

Milestones in Cryptography

Cryptography · Practice Test · 8 Questions

1. Which ancient Greek device, consisting of a cylinder and a strip of parchment, is considered the earliest known military transposition cipher?

- A) Scytale
- B) Tabula Recta
- C) Atbash
- D) Polybius Square

2. Who is credited with the first published description of a polyalphabetic cipher in his 1467 work 'De Componendis Cyfris', earning the title 'the father of Western cryptology'?

- A) Giovan Battista Bellaso
- B) Leon Battista Alberti
- C) Blaise de Vigenère
- D) Johannes Trithemius

3. The 'Zimmermann Telegram', which influenced the United States' entry into World War I, was intercepted and decrypted by which British intelligence organization?

- A) MI6
- B) Government Code and Cypher School
- C) Room 40
- D) The Black Chamber

4. What was the primary cryptographic weakness exploited by Alan Turing and the Bletchley Park team to break the Enigma machine's daily settings?

- A) Frequency analysis of vowels
- B) The mandatory inclusion of a 'crib' or known plaintext
- C) The mechanical wear on the rotors
- D) The use of the same plugboard setting for an entire month

5. In 1977, the Data Encryption Standard (DES) was published by the NBS. Which company originally developed the algorithm under the name 'Lucifer'?

- A) IBM
- B) Bell Labs
- C) Motorola
- D) Intel

6. Which Renaissance-era cryptographer authored 'Steganographia', a work that disguised secret messages within mundane text using occult themes?

- A) Giambattista della Porta
- B) Johannes Trithemius
- C) Blaise de Vigenère
- D) Leon Battista Alberti

7. Before the advent of modern computers, what was the first fully automated, electromechanical rotor machine used for commercial encryption in the 1920s?

- A) Hebern Rotor Machine
- B) SIGABA
- C) Typex
- D) Purple

8. What is the significance of the 1976 paper 'New Directions in Cryptography' by Diffie and Hellman?

- A) It invented the first quantum key distribution protocol
- B) It introduced the concept of public-key cryptography
- C) It proved that the One-Time Pad was unbreakable
- D) It established the first international standard for AES