Bacharelado em Ciência da Computação

CCMP3079 Segurança de Redes de Computadores

Atividade Cap. 10

Prof. Sérgio Mendonça

Nome Completo: Luan Valentino Sampaio Marques

Data: 05/02/2024

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

Os usuários A e B utilizam a técnica de troca de chaves Diffie-Hellman com um primo comum $q = 71$ e uma raiz primitiva $\alpha = 7$.

(a) Se o usuário A tem chave privada $X_A = 5$, qual é a chave pública de A, Y_A?

A chave pública de A é calculada como $Y_A = \alpha^{X_A} \mod q = 7^5 \mod 71$.

$$7^5 = 16807 \quad \text{e} \quad 16807 \mod 71 = 49$$

Portanto, a chave pública de A é $Y_A = 49$.

(b) Se o usuário B tem chave privada $X_B = 12$, qual é a chave pública de B, Y_B?

A chave pública de B é calculada como $Y_B = \alpha^{X_B} \mod q = 7^{12} \mod 71$.

$$7^{12} = 13,841,287,201 \quad \text{e} \quad 13,841,287,201 \mod 71 = 64$$

Portanto, a chave pública de B é $Y_B = 64$.

(c) Qual é a chave secreta compartilhada?

A chave secreta compartilhada é calculada por ambos como $K = Y_B^{X_A} \mod q$ para A e $K = Y_A^{X_B} \mod q$ para B. Ambas as operações resultam no mesmo valor:

$$K = 64^5 \mod 71 = 16807 \mod 71 = 49$$

Portanto, a chave secreta compartilhada é $K = 49$.

Questão 2

Considere um esquema Elgamal com um primo comum $q = 71$ e uma raiz primitiva $\alpha = 7$.

(a) Se B tem chave pública $Y_B = 3$ e A escolheu um inteiro aleatório $k = 2$, qual é o texto cifrado de $M = 30$?

O texto cifrado consiste em dois valores C_1 e C_2. Calculamos primeiro C_1:

$$C_1 = \alpha^k \mod q = 7^2 \mod 71 = 49$$

E agora C_2:

$$C_2 = M \cdot Y_B^k \mod q = 30 \cdot 3^2 \mod 71 = 30 \cdot 9 \mod 71 = 270 \mod 71 = 57$$

Portanto, o texto cifrado é $(C_1, C_2) = (49, 57)$.

(b) Se A, então, selecionar um valor diferente de k, de modo que a codificação de $M = 30$ seja $C = (59, C_2)$, qual é o inteiro C_2?

Sabemos que $C_1 = 59$. Como $C_1 = \alpha^k \mod q$, precisamos encontrar k tal que $7^k \mod 71 = 59$. Calculando o valor de k, temos:

$$k = \log_7 59 \mod 71$$

Através de tentativa e erro ou tabela pré-calculada, encontramos que $k = 10$. Agora, podemos calcular C_2:

$$C_2 = M \cdot Y_B^k \mod q = 30 \cdot 3^{10} \mod 71 = 30 \cdot 59 \mod 71 = 1770 \mod 71 = 54$$

Portanto, o valor de C_2 é 54.

Questão 3

Demonstre que as duas curvas elípticas da Figura 10.4 satisfazem, cada uma, as condições para um grupo sobre os números reais.

Resposta: Para que uma curva elíptica forme um grupo sobre os números reais, ela deve satisfazer três condições principais:

1. Fechamento: Para quaisquer dois pontos P e Q na curva, a soma $P + Q$ também deve estar na curva.
2. Associatividade: Para quaisquer três pontos P, Q, e R na curva, a equação $(P + Q) + R = P + (Q + R)$ deve ser válida.
3. Elemento neutro e inverso: Deve existir um ponto neutro O tal que $P + O = P$ para qualquer ponto P na curva, e para cada ponto P, deve existir um ponto $-P$ tal que $P + (-P) = O$.

As curvas elípticas mencionadas na Figura 10.4 devem ser verificadas quanto a essas propriedades.

Questão 4

(4, 7) é um ponto na curva elíptica $y^2 = x^3 - 5x + 5$ sobre números reais?

Resposta: Para verificar se o ponto $(4, 7)$ está na curva, substituímos $x = 4$ e $y = 7$ na equação da curva:

$$7^2 = 4^3 - 5(4) + 5 \implies 49 = 64 - 20 + 5 = 49$$

Como a igualdade é verdadeira, o ponto $(4, 7)$ está de fato na curva.