

Questão 1

Marque a alternativa que apresenta os tipos de criptografias:

- A Chave simétrica, chave assimétrica e função Hash.
- B Quântica e Hash.
- C SHA, MD5 e PCK.
- D Firewall e antivírus.
- E Criptografia transsimétrica

check_circle

check_circle

Parabéns! A alternativa A está correta.

Criptografia de chave simétrica, criptografia de chave assimétrica e função Hash. O motivo da existência de três tipos de criptografia é que cada esquema é otimizado para alguma aplicação específica. As funções de hash, por exemplo, são adequadas para garantir a integridade dos dados. A criptografia de chave secreta, por sua vez, é ideal para criptografar mensagens, proporcionando privacidade e confidencialidade. A troca de chaves é uma aplicação importante da criptografia de chave pública.

Questão 2

Selecione a opção que apresenta todos os itens que compõem um certificado digital:

- A Nome do titular do certificado, biometria, o indivíduo ou a entidade identificada pelo certificado, datas de expiração, cópia da chave pública do detentor de certificado.
- B Nome do titular do certificado, número de série usado para identificar exclusivamente um certificado, o indivíduo ou a entidade identificada pelo certificado, datas de expiração, cópia da chave pública do detentor de certificado.
- C Nome do titular do certificado, número de série usado para identificar exclusivamente um certificado, o indivíduo ou a entidade identificada pelo certificado, datas do envio do certificado, cópia da chave pública do detentor de certificado.

check_circle

- D Nome do titular do certificado, número de série usado para identificar exclusivamente um certificado, o indivíduo ou a entidade identificada pelo certificado, datas de expiração, trechos criptografados da mensagem.
- E Nome do titular do certificado, chave criptográfica, data de nascimento, nome da mãe, datas de envio do certificado, entidade identificada pelo certificado.

check_circle

Parabéns! A alternativa B está correta.

O certificado digital destina-se a qualquer pessoa, física ou jurídica, sendo emitido por uma Autoridade Certificadora (AC). A AC emite um certificado digital criptografado contendo o nome do sujeito (a organização ou indivíduo certificado), a chave pública do sujeito, um número de série (para identificar exclusivamente o certificado), uma data de validade, a assinatura da autoridade de certificação confiável e qualquer outra informação relevante. O objetivo é garantir a autenticidade do usuário, ou companhia que faça uso do certificado digital, ou seja, certificar que o usuário ou a empresa são, de fato, quem dizem ser.