BT (Hons) in Information and Communication Technology Degree Programme

INFORMATION SECURITY-ITIC 3123

Assignment 02

Instructions:

This an individual assignment.

Deadline: 02nd April 2024 on or before 2.30PM.

Submission Type: Softcopy (Write a short answers).

Use attached cover page.

QUESTIONS

1. What are the key differences between substitution ciphers and transposition ciphers? Provide examples of each type and explain how they work.
2. Explain the concept of a polyalphabetic cipher.
3. How does the Vigenère cipher improve simple substitution ciphers?
4. Discuss the challenges in cryptanalysis of polyalphabetic ciphers.
5. What role did the Caesar cipher play in ancient cryptography, and how does it relate to modern cryptographic techniques?
6. Explain the concept of a one-time pad and its properties in terms of security and practicality.
7. How did the development of modern cryptographic algorithms, such as AES and RSA, improve upon classic cryptographic techniques?
8. Discuss the key advancements and features of modern cryptography.
9. What ethical considerations should be taken into account when studying classic cryptographic techniques?
10. How do these techniques relate to contemporary issues of privacy, surveillance, and cybersecurity?