

Cryptography and Network Security | (6th Edition)

Chapter 9, Problem 2P

Bookmark

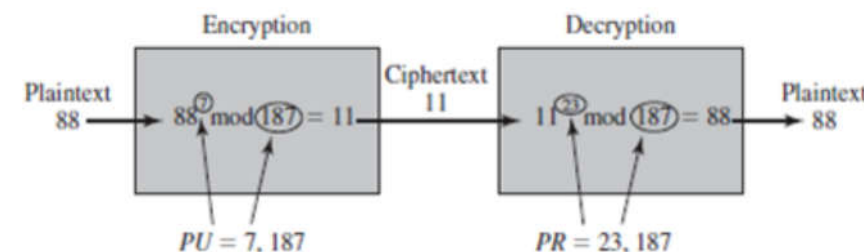
Show all steps:

ON

Problem

Perform encryption and decryption using the RSA algorithm, as in Figure, for the following:

Figure Example of RSA Algorithm



a. $p = 3$; $q = 11$; $e = 7$; $M = 5$

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

Hint: Decryption is not as hard as you think; use some finesse.

Step-by-step solution

Step 1 of 7

Rivest, Shamir, Adleman (RSA) algorithm:

- RSA is the first public-key encryption algorithm.
- It uses public key to encrypt the content and the private secret key to decrypt the content.
- Two large prime numbers are used to create and publish the public key and the prime numbers are kept in secret to decode the message.
- Key generation:
 - o Step 1: Select two prime numbers "p" and "q".
 - o Step 2: Calculate $n = p \times q$ (1)
 - o Step 3: Calculate $\phi(n) = (p - 1)(q - 1)$ (2)
 - o Step 4: Select an integer "e" and it should be in the following state:
 $\gcd(\phi(n), e) = 1$; $1 < e < \phi(n)$ (3)
 - o Step 5: Calculate d and its value fulfills the following condition:
 $de \bmod \phi(n) = 1$ (4)
 - o Step 6: Encryption:
 - Plain text $M < n$.
 - Cipher text $C = M^e \pmod{n}$ (5)
 - o Step 7: Decryption:
 - Cipher text C.
 - Plain text $M = C^d \pmod{n}$ (6)

[Comment](#)

Step 2 of 7

Note: Refer the "Figure 21.6" in text book.

a.

Encryption:

• $P = 3$, $q = 11$, $e = 7$, $M = 5$

• Calculate $n = p \times q$:

o Apply the p value and q value in formula (1).

$$n = p \times q$$

$$n = 3 \times 11$$

$$n = 33$$

• Calculate $\phi(n)$:

o Apply the p value and q value in formula (2).

$$\phi(n) = (p - 1)(q - 1)$$

$$\phi(n) = (3 - 1)(11 - 1)$$

$$\phi(n) = 2 \times 10$$

$$\phi(n) = 20$$

• Calculate d:

o Apply the $\phi(n)$ value in $de \bmod \phi(n) = 1$ to find the d value.

$$de \bmod 20 = 1 \text{ (7)}$$

$$\text{Note: } d < 20$$

Consider that the value of "d" is 3; this value can be calculated by trial and error method applied over the equation (7).

$$d = 3$$

$$\text{Because } 3 \times 7 = 21$$

$$21 \bmod 20 = 1, \text{ it satisfies the condition } de \bmod \phi(n) = 1.$$

• Encrypt the plain text into Cipher text:

o Apply the M, e, n value in formula (5).

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

$$C = 5^7 \bmod 33$$

$$C = 78,125 \bmod 33$$

$$C = 14$$

Decryption:

• Decrypt the Cipher text into plain text:

o Apply the C, d, n value in formula (6).

$$M = C^d \pmod{n}$$

$$M = 14^3 \bmod 33$$

$$M = 2,744 \bmod 33$$

$$M = 5$$

b.

Encryption:

• $P = 5$, $q = 11$, $e = 3$, $M = 9$.

• Calculate $n = p \times q$:

o Apply the p value and q value in formula (1).

$$n = p \times q$$

$$n = 5 \times 11$$

$$n = 55$$

• Calculate $\phi(n)$:

o Apply the p value and q value in formula (2).

$$\phi(n) = (p - 1)(q - 1)$$

$$\phi(n) = (5 - 1)(11 - 1)$$

$$\phi(n) = 4 \times 10$$

$$\phi(n) = 40$$

• Calculate d:

o Apply the $\phi(n)$ value in $de \bmod \phi(n) = 1$ to find the "d" value.

$$de \bmod 40 = 1 \text{ and } d < 40$$

$$d = 21$$

$$\text{Because } 27 \times 3 = 81$$

$$81 \bmod 40 = 1, \text{ it satisfies the condition } de \bmod \phi(n) = 1$$

• Encrypt the plain text into Cipher text:

o Apply the M, e, n value in formula (5).

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

$$C = 9^3 \bmod 55$$

$$C = 729 \bmod 55$$

$$C = 14$$

Decryption:

• Decrypt the Cipher text into plain text:

o Apply the C, d, n value in formula (6).

$$M = C^d \pmod{n}$$

$$M = 14^{21} \bmod 55$$

$$M = 8,819,763,977,946,281,130,444,984,418,304 \bmod 55$$

$$M = 9$$

[Comment](#)

Step 3 of 7

c.

Encryption:

• $P = 7$, $q = 11$, $e = 17$, $M = 8$

• Calculate $n = p \times q$:

o Apply the p value and q value in formula (1).

$$n = p \times q$$

$$n = 7 \times 11$$

$$n = 77$$

• Calculate $\phi(n)$:

o Apply the p value and q value in formula (2).

$$\phi(n) = (p - 1)(q - 1)$$

$$\phi(n) = (7 - 1)(11 - 1)$$

$$\phi(n) = 6 \times 10$$

$$\phi(n) = 60$$

• Calculate d:

o Apply the $\phi(n)$ value in $de \bmod \phi(n) = 1$ to find the d value.

$$de \bmod 60 = 1 \text{ and } d < 60$$

$$d = 23$$

$$\text{Because } 53 \times 17 = 901$$

$$901 \bmod 60 = 1, \text{ it satisfies the condition } de \bmod \phi(n) = 1$$

• Encrypt the plain text into Cipher text:

Post a question

Answers from our experts for your tough homework questions

Enter question

CONTINUE TO POST

20 questions remaining

My Textbook Solutions

Add a textbook

Cryptography and Network Security, 6th Edition

Numerical Methods, 6th Edition

View all solutions

Chegg tutors who can help right now

Alfredo
Rasmussen College

95

Michael
Fuller Theological Seminary

223

Gorank
Indian Institute of Technology

127

FIND ME A TUTOR

Was this solution helpful? 0 0