Segunda parte do exame da época normal de Criptografia Aplicada

11 de janeiro de 2024 **14h00m – 15h30m/17h00m**

1.0 **11:** A distribuição de chaves públicas é atualmente feita maioritariamente através de certificados públicos X.509. Explique:

a) Qual é a principal função de um certificado de uma chave pública?

b) Por que razão um certificado tem de ser assinado digitalmente?

1.0 **12:** Considere o conceito de revogação de um certificado de chave pública X.509. Explique:

a) Em que consiste?

b) Quem é que é responsável por comunicar a mesma?

c) Como é que essa comunicação pode ser realizada?

1.0 **13:** Um certificado de chave pública X.509 pode ser uma raiz de uma cadeia de certificação. Explique:

a) O que é uma cadeia de certificação?

b) O que faz com que um certificado seja raiz de uma cadeia de certificação?

1.0 **14:** *Long Term Validation* (LTV) é uma expressão que é usada para referir a capacidade de uma assinatura digital ser verificável de forma confiável muitos anos depois de ter sido produzida. Qual é o principal problema que a passagem do tempo cria na validação de assinaturas, e que levou à criação dos mecanismos que permitem a LTV (não os descreva!)?

1.0 **15:** O não-repúdio é uma característica que normalmente é desejável relativamente às assinaturas digitais de documentos. Explique:

a) Em que consiste o não-repúdio?

b) Qual é a relevância que dispositivos como os smartcards, como o Cartão de Cidadão, têm para assegurar esta característica?

1.0 **16:** Como é que é feita a adição de pontos numa curva elíptica?

1.0 **17:** Explique como se pode multiplicar eficientemente um ponto de uma curva elíptica por um número inteiro negativo.

1.0 **18:** Explique como se pode partilhar um segredo entre n entidades, $n \geq 2$, em que apenas t entidades, $2 \leq t \leq n$, são necessárias para revelar o segredo. Considere os casos $t < n$ e $t = n$.

1.0 **19:** A técnica *one-of-two oblivious transfer* permite que uma entidade extraia um item de informação (de um conjunto de dois itens) de uma outra entidade sem que esta consiga saber qual dos itens foi extraído. Explique como pode adaptar essa técnica para extrair um de n, com $n > 2$. A técnica é escalável, isto é, a sua utilização para n grande é prática?

1.0 **20:** Os resíduos quadráticos são indiretamente usados em protocolos de prova de identidade que não revelam informação (*zero knowledge proofs*). Qual é o problema matemático que os torna atrativos neste contexto?