CHAPTER 28

Network Security

Exercises

1. Substitute the character that is 4 characters down. For example, X is 4 characters down from T and L is 4 characters down from H. The encrypted message is

XLMW MW E KSSH IBEQTPI

3. Using statistics, we can find

ENCRYPTION IS LIKE ENCLOSING A SECRET IN AN ENVELOPE

5.

```
a. 65    66    67    65    68    69    70    71    72
b. 0     1     2     0     3     4     5     6     7
c. 00000 00001 00010 00000 00011 00100 00101 00110 00111
```

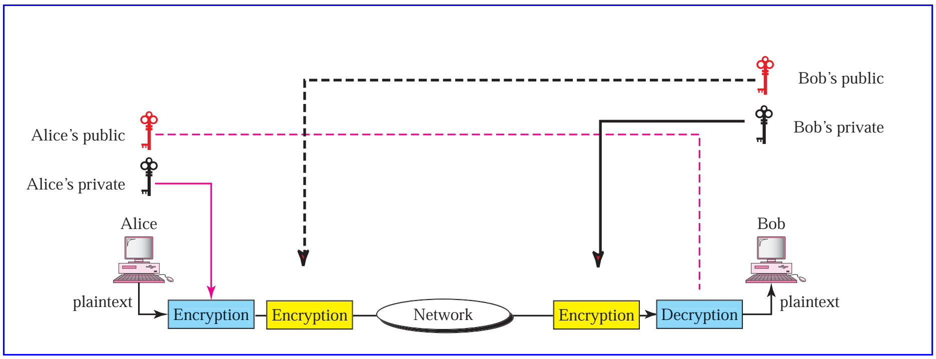
7.
$N = 19 \times 23 = 437$
$(p - 1)(q - 1) = 396$
Select an e such that it is relatively prime to 396. An $e = 5$ satisfies the condition. Now we need a d such that $(5 \times d) \bmod 396 = 1$. Solve the equation $396y = 5d - 1$, with y an integer. We need a y that when multiplied by 396, the ones' digit is 4 or 9 so that it is evenly divisible by 5. If y is 4, then d = 317.

9.

```
( 1 × 227) mod 100  = 27
(27 × 227) mod 100  = 29
(29 × 227) mod 100  = 83
(83 × 227) mod 100  = 41
(41 × 227) mod 100  =  7
( 7 × 227) mod 100  = 89
(89 × 227) mod 100  =  3
( 3 × 227) mod 100  = 81
(81 × 227) mod 100  = 87
(87 × 227) mod 100  = 49
(49 × 227) mod 100  = 23
(23 × 227) mod 100  = 21
(21 × 227) mod 100  = 67
(67 × 227) mod 100  =  9
( 9 × 227) mod 100  = 43
(43 × 227) mod 100  = 61
```

11. See Figure 28.1.

Figure 28.1 *Exercise 11*



13.

$G^{xy} \bmod N = 7^6 \bmod 11 = \mathbf{4}$

$(G^x \bmod N)^y = (7^2 \bmod 11)^3 \bmod 11 = 5^3 \bmod 11 = \mathbf{4}$

15.

$R_1 = 7^3 \bmod 23 = 21$

$R_2 = 7^5 \bmod 23 = 17$

$K = 17^3 \bmod 23 = \mathbf{14}$

$K = 21^5 \bmod 23 = \mathbf{14}$

The symmetric key K is 14

17.

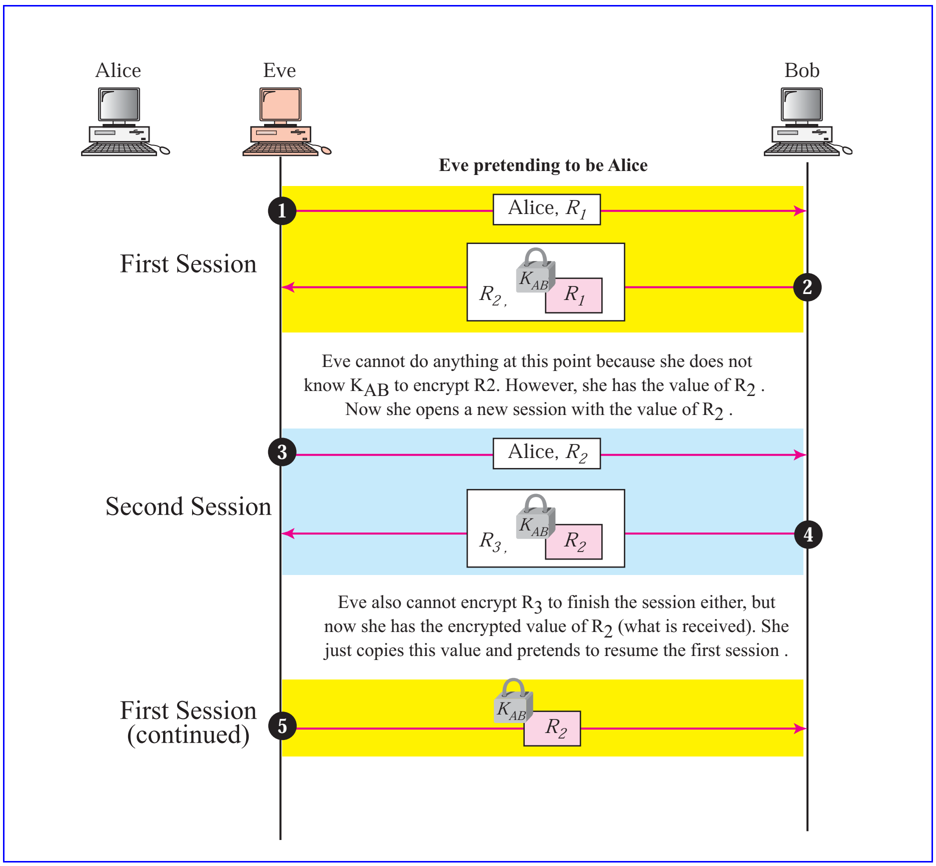
If X = Y, then $R_1 = R_2$. The session key is just one value. Let X = Y = 2, G = 7 and N = 11

$R_1 = R_2 = 7^2 \bmod 11 = 5$

$K = 5^2 \bmod 11 = 3$

19. Eve can impersonate Alice using the reflection attack as shown in Figure 28.2.

Figure 28.2 *Exercise 19*



Eve can start the first exchange and receive the response of Bob. However, she needs to encrypt R_2 and send it to Bob to complete the process, but she does not have the shared key to do so.

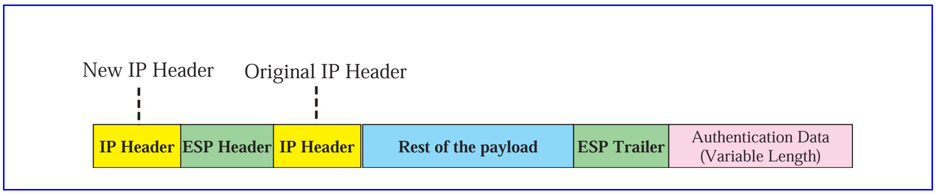
Eve pretends that she is Alice again and opens a new session, this time with the same nonce that she has received from Bob. Bob repeats the second transaction, but he encrypts the new nonce R_2 this time. This is what Eve is looking for.

Eve now sends the encrypted R_2 received in the fourth exchange and pretends that she is Alice continuing the first session. Bob is totally fooled; Alice is authenticated for Bob.

To prevent such an attack, one can either use different shared keys for each direction or use nonces from different sets in each direction.

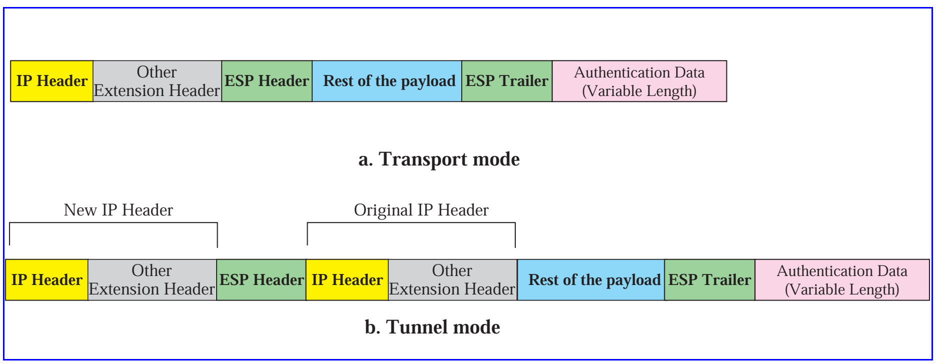
21. See Figure 28.3.

Figure 28.3 *Exercise 21*



23. See Figure 28.4.

Figure 28.4 *Exercise 23*



25. Anytime symmetric keys are involved, there is a need for a trusted third party to distribute the keys. KDC is a trusted party.