

Lista 03 - Criptografia

Professor: Fábio Engel de Camargo
Disciplina: Segurança em Tecnologia da Informação
Meio para entrega: Moodle

1. _____ oferece um mecanismo para obter quatro objetivos em segurança: confidencialidade, integridade, autenticação e não repúdio.
 - a) Associação de Segurança (SA - *Security Association*)
 - b) Camada de Soquetes Seguros (SSL - *Secure Socket Layer*)
 - c) Criptografia
 - d) Nenhuma das alternativas anteriores
2. Uma função de hash forte é projetada de modo que uma mensagem não possa ser forjada, resultando no mesmo hash de uma mensagem legítima.
 - a) Verdadeiro
 - b) Falso
3. O ato de misturar texto claro para gerar texto cifrado é conhecido como _____.
 - a) Decriptação
 - b) Encriptação
 - c) Texto puro
 - d) Texto claro
4. Um algoritmo usado para fins criptográficos é conhecido como um(a) _____.
 - a) Hash
 - b) Chave privativa
 - c) Chave pública
 - d) Cifra
5. Cifras de encriptação podem ser de duas categorias gerais: chave simétrica(privativa) e chave assimétrica (pública).
 - a) Verdadeiro
 - b) Falso

6. Uma cifra de encriptação que use a mesma chave para encriptar e decriptar é chamada de chave _____.
- a) Simétrica (privativa)
 - b) Assimétrica (pública)
 - c) Encriptação de chave
 - d) Nenhuma das alternativas anteriores
7. _____ atesta a identidade de uma entidade, seja o emissor, o computador do emissor, algum dispositivo ou alguma informação.
- a) Não repúdio
 - b) Confidencialidade
 - c) Integridade
 - d) Autenticação
8. Os dois tipos básicos de cifras são transposição e substituição
- a) Verdadeiro
 - b) Falso
9. Um(a) _____ é usado(a) para detectar falsificações.
- a) Função de hash
 - b) cifra
 - c) Valor de hash
 - d) KDC
10. DES, IDEA, RC4 e WEP são exemplo de _____.
- a) Revogação de chave
 - b) Segurança de redes sem fio 802.11b
 - c) Algoritmos (ou padrões) de chave assimétrica
 - d) Algoritmos (ou padrões) simétricos
11. Uma assinatura _____ é uma representação de uma assinatura física armazenada em um formato digital.
- a) Digital
 - b) Digitalizada
 - c) De chave privativa
 - d) De chave pública