Criptografia

MIETI

2º Teste – 14 de Dezembro 2017

Questão 1

1. Quais os principais passos envolvidos no processo de criação de um certificado X509?
2. Comente a seguinte afirmação: "*A utilização de certificados X509 pressupõe o estabelecimento de uma* relação de confiança".
3. No que consiste uma "cadeia de certificação"? Qual o impacto dessas cadeias nas "relações de confiança" que a utilização desses certificados pressupõe?
4. A utilização efectiva dos certificados digitais pressupõe a sua validação. Descreva os principais passos envolvidos na validação de uma cadeia de certificados X509.

Questão 2 Relembre protocolo *Station-to-Station (StS)* estudado no curso (fixados os parâmetros p e g):

A→B: $+x;\ g^x$

B→A: $+y;\ g^y, E_K(S_B(g^y, g^x)), Cert_B$

A→B: $E_K(S_A(g^x, g^y)), Cert_A$

1. Explique como é que o protocolo *StS* ultrapassa a vulnerabilidade do protocolo original *Diffie-Hellman* a ataques do tipo *man-in-the-middle*.
2. Qual o papel reservado à troca de certificados no segundo e terceiro passos do protocolo? Explicite em particular que assumpções de confiança estão pressupostas nessa troca.
3. Considere o cenário em que o adversário (Eve) disponha também de um certificado emitido de forma análoga ao dos intervenientes legítimos (Alice e Bob). Não pode agora Eve conduzir novamente o ataque *man-in-the-middle*, tal como no protocolo *Diffie-Hellman* original, mas trocando o certificado do agente legítimo pelo seu próprio? Justifique.

Questão 3 Relembre a primitiva criptográfica RSA estudada no curso.

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

1. Explique o que é uma cifra de chave pública, e como é que deve ser utilizada.
2. A segurança do RSA está intimamente relacinada com a dificuldade de se factorizarem números grandes. Explique a afirmação explicitando em particular como é que, conseguindo calcular a factorização de qualquer número, se pode atacar o RSA.
3. Um dos problemas apontados à utilização directa da primitiva RSA como uma cifra de chave pública é o de se tratar de uma cifra determinística. Explique qual o significado e impacto desse facto na avaliação da segurança da cifra.