Tecnologia Criptográfica

MIEI

2º teste – 8 de Janeiro 2018

Questão 1 (Assinale a veracidade das afirmações seguintes com as letras V/F) Um certificado de chave pública "deve" ser revogado

☐ após ser utilizado numa operação de cifra

☐ quando expira o prazo de validade

☐ quando a chave privada associada for comprometida

☐ quando o certificado for auto-assinado

Questão 2

1. Quais as propriedades de segurança associadas à assinatura digital? No que consiste um ataque a essa técnica criptográfica?
2. Uma assinatura digital vincula "toda" a mensagem assinada. Porque é que então o tamanho de uma assinatura não é proporcional ao tamanho da mensagem? Justifique, indicando em particular porque é que esse facto não compromete a segurança da assinatura.
3. Uma aplicação das assinaturas digitais é a assinatura de documentos PDF. Refira, nesse cenário,
   (a) que utilização é feita dos certificados e com que fim.
   (b) o que é, e porque é que se recomendada, a utilização de um mecanismo de *time-stamping* nessas assinaturas.
4. Relembre a utilização das assinaturas digitais na aplicação cliente/servidor realizada na componente prática da UC. Enumere os vários passos requeridos na validação dessas assinaturas, incluindo a utilização dos certificados associados (pode apresentar fragmentos de código, se desejar).

Nome:_____ **Número:**_____

Questão 3 (Assinale a veracidade das afirmações seguintes com as letras V/F) O mecanismo de certificação

☐ permite associar a chave pública à entidade que detém a chave privada correspondente

☐ é utilizado para garantir a confidencialidade das chaves públicas

☐ permite atestar que a técnica criptográfica em consideração oferece protecção para a(s) propriedade(s) de segurança pretendida(s)

☐ pressupõe que se deposite "confiança" na entidade responsável (EC)

Questão 4 Relembre a cifra *El-Gamal* estudada no curso: dado um primo p e um gerador g.

- **Inicialização**: gera um número aleatório x $(0 < x < p)$ e faz-se $\mathsf{sk} = x$ e $\mathsf{pk} = g^x \ [p]$.
- **Cifrar**: gera-se um número aleatório r $(0 < r < p)$, sendo o criptograma $c = \text{Enc}(\mathsf{pk}, m) = \langle g^r \ [p], m * \mathsf{pk}^r \ [p] \rangle$.
- **Decifrar**: dado um criptograma $c = \langle c_1, c_2 \rangle$, a mensagem é recuperada como $c_2/(c_1^x) \ [p]$.

1. Apresente um argumento informal para a segurança da cifra (Valorização: Como podem esse tipo de argumento ser expresso/demonstrado de forma rigorosa?)
2. No entanto, a cifra é "maleável", na medida em que é possível manipular um criptograma por forma a decifrar num resultado relacionado.
   (a) Mostre como pode manipular $c = \text{Enc}(\mathsf{pk}, m)$ por forma a decifrar em m^2.
   (b) Sugira, justificando, uma forma de impedir este tipo de manipulação.