Teste de SI

Question 1 Answer
Para que o RSA é comumente utilizado?

a.
Encriptação rápida de comunicações em tempo real

b.
Criptografia de dados e assinaturas digitais

c.
Autenticação de duas vias em redes sem fio

d.
Geração de números aleatórios para uso em criptografia

e.
Proteção de dados em repouso, como em

discos rígidos

Question 2 Answer
Em algoritmos simétricos, como se diferenciam as estratégias de cifragem por substituição e por transposição?

a.
A substituição e a transposição são essencialmente o mesmo método, mas com nomes diferentes

b.
A substituição troca caracteres por outros, enquanto a transposição rearranja a ordem dos caracteres

c.
Na substituição, a ordem dos caracteres é alterada, enquanto na transposição, os caracteres são substituídos

d.
A transposição é um método de encriptação de chave pública, enquanto a substituição usa chaves simétricas

e.
A substituição é um método mais antigo e menos seguro que a transposição

Question 3 Answer
Qual é a principal diferença entre segurança incondicional e segurança computacional em criptografia?

a.
A segurança incondicional depende da capacidade de armazenamento, enquanto a computacional da velocidade de processamento

b.

A segurança incondicional não depende de limitações computacionais, enquanto a segurança computacional sim

c.
A segurança incondicional é sempre baseada em algoritmos de chave pública, enquanto a computacional em chave privada

d.
A segurança incondicional é menos segura do que a computacional

e.
A segurança incondicional usa chaves mais longas do que a segurança computacional

Question 4 Answer
O que caracteriza o algoritmo RSA na criptografia?

a.
Baseia-se na dificuldade de encontrar a raiz quadrada de um número grande

b.
Utiliza dois números primos grandes para gerar um par de chaves, uma pública e outra privada

c.
Depende da computação de logaritmos discretos para segurança

d.
Emprega um algoritmo de hash criptográfico para a geração de chaves

e.
Usa a mesma chave para criptografia e descriptografia

Question 5 Answer

Qual é a característica principal da Cifra de Transposição Colunar?

a.
Inverte a ordem das letras da mensagem original e aplica um deslocamento fixo baseado em uma chave

b.
Substitui cada letra da mensagem por outra letra do alfabeto com base em uma chave numérica

c.
Codifica a mensagem através de um sistema binário, substituindo letras por combinações de 0s e 1s

d.
Reorganiza as letras da mensagem original escrevendo-as em linhas e lendo-

as em colunas segundo uma chave

e.
Usa uma palavra-chave para realizar múltiplas substituições de letras ao longo da mensagem

Question 6 Answer
Em que princípio matemático a segurança do algoritmo RSA se baseia principalmente?

a.
Na impossibilidade de inverter funções de hash criptográficas

b.
Na dificuldade de fatorar o produto de dois números primos grandes

c.
Na complexidade de calcular logaritmos

discretos

d.
Na dificuldade de resolver problemas de curvas elípticas

e.
Na dificuldade de prever a sequência de números aleatórios

Question 7 Answer
Qual das seguintes afirmações melhor descreve a cifra de Vigenère?

a.
É uma técnica de cifragem que utiliza uma série de diferentes cifras de César baseadas em uma palavra-chave

b.
É um tipo de cifra assimétrica que usa um

par de chaves matematicamente relacionadas

c.
Baseia-se na transposição de linhas e colunas de acordo com uma chave numérica

d.
Utiliza um algoritmo de chave pública onde a chave de criptografia é diferente da chave de descriptografia

e.
É uma cifra de substituição simples que usa um deslocamento fixo para todas as letras do alfabeto

Question 8 Answer
Qual é uma desvantagem comum da criptografia assimétrica em comparação com a simétrica?

a.
Processamento mais lento devido à complexidade matemática

b.
Impossibilidade de criptografar mensagens longas

c.
Incompatibilidade com a maioria dos protocolos de internet

d.
Falta de suporte para autenticação de mensagens

e.
Incapacidade de gerar chaves de forma dinâmica

Question 9 Answer

Qual é um dos principais desafios de segurança associados ao problema do logaritmo discreto na criptografia?

a.
Necessidade de atualizações frequentes de chaves

b.
Incapacidade de se adaptar a redes de comunicação de alta velocidade

c.
D

d.
Falhas de segurança em sistemas operacionais que comprometem a aplicação prática

e.

Vulnerabilidade potencial a avanços em computação quântica

Question 10 Answer
Qual das seguintes é uma propriedade essencial das funções hash criptográficas?

a.
Resistência a colisões: é computacionalmente inviável encontrar duas entradas diferentes que produzam o mesmo hash

b.
Compressibilidade: a função hash pode ser comprimida em um arquivo menor

c.
Reversibilidade: a saída da função hash pode ser facilmente convertida de volta para a entrada original

d.
Expansibilidade: a função hash sempre aumenta o tamanho da entrada

e.
Simetria: a função hash trata todas as entradas de maneira igual

Question 11 Answer
Qual é uma característica notável e uma potencial desvantagem do modo Electronic Codebook (ECB) na criptografia de blocos?

a.
ECB permite que um erro na cifragem de um bloco se propague para os blocos seguintes

b.
Cada bloco de texto cifrado é dependente

dos blocos de texto cifrado anteriores

c.
ECB é o modo mais rápido e seguro de operação para criptografia de blocos

d.
Em ECB, a chave de criptografia muda com cada bloco de texto, aumentando a segurança

e.
Blocos idênticos de texto plano resultam em blocos idênticos de texto cifrado, o que pode revelar padrões

Question 12 Answer
Considere um sistema de criptografia simétrica que utiliza uma chave de 256 bits. Qual das seguintes afirmações é mais precisa em relação aos desafios e características deste sistema?

a.
O uso de uma chave de 256 bits automaticamente torna o sistema seguro contra todos os tipos de ataques criptográficos

b.
Uma chave de 256 bits é inerentemente vulnerável a ataques de força bruta devido à sua extensão

c.
O principal desafio é garantir a distribuição segura da chave, pois a força da criptografia depende da sua confidencialidade

d.
Este sistema é considerado inseguro, pois algoritmos simétricos não são adequados para chaves de tamanho tão grande

e.
A principal vantagem deste sistema é a sua velocidade comparativamente lenta, o que aumenta a segurança

Question 13 Answer
Qual é a principal função do arquivo shadow em sistemas Unix/Linux?

a.
Armazenar backups das configurações do sistema

b.
Registrar tentativas de login e atividades de rede

c.
Armazenar as senhas dos utilizadores de forma segura, geralmente usando hash e sal

d.
Monitorar as atividades do utilizador no sistema

e.
Controlar o acesso dos utilizadores aos comandos do terminal

Question 14 Answer
O que é um Message Authentication Code (MAC) em criptografia?

a.
Um código usado para verificar a integridade e autenticidade de uma mensagem, combinando a mensagem com uma chave secreta
b.
Um protocolo para troca segura de chaves criptográficas
c.

Uma técnica para aumentar a velocidade da criptografia simétrica

d.

Um código gerado por uma função hash sem a necessidade de uma chave secreta

e.

Um algoritmo para encriptar mensagens de texto