CHAPTER 30

Cryptography

Solutions to Review Questions and Exercises

Review Questions

1. Only ***one key*** (the shared secret key) is needed for two-way communication. However, for more security, it is recommended that a different key be used for each direction.
2. A shared secret key can only be used between two entities. Alice needs a shared secret key to communicate with Bob and a different shared secret key to communicate with John.
3. Each person in the first group needs to have **10** keys to communicate with all people in the second group. This means we need at least 10 × 10 = **100** keys. Note that the same keys can be used for communication in the reverse direction. However, note that we are not considering the communication between the people in the same group. For this purpose, we would need more keys.
4. Each person needs 9 keys to communicate with the other people. At first glance, it looks like we need 10 × 9 keys. However, if the same key can be used in both directions (from A to B and from B to A), then we need only (10 × 9) / 2 = **45 keys**.
5. For two-way communication, **4** keys are needed. Alice needs a private key and a public key; Bob needs a private key and a public key.
6. Alice can use the same pair of keys (private and public) to communicate with both Bob and John. However, if there is a need for two-way communication, Bob and John need to have their own pair of keys. In other words, for two-way communication **6** keys are needed, two for each entity.
7. For two-way communication, the people in the first group need 10 pairs of keys, and the people in the second group need a separate 10 pairs of keys. In other words, for two-way communication **40** keys are needed.
8. Each person in the group needs only one pair of keys (private and public). In other words, **20** keys are needed for two-way communication.

Exercises

9. If the two persons have two pairs of asymmetric keys, then they can send messages using these keys to create a ***session symmetric key***, a key which is valid for one session and should not be used again. Another solution is to use a ***trusted center*** that creates and send symmetric keys to both of them using the symmetric key or asymmetric key that has been already established between each person and the trusted center. We will discuss this mechanism in Chapter 31.
10. Each person can create a pair of keys. Each person then keeps the private key and advertises the public key (for example, posting on her web site). Another common solution is to use a ***trusted party*** that accepts the private key of individual and then distributes it using certificates. We will discuss this mechanism in Chapter 31.
11.
    a. We can show the encryption character by character. We encode characters A to Z as 0 to 25. To wrap, we subtract 26.

T	**19 + 20 = 39 – 26 = 13**	→	**N**
H	**07 + 20 = 27 – 26 = 01**	→	**B**
I	**08 + 20 = 28 – 26 = 02**	→	**C**
S	**18 + 20 = 38 – 26 = 12**	→	**M**
I	**08 + 20 = 28 – 26 = 02**	→	**C**
S	**18 + 20 = 38 – 26 = 12**	→	**M**
A	**00 + 20 = 20**	→	**U**
N	**13 + 20 = 33 – 26 = 07**	→	**H**
E	**04 + 20 = 24**	→	**Y**
X	**23 + 20 = 43 – 26 = 17**	→	**R**
E	**04 + 20 = 24**	→	**Y**
R	**17 + 20 = 37 – 26 = 11**	→	**L**
C	**02 + 20 = 22**	→	**W**
I	**08 + 20 = 28 – 26 = 02**	→	**C**
S	**18 + 20 = 38 – 26 = 12**	→	**M**
E	**04 + 20 = 24**	→	**Y**

The encrypted message is ***NBCM CM UH YRYLWCMY***.

b. We can show the decryption character by character. We encode characters A to Z as 0 to 25. To wrap the negative numbers, we add 26.

N	**13 – 20 = –07 + 26 = 19**	→	**T**
B	**01 – 20 = –19 + 26 = 07**	→	**H**
C	**02 – 20 = –18 + 26 = 08**	→	**I**
M	**12 – 20 = –08 + 26 = 18**	→	**S**
C	**02 – 20 = –18 + 26 = 08**	→	**I**
M	**12 – 20 = –08 + 26 = 18**	→	**S**
U	**20 – 20 = 00**	→	**A**
H	**07– 20 = –13 + 26 = 13**	→	**N**
Y	**24 – 20 = 04**	→	**E**
R	**17 – 20 = –03 + 26 = 23**	→	**X**
Y	**24 – 20 = 04**	→	**E**
L	**11 – 20 = –09 + 26 = 17**	→	**R**
W	**22 – 20 = 02**	→	**C**
C	**02 – 20 = –18 + 26 = 08**	→	**I**
M	**12 – 20 = –08 + 26 = 18**	→	**S**
Y	**24 – 20 = 04**	→	**E**

The decrypted message is ***THIS IS AN EXERCISE***.

12. We can, ***but it is not safe at all***. This is a shift cipher with key = 2 and only two symbols. All 0s are changed to 1s and all 1s are changed to 0. The intruder can easily intercept the ciphertext and find the plaintext.

13. We can, ***but it is not safe at all***. The best we can do is to change a 0 sometimes to 0 and sometimes to 1 and to change a 1 sometimes to 0 and sometimes to 1. It can be easily broken using trial and error.

14. We divide the message into five-character blocks and add two bogus characters (Z) at the end. We have:

Plaintext:	**INTER**	**NETZZ**
Ciphertext:	**TRNIE**	**TZENZ**

15. Input: 111001 → output: **001111**

16. Input: 100111 → output: **111100**

17.

a. Input: **1 1 0 0 1 0** → output: **0 1**

b. Input: **1 0 1 1 0 1** → output: **0 0**

18. The possible number of inputs is 2^6 = **32** (000000 to 111111). The possible number of output is 2^2 = **4** (00 to 11).

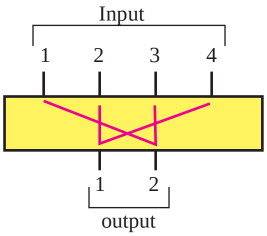
19.

a. Input: 1011 (the leftmost bit is 1), the output is: **110**

b. Input: 0110 (the leftmost bit is 0), the output is: **011**

20. See Figure 30.1. It is a ***compression permutation*** because the number of outputs is less than the number of inputs.

Figure 30.1 *Solution to Exercise 20*



21. We can follow the process until we find the value of *d*. For the last step, we need to use an algorithm defined in abstract algebra. We don't expect students know how to do it unless they have taken a course in abstract algebra or cryptography.

a. $n = p \times q = 19 \times 23 =$ ***437***

b. $\phi = (p - 1) \times (q - 1) = 18 \times 22 =$ ***396***

c. $e =$ ***5*** $d =$ ***317***

We can check that $e \times d = 5 \times 317 = 1 \bmod 396$

22. The main point in the RSA method is that *n* needs to be a very large number so that an intruder cannot factor it. In our example, *n* can be easily broken because, the intruder can find that $n = 187 = 17 \times 11$. In other words, *p* is 17 and *q* is 11. Now, the intruder can calculate the value of $\phi = (17 - 1) \times (11 - 1) = 160$, When the intruder knows this number and the public value of $e = 17$, the value of *d* can be found as ***d = 113***. The secret can be broken.

23. Bob knows *p* and *q*, so he can calculate $\phi = (p - 1) \times (q - 1)$ and find d such that $d \times e = 1 \bmod \phi$. Eve does not know the value of *p* or *q*. She just knows that $n = p \times q$. If *n* is very large (hundreds of digits), it is very hard to factor it to *p* and *q*. Without knowing one of these values, she cannot calculate ϕ. Without ϕ, it is impossible to find *d* given *e*. The whole idea of RSA is that *n* should be so large that it is impossible to factor it.

24.

a. Encryption:

P1 = "F" = 05	→	**C1 = 05^{13} mod 77 = 26**
P2 = "I" = 08	→	**C2 = 08^{13} mod 77 = 50**
P3 = "N" = 13	→	**C3 = 13^{13} mod 77 = 41**
P4 = "E" = 04	→	**C4= 04^{13} mod 77 = 53**

b. Decryption:

C1 = 26 → P1 = 26^{37} mod 77 = 05 = "F"
C2 = 50 → P2 = 50^{37} mod 77 = 08 = "I"
C3 = 41 → P3 = 41^{37} mod 77 = 13 = "N"
C4 = 53 → P4 = 53^{37} mod 77 = 04 = "E"

25. The value of *e* = 1 means no encryption at all because **$C = P^e = P$**. The ciphertext is the same as plaintext. Eve can intercept the ciphertext and use it as plaintext.
26. If the value of *e* is so small, and the value of P is not very large, modular arithmetic looses its effect. For example, if **$C = P^2$** is always smaller than *n*, Eve can easily find the value of P by using $P = (C)^{1/2}$. It it therefore recommended not to choose a very small value for *e*.
27. Although Eve can use what is called the *ciphertext attack* to find Bob's key, she could have done it by intercepting the message. In the ciphertext attack, the intruder can get several different ciphertexts (using the same pair of keys) and find the private key of the receiver. If the value of the public key and *n* are very large, this is a very time-consuming and difficult task.
28.
    R1 = 7^2 mod 23 = **3**
    R2 = 7^5 mod 23 = **17**
    Alice calculates K = $(R2)^2$ mod 23 = 17^2 mod 23 = **13**
    Bob calculates K = $(R1)^2$ mod 23 = 3^5 mod 23 = **13**
29. Nothing happens in particular. Assume both Alice and Bob choose x = y = 9. We have the following situation with *g* = 7 and *p* = 23:
    R1 = 7^9 mod 23 = **15**
    R2 = 7^9 mod 23 = **15**
    Alice calculates K = $(R2)^9$ mod 23 = 15^9 mod 23 = **14**
    Bob calculates K = $(R1)^9$ mod 23 = 15^9 mod 23 = **14**