

THE OPEN UNIVERSITY OF SRI LANKA
BSc (IT) DEGREE PROGRAMME: LEVEL 04

FINAL EXAMINATION: 2024/2025

COU4306: CRYPTOGRAPHY

DURATION: TWO HOURS (2 HOURS)

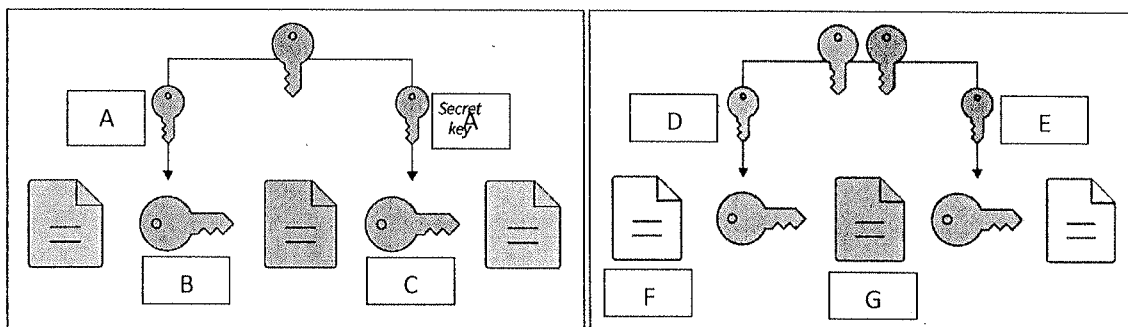


Date: 15.11.2025

Time: 9.30 am – 11.30 am

Answer FOUR Questions ONLY.

Q1. Use the diagram below to answer parts (a) and (b).



a) The above diagram shows two types of encryption methods. Identify items A to G and write the appropriate terms for each. (A, D, and E are keys)

(b) Explain how encryption occurs in each of the two methods, in your own words. Use examples if necessary to illustrate your explanation.

(c) Copy the table below into your answer sheet and fill in the blanks with the correct information.

Feature	DES	AES
Key size		
Block Size		
Secure? If not, vulnerable to which attacks?		
Speed & efficiency		

(d) This question is mainly based on the Vigenère cipher encryption method.

Modified Vigenère Cipher — Encryption Rules

1. Capital letters (A–Z) are numbered as in the standard Vigenère cipher (Note that **numbering start from 0**)
2. Lowercase letters (a–z) continue the numbering immediately after Z
3. After applying the encryption process, +5 is added to all letter values (Both uppercase and lowercase, The **+5 adjustment applies only to letters.**)
4. **No additional key is used**; the +5 adjustment is applied instead of using a key.
5. Digits (0–9) are represented using lowercase letters a–j.
where $a = 0, b = 1, c = 2, \dots, j = 9$.
These letters are written directly in the ciphertext followed by a slash (/) to indicate that they represent digits.
 - Example: $0 \rightarrow a/$
6. Spaces in the message are denoted by the symbol '@'.

Consider the ciphertext Jsylw@d/f/i/b to answer the following questions:

- (i) Identify the letters and numbers in the ciphertext.
- (ii) Decrypt the ciphertext considering the encryption rules that were applied to create it. Show all working steps for the decryption process. (Hint: You cannot apply the encryption steps directly for decryption)

Q2. Part A: Data Breach at SkyLink Online Banking

SkyLink Bank is one of the largest online banking providers in Asia. The bank recently noticed abnormal traffic and reports from customers claiming unauthorized access to their accounts.

After investigation, the cybersecurity team discovered:

- Attackers used a downgrade attack to force the system from TLS 1.3 to SSL 3.0, exploiting old compatibility settings.
- Some servers were still supporting SSLv2, which made them vulnerable to one type of attack.
- Encrypted traffic was captured and later decrypted using brute-force and frequency analysis on weak encryption keys.
- A few compressed HTTPS sessions were exploited to leak session cookies.

The company's security director now needs to design a long-term cryptographic defense plan to prevent such multi-layered attacks.

- (a) Explain what type of attacks were used against SkyLink Bank.
- (b) As a consultant, outline three long-term strategies the bank should adopt to maintain strong cryptographic protection.

Part B

A secret intelligence agency uses a *monoalphabetic substitution cipher* to encrypt messages. The cipher key is unknown, but you intercepted the following ciphertext:

‘ZIT JXOEA WKG V ZIT YFB QGMJ VN ZIT UGRC’

- (a) Explain what a monoalphabetic cipher is and how it differs from a polyalphabetic cipher.
- (b) Perform frequency analysis on the ciphertext to identify possible substitutions for the most common letters. (Show at least 3 likely substitutions.)
- (c) Discuss two major weaknesses of monoalphabetic ciphers and explain how modern cryptography has overcome these vulnerabilities.

Q3. Part A: Hidden Data in the “Operation Blue Pixel” Incident

In 2022, cybersecurity researchers at Interpol's Cyber Crime Centre uncovered an international smuggling ring using image-based steganography to communicate secretly across borders. Criminals embedded encrypted instructions and money transfer details inside JPEG photographs posted on a public art-sharing website. The operation was codenamed “Operation Blue Pixel.”

When investigators analyzed these images, they found:

- Unusual file sizes that didn't match their visual quality.
- Metadata irregularities.
- Binary data hidden in the least significant bits (LSB) of pixel values.

You are a digital forensic analyst tasked with explaining and demonstrating how steganography was used in this case, its detection, and preventive measures.

- (a) Define steganography and explain how it differs from cryptography.

(b) Describe how image-based steganography works and why the criminals in “Operation Blue Pixel” used it to avoid detection.

(c) Explain how the steganographic technique was applied and how investigators detected it.

Part B

(a) List and explain three real-world applications of cryptography in everyday digital life.

(b) Explain how cryptography is applied in digital signatures and electronic voting systems to ensure authenticity and integrity.

Q4.

(a) Define *Post-Quantum Cryptography* and explain why it is essential for future cybersecurity.

(b) What are the main differences between Quantum Cryptography and Post-Quantum Cryptography?

(c) State the role of photons in quantum communication.

(d) Describe one advantage and one limitation of Quantum Cryptography.

(e) Provide brief descriptions on any three quantum-safe certificates.

Q5.

(a) Write concise notes comparing the following:

i) True Random Number Generators vs Pseudo-Random Number Generators

ii) Stream Cipher vs Block Cipher

iii) Cipher-based Message Authentication Code vs Hash-based Message

Authentication Code

(b) Discuss three essential properties of cryptographic hash functions.

(c) Define perfect secrecy in cryptography and illustrate it with a suitable example.

(d) Describe the steps involved in password-based encryption (PBE).

(e) List five different types of biometric authentication methods.

Q6. Part A

- (a) Define Authenticated Key Exchange (AKE) and explain its purpose in secure communications.
- (b) What is a secure protocol? Discuss its key characteristics.
- (c) Briefly explain Transport Layer Security (TLS), highlighting its role in protecting data during network communication.
- (d) Compare Kerberos and X.509 certificates, clearly stating their differences.

Part B

- (a) As a student at university, explain the practical uses of cryptography in your academic, personal, and online activities. Provide relevant examples to support your answer.
- (b) Discuss the role of cryptography in securing online transactions and communications. Include examples such as e-banking, e-learning platforms, or social media.

*** All Rights Reserved ***

