Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ)

CARGO 18: ANALISTA JUDICIÁRIO – ÁREA: APOIO ESPECIALIZADO ESPECIALIDADE: SUPORTE EM TECNOLOGIA DA INFORMAÇÃO

Prova Discursiva

Aplicação: 01/12/2024

PADRÃO DE RESPOSTA DEFINITIVO

A criptografia simétrica ou criptografia de chave secreta ou compartilhada utiliza uma única chave, que é compartilhada entre o emissor e o receptor da mensagem. Um algoritmo aplica uma série de regras matemáticas para transformar os dados em um código ilegível, e esse algoritmo depende de uma chave, que é uma sequência de *bits* que define como o código será gerado. A criptografia assimétrica ou criptografia de chave pública ou de dois fatores utiliza um par de chaves: uma pública e uma privada. O emissor deve ter a chave pública do receptor antes de enviar os dados. Assim, ele usa essa chave para cifrar os dados antes de enviá-los. O receptor, por sua vez, usa a sua chave privada para decifrar os dados após recebê-los.

O certificado digital é um documento eletrônico que serve para identificar uma pessoa ou empresa na Internet, permitindo a realização de transações digitais de forma segura. O certificado digital é utilizado para assinar documentos digitalmente, com validade jurídica; para cessar serviços públicos, como o da Receita Federal ou INSS; para realizar operações bancárias; para validar o acesso a sistemas da empresa; para emitir notas fiscais eletrônicas, participar em leilões da Receita Federal etc.

Os algoritmos de *hash* são funções criptográficas que transformam uma entrada de dados de qualquer tamanho em uma sequência fixa de caracteres. É amplamente utilizada em segurança digital, especialmente na verificação de integridade de dados e em assinaturas digitais. Os princípios dos algoritmos de *hash* são: irreversibilidade; unicidade; resistência à colisão; e recorrência.

QUESITOS AVALIADOS

QUESITO 2.1 Funcionamento dos protocolos de criptografia simétrica e assimétrica
Conceito 0 – Não atendeu ao quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu de maneira parcialmente correta apenas um dos conceitos (criptografia simétrica ou assimétrica) e não abordou o outro ou o abordou de forma totalmente equivocada.
Conceito 2 – Descreveu corretamente apenas um dos conceitos e não abordou o outro ou o abordou de forma totalmente equivocada OU descreveu de forma parcialmente correta os dois conceitos.
Conceito 3 – Descreveu corretamente um dos conceitos e o outro de forma parcialmente correta.
Conceito 4 – Descreveu corretamente os dois conceitos.

QUESITO 2.2 Conceito de certificado digital e dois de seus usos
Conceito 0 – Não atendeu ao quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu o conceito de maneira parcialmente correta e não citou os usos.
Conceito 2 – Descreveu corretamente o conceito, mas não citou os usos.
Conceito 3 – Descreveu corretamente o conceito, mas citou corretamente apenas um uso.
Conceito 4 – Descreveu corretamente o conceito e citou corretamente ambos os usos.

QUESITO 2.3 Conceito de algoritmos de *hash* e seus princípios
Conceito 0 – Não atendeu ao quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu apenas o conceito, e o fez de maneira parcialmente correta.
Conceito 2 – Descreveu o conceito corretamente, mas não citou os princípios.
Conceito 3 – Descreveu o conceito corretamente, mas apresentou os princípios dos algoritmos de *hash* de maneira parcialmente correta.
Conceito 4 – Descreveu o conceito corretamente e apresentou corretamente os princípios dos algoritmos de *hash*.