Questão 1 – Cite os cinco principais pilares da segurança da informação e explique resumidamente o que cada um deles representa.

1- Confidencialidade
2- Integridade
3- Disponibilidade
4- Autenticidade
5- Legalidade

Questão 2 – Explique a estratégia utilizada por cada um dos tipos de criptografia a seguir: transposição, substituição e esteganografia.

1-Na criptografia clássica, uma cifra de transposição procede à mudança de cada letra (ou outro qualquer símbolo) no texto a cifrar para outro (sendo a decifração efectuada simplesmente invertendo o processo). Ou seja, a ordem dos caracteres é mudada.

2-Em criptografia, uma cifra de substituição é um método de criptografia que opera de acordo com um sistema pré-definido de substituição.

3- Esteganografia é uma técnica que consiste em esconder um arquivo dentro do outro, de forma criptografada.

Questão 3 – Indique corretamente as características da criptografia (A) assimétrica, (B) simétrica ou (C) para características que são de ambas.

( ) Algoritmo AES
( ) Computacionalmente mais eficiente
( ) Chave privada e pública
( ) Usada dentro do protocolo HTTPS
( ) Algoritmo RSA
( ) Usa chaves criptográficas de maior tamanho em bits
( ) Usa a mesma chave para cifrar e decifrar a mensagem
( ) Criptografia de curvas elípticas
( ) Algoritmo DES
( ) Usado na assinatura digital

Questão 4 – Cite as principais características desejadas para um algoritmo de Hash criptográfico.

1- Unidirecionalidade:
2- Compressão
3- Facilidade de cálculo
4- Difusão
5- Difusão
6- Colisão forte

Questão 5 - Explique o que é um certificado digital e dê exemplos de onde podemos utilizá-lo.

O Certificado Digital é basicamente uma identidade eletrônica para a pessoa física ou jurídica, funcionando como um RG do mundo digital. Esse documento identifica e te representa na internet. Ele pode ser usado, por exemplo, para te reconhecer de forma online em portais oficiais do governo e prefeitura.

Questão 7 – Assinale (F) para as afirmações falsas e (V) para as verdadeiras.

(Falso) MD5 e SHA são funções de resumo de mensagem (funções hash). Esses algoritmos têm a finalidade de garantir a integridade de mensagens de tamanho arbitrário (CESPE/CEBRASPE, 2004, concurso da Polícia Federal para perito criminal federal - informática).

(Verdadeiro) No padrão RSA, a assinatura digital é um código de verificação concatenado a uma mensagem que é o hash da mensagem cifrada com a chave privada de quem emite a mensagem (CESPE/CEBRASPE, 2010, concurso do Banco da Amazônia para técnico científico – tecnologia da informação – redes e telecomunicações).

(Falso) Considerando-se os algoritmos de criptografia tradicionais (RSA, por exemplo), tem-se a garantia que é impossível determinar a chave privada a partir do conhecimento da chave pública (CESPE/CEBRASPE, 2021, concurso para técnico jurídico – tecnologia e informação).

(Falso) O resultado e o tamanho do método criptográfico hash variam de acordo com o tamanho da informação à qual ele seja aplicado (CESPE/CEBRASPE, 2021, concurso da PG-DF para analista jurídico – analista de sistema, suporte e infraestrutura).

(Falso) O desenvolvimento de software seguro é uma funcionalidade presente em todas as ferramentas e padrões existentes no mercado. Assim, o programador precisa focar apenas na criatividade e no atendimento aos requisitos do cliente, pois segurança, hoje, é uma questão secundária (CESPE/CEBRASPE, 2008, concurso do SERPRO para analista de desenvolvimento de sistemas).

(Verdadeiro) A autoridade certificadora é uma entidade responsável por validar a identidade de um usuário em uma infraestrutura de chaves públicas ICP (CESPE/CEBRASPE, 2021, concurso do SEFAZ-AL para auditor fiscal).

(Verdadeiro) O uso de senhas ou a adoção de identificação física, como biometrias, são formas de autenticação para fins de identificação única e exclusiva de usuários (CESPE/CEBRASPE, 2021, concurso do SEFAZ-AL para auditor fiscal).

(Verdadeiro) Apesar de a criptografia moderna estar presente no cotidiano dos usuários, a implantação de mecanismos criptográficos requer diversos cuidados, como a utilização de algoritmos e protocolos conhecidos e extensivamente analisados e o uso de primitivas criptográficas adequadas para cada situação (CESPE/CEBRASPE, 2020, concurso do Ministério da Economia para tecnologia da informação).