1º TESTE DE SEGURANÇA INFORMATICA E DAS TELECOMUNICAÇÕES

Turma: LECC41 [Pontuação máxima: 100] Data: 24 Abril 2024

1º Semestre **Correção** Duração: 80 min

Docente: Eng. Emírcio Zeca Vieira 1º Semestre

NOME: Nº

1. Uma pessoa conseguiu gerar o mesmo valor aplicando uma função de hash para duas mensagens diferentes e com semânticas totalmente opostas. O algoritmo de hash utilizado é também utilizado para assinatura digital em um sistema. Nesse contexto, analise as questões a seguir:

   I. É uma situação esperada e que não representa um problema porque os algoritmos de assinatura digital tratam essas questões;

   II. O algoritmo de hash utilizado possui uma baixa resistência à colisão; e

   III. A função de hash em questão gera saídas com tamanhos variáveis.

   6

   Selecione a alinea correcta.

   A) Apenas I.
   B) Apenas II.
   C) Apenas III.
   D) Apenas II e III.
   E) I, II e III.

2. A segurança da informação se refere à proteção das informações tanto corporativas quanto pessoais. São diversos mecanismos recomendados para aplicação de segurança. Dentre os mecanismos de segurança da informação, há aqueles que apoiam os controlos lógicos, como o uso de funções de "hashing" ou checagem, que geram um código único usado para confirmar que os dados não foram alterados. Qual é esse mecanismo?

   6

   Selecione a afirmação correcta:

   A) Controles físicos.
   B) Mecanismos de criptografia.
   C) Mecanismos de controle de acesso.
   D) Mecanismos de garantia da integridade.

3. Uma empresa vai dar ênfase a característica de Segurança de Informação, no qual pretende-se garantir que os dados sejam mantidos em segredo, gerido e controlando o acesso às informações, evitando-se o compartilhamento não autorizado de dados. Essa caraterística é conhecida como:

   10

   Selecione a afirmação correcta e justifique:

   A) Confidencialidade;
   B) Integridade;
   C) Disponibilidade; e
   D) Veracidade.

O princípio é aplicado em diversos contextos, como na comunicação entre partes, no armazenamento de dados, em transações financeiras, em ambientes corporativos, entre outros. A confidencialidade é essencial para proteger informações pessoais, financeiras, comerciais e estratégicas contra acesso não autorizado, roubo de identidade, espionagem industrial e outras ameaças à segurança.

4. Uma empresa de comunicações trabalha com mensagens com criptografia simétrica. Um exemplo de algoritmo para esse tipo de criptografia é: 10

   Selecione a afirmação correcta e justifique:
   A) RSA;
   B) 3DES;
   C) AES; e
   D) Diffie-Helman.

3DES é um algoritmo de criptografia simétrica que aplica a cifra DES (Data Encryption Standard) três vezes em sequência para melhorar a segurança. O DES é um algoritmo de chave simétrica que foi amplamente utilizado, porém, com o tempo, tornou-se vulnerável a ataques de força bruta devido ao tamanho curto da chave.

5. Escolha uma das opções e justifique que o certificado digital visa a garantir a associação de uma chave pública a uma pessoa, entidade ou host. 10

   Para isso, a Autoridade Certificadora (AC) que emite o certificado digital deve:

   Selecione a afirmação correcta e justifique.

   A) Apenas gerar sua assinatura digital para o certificado emitido.

   B) Apenas fazer a criptografia assimétrica do certificado emitido;

   C) Apenas fazer a criptografia simétrica do certificado emitido; e

   D) Gerar sua assinatura digital para o certificado emitido e fazer a criptografia assimétrica desse certificado.

Uma Autoridade Certificadora (AC) é uma entidade, pública ou privada, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).

6. Na figura 3, Bob deseja enviar uma longa mensagem para Alice. Ele coloca sua longa mensagem original em uma função de hash, que gera um resumo curto dessa mensagem. Em seguida, utiliza sua chave criptográfica privada para criptografar o hash resultante (resumo). A mensagem original, em texto aberto, e o resumo criptografado dessa mensagem são, então, enviados para Alice.

10

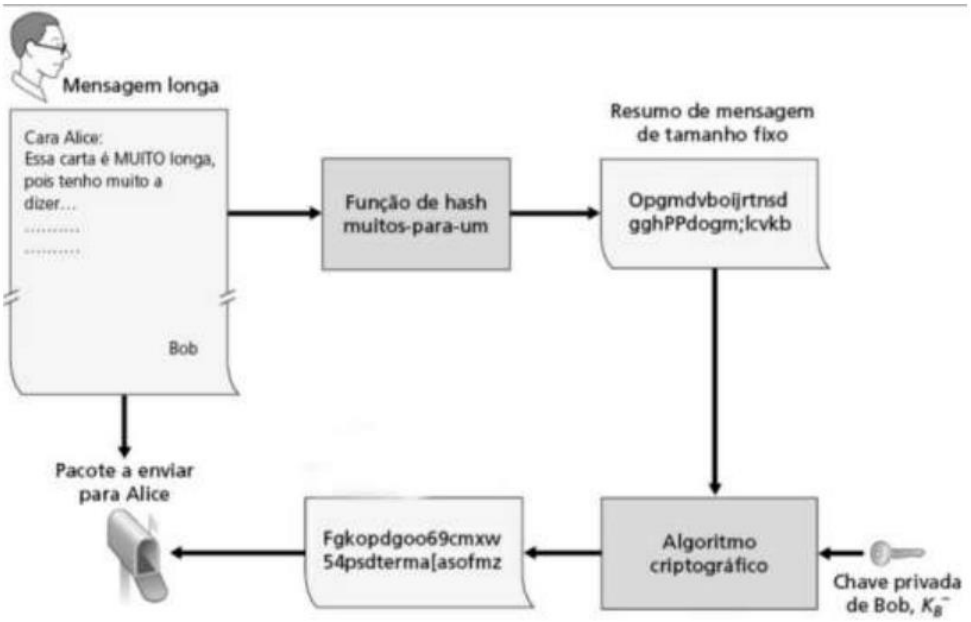

Figura 3
Fonte: Kurose; Ross (2021, s/p)

Esse processo de envio da mensagem longa de Bob para Alice, ilustrado na figura 3, é denominado:

Selecione a afirmação correcta e justifique:

A) Certificação Digital;

B) **Assinatura Digital**;

C) Criptografia Simétrica;

D) Criptografia Assimétrica;

E) Autoridade Certificadora.

Para garantir a autenticidade da mensagem, Bob assina digitalmente usando a sua chave privada. Isso permite que Alice consiga verificar que a mensagem foi realmente enviada por Bob e não foi alterada durante a transmissão.

No processo de envio da mensagem de Bob para Alice, houve o uso da chave privada de Bob para criptografar a mensagem.

7. O procedimento de descriptografia do algoritmo RC2, toma como entrada quatro palavras de texto cifrado: R [0] R [1] R [2] R [3], que formam um bloco de dados criptografados. Cada bloco de dados será descriptografado usando as mesmas 64 palavras da chave secreta expandida: K [0] K [1] ... K [63].

Quais são as etapas de descriptografia que são realizadas em cada bloco de texto cifrado? 24

1. Inicialização do contador K para 63;
2. Execução de cinco rodadas de mistura R;
3. Execução de uma Rodada R-Mashing;
4. Execução de seis rodadas de mistura R;
5. Execução de uma Rodada R-Mashing;
6. Execução de cinco rodadas de mistura R.

8. Alice e Bob devem negociar um número inteiro (qualquer) e um número primo, pois é de difícil factoração de produtos de números primos, sendo α = 3 e q = 17.

Após isso, cada um deles escolhe um número secreto. Esses números não serão transmitidos, sendo Alice: X_a = 54 e Bob: X_b = 24. 24

Qual é a chave privada de Bob e da Alice?

1. Alice calcula $Y_a = \alpha^{Xa} \ mod \ q = 3^{54} \ mod \ 17 = 15$ e de seguida envia o $Y_a = 15$
2. Bob calcula $Y_b = \alpha^{Xb} \ mod \ q = 3^{24} \ mod \ 17 = 16$ e de seguida envia o $Y_b = 16$ para Alice;
3. *Chave secreta* de Alice: $K = (Y_b)^{(Xa)} \ mod \ q = (16)^{(54)} \ mod \ 17 = 1$ *Chave secreta* de Bob: $K = (Y_b)^{(Xb)} \ mod \ q = (15)^{(24)} \ mod \ 17 = 1$

A chave secreta de Alice e a chave secreta de Bob são iguais.

Bom trabalho! *"É sem medo de errar que conseguimos os melhores acertos."*