.

2. Considere o estabelecimento de uma sessão SSL em modo de autenticação mútua. Quais os certificados envolvidos na fase de *handshake* desse protocolo e qual o seu papel no estabelecimento das garantias pretendidas?

3. O que é uma CRL? Como deve ser utilizada e quais os problemas associados a essa utilização?

4. Quais os passos envolvidos na obtenção de um certificado X509? (sugestão: ilustre cada um desses passos mostrando como podem ser concretizados utilizando a ferramenta `openssl`).

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

Criptografia Aplicada

LESI / LMCC

Teste final – 23 de Janeiro de 2008

Questão 2 Relembre a primitiva criptográfica RSA estudada no curso.

- **Inicialização**: geram-se dois números primos p e q ($n = p \cdot q$), e um inteiro e tal que $gcd(e, \varphi(n)) = 1$. Calcula-se d tal que $e \cdot d = 1\ [\varphi(n)]$.
- **Cifrar**: $c = m^e\ [n]$ (com $0 \leq m < n$).
- **Decifrar**: $m = c^d\ [n]$.

1. A segurança do RSA está intimamente relacinada com a dificuldade de se factorizarem números grandes. Explique como é que, conhecendo a factorização de n, se pode atacar o RSA.
2. Um problema associado à utilização directa da primitiva RSA na implementação de uma cifra assimétrica é a sua *natureza determinística*. Explique como tirar partido dessa característica num ataque à cifra e como é que técnicas como RSA-OAEP ultrapassam esse problema?
3. Que garantias se pretende estabelecer com uma assinatura digital? Explique como pode ser implementado um esquema de assinatura digital utilizando a primitiva RSA (descreva em particular os procedimentos de geração da assinatura e de verificação).
4. Nas assinaturas digitais estudadas, a assinatura é concatenada à mensagem assinada. Suponha então que A envia uma mensagem M juntamente com a respectiva assinatura a B. Não pode então um adversário I substituir a assinatura de A pela sua própria (fazendo assim crer a B que a origem de M foi I)? (obs: discuta/justifique convenientemente a sua resposta).

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