Exercicios de Revisão

Criptografia Aplicada

Q1: Por que os algoritmos de criptografia usam chaves? Indique todas que aplicarem.

A. Para tornar os algoritmos mais rápidos.

B. Para tornar os algoritmos mais simples.

C. Para permitir que os algoritmos de criptografia sejam padronizados.

D. Para permitir que um único algoritmo possa proteger várias comunicações de pessoas diferentes.

E. Para que ele possa funcionar em rede.

Q2: O que significa ESPAÇO DE CHAVES em um algoritmo de criptografia?

A. É o tamanho da chave.

B. É sempre 2 elevado ao tamanho da chave em bits.

C. É um número que pode ser maior que 2 elevado ao tamanho da chave em bits.

D. É o número de valores diferentes que uma chave pode assumir.

E. É um número igual ao número de letras no alfabeto.

Q3. Por que a função de XOR é comumente usada em criptografia? Indique todas as que aplicarem.

A. Porque ela é inversível: A xor B = C e C xor B = A.
B. Porque é uma operação simples e muito rápida.
C. Porque é uma operação muito segura.
D. Porque é uma operação que pode ser feita em binário.
E. Porque é uma operação ONE-WAY, isto é, não inversível.

Q4. Indique a alternativa que define corretamente as propriedades de Confusão e Difusão em algoritmos de criptografia. Indique todas que aplicarem.

A. Confusão indica o quanto a mensagem criptografada é diferente da original.
B. Difusão indica que mensagens com pequenas diferenças, mesmo se criptografadas com a mesma chave, geram resultados totalmente diferentes.
C. Confusão indica que cada bit da mensagem criptografada dependente de vários bits da chave de criptografia.
D. Difusão indica que mensagens semelhantes antes da criptografia, geram mensanges semelhantes após a criptografia.
E. Difusão indique que a chave de criptografia tem muitos bits diferentes.

Q5: Quais propriedades o algoritmo de XOR cipher simples, sem vetor de inicialização, satisfaz?

A. Apenas Confusão.

B. Apenas Difusão.

C. Confusão e Difusão.

D. Nenhuma das duas.

E. Depende do tamanho da chave.

Q6: Analisando o resultado a seguir, quais propriedades o algoritmo RC4 (baseado em XOR) satisfaz?

MSG= TESTE, K=0102030405, CRIPTO= kG0mVqR44gfByQ==
MSG= TESTE, K=0202030405, CRIPTO= CH/gngCwgy5kZw==
MSG= PESTE, K=0102030405, CRIPTO= kGkmVqR44gfByQ==

A. Apenas Confusão.

B. Apenas Difusão.

C. Confusão e Difusão.

D. Nenhuma das duas, pois é baseado em XOR.

E. Depende do valor da chave e do tamanho da mensagem.

Q7. A Cifra de Feistel divide a mensagem em blocos e faz muitos rounds de XOR com chaves diferentes. Qual a razão desse procedimento? Indique todas as que aplicarem.

A. Tornar o algoritmo mais eficiente permitindo o processamento em paralelo.
B. Aumentar a confusão e difusão do algoritmo.
C. Tonar o algoritmo seguro mesmo para chaves muito pequenas.
D. Permitir a criptografia de mensagens de qualquer tamanho.
E. Tornar a descriptografia por análise de frequência mais difícil.

Q8. Os algoritmos denominados block ciphers dividem a mensagem em blocos de tamanho igual antes de efetuar a criptografia. Em relação a como os blocos são processados, relacione as colunas.

A. Permite o processamento paralelo, mas não confere integridade.

B. Considerado obsoleto, pois criptografa cada bloco separadamente.

C. Não permite que os blocos sejam processados de maneira paralela.

D. Permite processamento paralelo e confere integridade.

I. ECB: Electronic Codebook Mode

II. CBC: Cipher Block Chaining

III. Counter Mode

IV. Galois Counter Mode

Q9. Qual a diferença entre os algoritmos de criptografia simétricos e assimétricos?

A. Apenas algoritmos assimétricos podem ser processados em blocos.

B. Algoritmos assimétricos utilizam chaves diferentes para criptografia e descriptografia.

C. Algoritmos simétricos são sempre do tipo stream ciphers.

D. Algoritmos assimétricos são geralmente baseados em permutação e substituição de bits.

E. Algoritmos que usam chaves grandes, maiores que 1024 bits são denominados assimétricos.

Q10: Alguns algoritmos usam uma chave de criptografia temporária chamada de chave de sessão. Do ponto de vista do uso da criptografia, o que é uma sessão? Indique todas que aplicarem (existem 3).

A. Todos os pacotes trocados com um mesmo computador de destino.

B. Todas as páginas acessadas em um mesmo servidor Web.

C. Mensagens trocadas após a autenticação do usuário até o momento em que ele não deseja mais continuar a usar a aplicação.

D. Todas as mensagens trocadas até um certo intervalo de tempo.

E. Todas as mensagens trocadas até que um volume de tráfego seja atingido.

Q11. O algoritmo RSA é um algoritmo assimétrico, e é considerado unidirecional, porque ele só oferece confidencialidade se as chaves forem usadas em um modo específico. Que modo é esse?

A. Quando a criptografia é com a chave privada e a descriptografia com a pública.

B. Quando a criptografia é com a chave pública e a descriptografia com a chave privada.

C. Quando a criptografia e descriptografia são feitas com a chave privada.

D. Quando a criptografia e descriptografia são feitas com a chave pública.

E. Quando as chaves pública e privadas nunca forem transmitidas em aberto pela rede .

RA3

Q12. Uma comunicação segura pela rede utiliza simultaneamente os algoritmos RSA e AES. Qual a função de cada um desses algoritmos?

A. Como o RSA não é bidirecional, ele criptografa as mensagens em um sentido e o AES no outro.

B. O AES sozinho precisa de uma chave simétrica que não pode ser combinada pela rede. O RSA permite que o AES opere com chaves assimétricas.

C. O RSA permite combinar um segredo entre duas partes. Esse segredo é usado para criar a chave de sessão simétrica utilizada pelo AES.

D. O AES e o RSA nunca são usados simultaneamente, porque o primeiro é simétrico e o segundo assimétrico.

RA3

Q13. Em relação aos algoritmos de chave pública, relacione as colunas utilizando a definição mais apropriada para cada algoritmo.

A. Algoritmo cuja segurança é baseada na dificuldade de fatorar grandes números em números primos.

B. Algoritmo no qual a relação entre as chaves privada e pública é feita através de operações em curvas eliptcas.

C. Algoritmo que combina um segredo compartilhado entre duas partes pela rede.

D. Algoritmo que combinar um segredo entre duas partes usando operações em curvas elípticas.

I. RSA

II. ECC

III. Diffie-Hellmann

IV. ECC Diffie-Hellmann

RA3

Q14. Qual são as diferenças entre o princípio de criptografia baseado em curvas elípticas (ECC) em relação ao RSA? Indique todas que aplicarem (existem 3)

A. A segurança do ECC não é baseada na dificuldade de fatoração de grandes números em números primos.

B. ECC precisa de chaves muito menores que o RSA para ofecer o mesmo nível de segurança.

C. Com um único par de chaves, o ECC pode proteger mensagens nos dois sentidos, e o RSA em apenas um.

D. O ECC precisa aumentar menos o tamanho da chave que o RSA, para se proteger do aumento da capacidade dos computadores.

E. O ECC é mais seguro, mas é consome mais recursos computacionais, não sendo adequado para IoT.