Bacharelado em Ciência da Computação

CCMP3079 Segurança de Redes de Computadores

Atividade Cap. 09

Prof. Sérgio Mendonça

Nome Completo: Luan Valentino Sampaio Marques

Data: 18/12/2023

Universidade Federal do Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
+55 (87) 3764-5500
http://www.ufape.edu.br

Questões retiradas do livro-texto da disciplina

Conforme conversamos em sala de aula, as atividades devem ser realizadas para apresentação e discussão em sala, sempre nas aulas das quintas-feiras, atribuindo ao estudante uma nota de 0 ou 1 por cada atividade realizada e apresentada.

Questão 1

Quais são os principais elementos de um criptossistema de chave pública?

Resposta:

Um criptossistema de chave pública, também conhecido como criptografia assimétrica, é um sistema de criptografia que utiliza um par de chaves: uma chave pública e uma chave privada. Os principais elementos de um criptossistema de chave pública são:

1. **Chave Pública**: Uma chave que pode ser compartilhada livremente e é usada para criptografar mensagens ou verificar assinaturas digitais. Ela não revela informações sobre a chave privada.

2. **Chave Privada**: Uma chave que é mantida em segredo pelo proprietário e é usada para descriptografar mensagens recebidas ou para assinar digitalmente uma mensagem.

3. **Algoritmo de Criptografia**: Um conjunto de regras matemáticas que define como os dados são criptografados e descriptografados. Exemplos incluem RSA, ECC (Curvas Elípticas), ElGamal, etc.

4. **Algoritmo de Assinatura Digital**: Um mecanismo que usa a chave privada para criar uma assinatura digital, que pode ser verificada com a chave pública correspondente.

5. **Função de Hash**: Utilizada para criar um resumo fixo de tamanho fixo a partir de dados arbitrários. É fundamental para a integridade dos dados e para a criação de assinaturas digitais.

Questão 2

Quais são os papéis da chave pública e da privada? Descreva-os com detalhes e com exemplos.

Resposta:

A chave pública e a chave privada desempenham papéis complementares em um criptossistema de chave pública:

1. **Chave Pública**: Esta chave é usada para criptografar dados que apenas a chave privada correspondente pode descriptografar. Por exemplo, se Alice deseja enviar uma mensagem segura para Bob, ela usará a chave pública de Bob para criptografar a mensagem. Quando Bob recebe a mensagem, ele usa sua chave privada para descriptografá-la.

Exemplo: No algoritmo RSA, se a chave pública de Bob for composta pelos números e e n, e ele deseja criptografar uma mensagem M, ele calcula o texto cifrado C como:

$$C = M^e \mod n.$$

2. **Chave Privada**: Esta chave é usada para descriptografar dados criptografados com a chave pública correspondente. Além disso, a chave privada é usada para assinar digitalmente mensagens, garantindo autenticidade e integridade.

Exemplo: Usando o RSA novamente, Bob usa sua chave privada d e n para descriptografar o texto cifrado C de Alice:

$$M = C^d \mod n.$$

A chave privada também é usada para criar uma assinatura digital. Se Bob quiser enviar uma mensagem assinada a Alice, ele usa sua chave privada para criar a assinatura. Alice, então, usa a chave pública de Bob para verificar se a assinatura é autêntica.

Questão 3

Quais requisitos os criptossistemas de chave pública precisam cumprir para serem considerados como um algoritmo seguro?

Resposta:

Para que um criptossistema de chave pública seja considerado seguro, ele deve atender aos seguintes requisitos:

1. **Confidencialidade**: Mensagens criptografadas com a chave pública só devem ser decifradas pela chave privada correspondente. O algoritmo deve ser computacionalmente seguro contra ataques que tentem recuperar a mensagem original sem a chave privada.

2. **Integridade**: Deve ser garantido que a mensagem recebida não foi alterada. Funções de hash criptográficas são frequentemente usadas para garantir a integridade dos dados.

3. **Autenticidade**: A chave privada é usada para assinar digitalmente as mensagens, enquanto a chave pública correspondente é usada para verificar a assinatura. Isso garante que a mensagem veio da fonte esperada.

4. **Não-repúdio**: O remetente da mensagem não deve ser capaz de negar a autoria da mensagem. A assinatura digital associada ao criptossistema garante esse atributo.

5. **Resistência a ataques de força bruta**: A chave privada deve ser suficientemente longa e o algoritmo suficientemente robusto para resistir a ataques de força bruta ou a outros métodos de criptoanálise.

Questão 4

Descreva, em termos gerais, um procedimento eficiente para se escolher um número primo.

Resposta:

Para escolher um número primo de maneira eficiente, é comum usar testes probabilísticos que verificam a primalidade de um número. Um procedimento eficiente geralmente envolve os seguintes passos:

1. **Gerar um número aleatório grande**: Escolha um número grande aleatório n, que é o candidato a primo.

2. **Aplicar um teste de primalidade probabilístico**: Use um teste como o teste de Miller-Rabin ou o teste de Fermat para verificar se o número é primo. Esses testes não garantem que um número seja primo, mas indicam se ele é provavelmente primo com um alto grau de confiança. Para melhorar a precisão, o teste pode ser repetido várias vezes com diferentes bases.

3. **Verificação adicional (opcional)**: Para certos sistemas críticos, pode ser interessante aplicar um teste determinístico (como o Teste de Primalidade AKS) para confirmar

que o número é primo, embora esses testes possam ser menos eficientes para números muito grandes.

4. **Repetição se necessário**: Se o número não for primo, gere outro número aleatório e repita o procedimento até que um número primo seja encontrado.

Esse procedimento permite escolher números primos de tamanhos desejados de maneira eficiente e segura, o que é fundamental em muitos algoritmos de criptografia de chave pública, como RSA e Diffie-Hellman.

Questão 5

Antes da descoberta de quaisquer esquemas de chave pública específicos, como RSA, uma prova de existência foi desenvolvida, cuja finalidade era demonstrar que a encriptação de chave pública é possível em teoria. Considere as funções $f_1(x_1) = z_1$; $f_2(x_2, y_2) = z_2$; $f_3(x_3, y_3) = z_3$, onde todos os valores são inteiros com $1 \leq x_i, y_i, z_i \leq N$. A função f_1 pode ser representada por um vetor M1 de tamanho N, em que a k-ésima entrada é o valor de $f_1(k)$. De modo semelhante, f_2 e f_3 podem ser representados pelas matrizes M2 e M3 de tamanho $N \times N$. A intenção é indicar o processo de encriptação/decriptação por pesquisas de tabela para aquelas com valores muito grandes de N. Essas tabelas seriam impraticavelmente grandes, mas, a princípio, poderiam ser construídas.

O esquema funciona da seguinte forma: construa M1 com uma permutação aleatória de todos os inteiros entre 1 e N; ou seja, cada inteiro aparece exatamente uma vez em M1. Construa M2, de modo que cada linha contenha uma permutação aleatória dos primeiros N inteiros. Finalmente, preencha M3 para satisfazer a seguinte condição:

$$f_3(f_2(f_1(k), p), k) = p \quad \text{para todo } k, p \text{ com } 1 \leq k, p \leq N.$$

Resumindo,

1. M1 toma uma entrada k e produz uma saída x.
2. M2 toma as entradas x e p, dando a saída z.
3. M3 toma as entradas z e k e produz p.

(a) Descreva o uso desse conjunto de tabelas para realizar a encriptação e decriptação entre dois usuários.

Resposta:

Para encriptação, o remetente deve escolher um índice k e um valor de mensagem p. Ele usa M1 para obter um valor intermediário x, depois utiliza M2 com x e p para obter uma saída z. O par (z, k) é então enviado ao destinatário.

Para decriptação, o destinatário utiliza M3 com z e k para recuperar o valor original p.

(b) Demonstre que esse é um esquema seguro.

Resposta:

Esse esquema é seguro porque cada função f_1, f_2, e f_3 depende de tabelas de permutação aleatórias que são únicas e secretas. Como cada permutação é aleatória e única, é computacionalmente inviável para um atacante prever as saídas sem conhecer as tabelas.

Questão 6

Realize a encriptação e decriptação usando o algoritmo RSA, como na Figura 9.5, para o seguinte:

(a) $p = 7$; $q = 11$, $e = 7$; $M = 5$;

(b) $p = 5$; $q = 11$, $e = 3$; $M = 9$;

(c) $p = 7$; $q = 11$, $e = 17$; $M = 8$;

(d) $p = 11$; $q = 13$, $e = 11$; $M = 7$;

(e) $p = 17$; $q = 31$, $e = 7$; $M = 2$.

Resposta:
Para calcular a encriptação usando RSA, precisamos dos seguintes passos:

1. Calcular $n = p \times q$ e $\phi(n) = (p-1)(q-1)$.
2. Escolher e tal que $1 < e < \phi(n)$ e $\gcd(e, \phi(n)) = 1$.
3. Calcular a chave privada d como o inverso multiplicativo de $e \mod \phi(n)$.
4. Para encriptar a mensagem M, calcular $C = M^e \mod n$.
5. Para decriptar o texto cifrado C, calcular $M = C^d \mod n$.

Aplicando para cada caso:

(a) $n = 77$, $\phi(n) = 60$, $e = 7$, $d = 43$, $C = 5^7 \mod 77 = 3$, $M = 3^{43} \mod 77 = 5$.

(b) $n = 55$, $\phi(n) = 40$, $e = 3$, $d = 27$, $C = 9^3 \mod 55 = 14$, $M = 14^{27} \mod 55 = 9$.

(c) $n = 77$, $\phi(n) = 60$, $e = 17$, $d = 53$, $C = 8^{17} \mod 77 = 57$, $M = 57^{53} \mod 77 = 8$.

(d) $n = 143$, $\phi(n) = 120$, $e = 11$, $d = 11$, $C = 7^{11} \mod 143 = 106$, $M = 106^{11} \mod 143 = 7$.

(e) $n = 527$, $\phi(n) = 480$, $e = 7$, $d = 343$, $C = 2^7 \mod 527 = 128$, $M = 128^{343} \mod 527 = 2$.

Questão 7

Em um sistema de chave pública usando RSA, você intercepta o texto cifrado $C = 10$ enviado a um usuário cuja chave pública é $e = 5$ e $n = 35$. O objetivo é encontrar o texto claro M.

Para encontrar o texto claro, precisamos determinar o valor de M tal que:

$$C \equiv M^e \pmod{n}$$

Ou seja:

$$10 \equiv M^5 \pmod{35}$$

Primeiro, precisamos encontrar o valor de M que satisfaz a congruência acima. Para isso, testamos valores possíveis para M de 0 a 34, verificando qual deles satisfaz a equação:

1. **Testando $M = 0$:**

$$0^5 \equiv 0 \pmod{35}$$

Não satisfaz.

2. **Testando $M = 1$:**

$$1^5 \equiv 1 \pmod{35}$$

Não satisfaz.

3. **Testando $M = 2$:**

$$2^5 = 32$$

$$32 \pmod{35} = 32$$

Não satisfaz.

4. **Testando $M = 3$:**

$$3^5 = 243$$

$$243 \pmod{35} = 243 - 6 \cdot 35 = 243 - 210 = 33$$

Não satisfaz.

5. **Testando $M = 4$:**

$$4^5 = 1024$$

$$1024 \pmod{35} = 1024 - 29 \cdot 35 = 1024 - 1015 = 9$$

Não satisfaz.

6. **Testando $M = 5$:**

$$5^5 = 3125$$

$$3125 \pmod{35} = 3125 - 89 \cdot 35 = 3125 - 3115 = 10$$

Satisfaz.

Portanto, o texto claro M é 5.

Resposta: $M = 5$