Instituto Superior de Engenharia de Lisboa e Porto

Eng. informatica

Eng- Comunição

Matemática I

1. (1,5%) A **dimen*são*** *de uma* assinatura digital (em bytes) é proporcional à **dimensão** da mensagem assinada?
2. (1,5%) Apresente uma forma de atacar uma implementação de um esquema de cifra assimétrica cujo algoritmo de cifra, Ea(K)(m), seja determinístico (isto é, se x = y então Ea(K)(x) = Ea(K)(y)).
3. (2%) No contexto dos esquemas de cifra baseados em primitivas de bloco, considere o modo de operação definido por:

   - Seja x = x1,..., XL a divisão nos blocos xi do texto em claro x, e y = y1,...,YL o criptograma resultante da cifra da mensagem x;
   - Seja yi = E(k)(xi + xi-1), para i = 1,...,L, onde E é a primitiva de cifra, + denota o ou-exclusivo bit a bit;
   - Seja x0 é o vector inicial (IV)

4. (4%) Considere a infra-estrutura de certificados X.509 e o protocolo TLS com troca de chaves usando RSA:
   4.1. Numa cadeia de certificados válida, a chave privada está presente em algum deles?
   4.2. Durante o *handshake*, como é obtida a raiz de confiança usada para validar o certificado do servidor?
5. (1,5%) Considere a função de *hash* H(m) definida por:

   - Seja Ep(k)(b) uma primitiva de cifra em bloco que usa chaves k de n bits e blocos b de n bits
   - O valor de hash é H(m) = yL.

   Explique porque motivo é computacionalmente fazível, dado m, obter m' != m tal que H(m') = H(m).