2.1. Answer the questions

1. When was cryptography changed from dark art into a science based on mathematics? Who changed it?

   A: By the end of the 19th century important steps were made in the development of cryptography. Auguste Kerckhoff was one of the most important men changed cryptography from dark art into a science based on mathematics.

2. Who was the father of Information Theory?

   A: Claude Elwood Shannon

3. What device was developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication?

   A: Purple machine

4. Who invented Enigma machine and when was it invented?

   A: Arthur Scherbius

5. Who introduced the idea of public-key cryptography? What are its algorithms based on?

   A: Whitefield Diffie and Martin Hellman. Algorithms are based on the computational complexity problem.

6. What device was developed by the Spartans of Greece? When was it developed?

   A: The scytale. It was developed in 487 B.C.

7. What did Leon Battista Alberti invented?

   A: A device based on two concentric discs that simplified the use of Caesar ciphers Which algorithms are the most widely used in the world among crypto algorithms?

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

1. Giovan Batista Belaso invented a device based on two concentric discs that simplified the use of Caesar ciphers.

   B. False

2. The idea of public-key cryptography belongs to Ronald Rivest, Adi Shamir, and Leonard Adleman.

   B. False

3. Charles Babbage developed the multiple frequency analysis techniques.

   A. True

4. Leon Battista Alberti was an Italian Renaissance humanist author, artist, architect, poet, priest, linguist, philosopher and cryptographer.

   C. NI

5. Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process are Belgian.

   A. True

2.3. Choose the best answer for the following questions

1. Who invented one-time pad encryption for Telex Traffic?

   B. Gilbert S. Vernam

2. What cipher did Julius Caesar use to secure military and government communications?

   B. simple substitution cipher

3. What is one of the most significant contribution provided by public-key cryptography?

   D.The digital signature

4. When was the Enigma cipher broken? Who broke it?

   B. In1939 -1942/The Allies

5. Which of the followings is one of the first block ciphers?

   C.Lucifer cipher

6. Who broke Japan’s Purple’s ciphers?

   A. William Friedman

7. What types of cipher were used in radio communications during World War I?

   D. A&B are correct

8. Why did the United States decide to take part in World War II?

   A.Because the Zimmerman Telegram was broken.