2.1. Answer the questions

1. What is asymmetric encryption?

Asymmetric encryption uses two different but related keys, and either key can be used to encrypt or decrypt the message

2. What symmetric encryption cryptosystems is one of the most popular public key cryptosystems?

One of the most popular public key cryptosystems is RSA, whose name is derived from Rivest-Shamir-Adleman, the algorithm's developers.

3. What is the foundation of public-key encryption?

Asymmetric algorithms

4. What is the highest value of the asymmetric encryption when one key is used as a private key?

This technique has its highest value when one key is used as a private key, which means that it is kept secret (much like the key in symmetric encryption), known only to the owner of the key pair, and the other key serves as a public key, which means that it is stored in a public location where anyone can use it

5. What is a mathematical trapdoor?

A mathematical **trapdoor** is a "secret mechanism that enables you to easily accomplish the reverse function in a one-way function."

6. What is public-key encryption based?

Public-key encryption is based on a hash value, which, as you learned earlier in this chapter, is calculated from an input number using a hashing algorithm.

7. What can users do and what can't they do with a trapdoor?

With a trapdoor, you can use a key to encrypt or decrypt the ciphertext, but not both, thus requiring two keys.

2.2. Decide whether the following statements are true (T), false (F) or no information (NI). Correct the False (F)

1. The great advantage of private key cryptography is that any two parties anywhere who have the private key software can securely exchange messages without having to make any prior arrangements.
B. False

2. With a trapdoor, encryption and decryption are performed by using the same key.

B. False

3. Asymmetric encryption is also called public-key encryption because tin a key pair, one key is stored in a public location where anyone can use it.

A. True

4. People who were using public key cryptography had to switch to 150-digit or 200-digit primes if they wanted security.

A. True

5. Symmetric encryption method is not as good as asymmetric encryption one, so no methods can replace it.

C. NI