# ZCAS University

## MASTER OF SCIENCE IN COMPUTER SCIENCE & MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

## CIT5342 - SECURITY MANAGEMENT

## MID-TERM EXAMINATION

**20$^{TH}$ OCTOBER 2023**

**16:30 – 19:30 HOURS**

**TIME ALLOWED: READING AND WRITING TIME – THREE HOURS AND FIVE MINUTES**

## INSTRUCTIONS:

1. Section A: **Question One** in Section A is **compulsory**.
2. Sections B: Answer **TWO** Questions from this section.
3. This examination paper carries a total of **100 marks**.
4. Do Not Open the paper Until told to do so by the Invigilator.

**SECTION A – COMPULSORY**

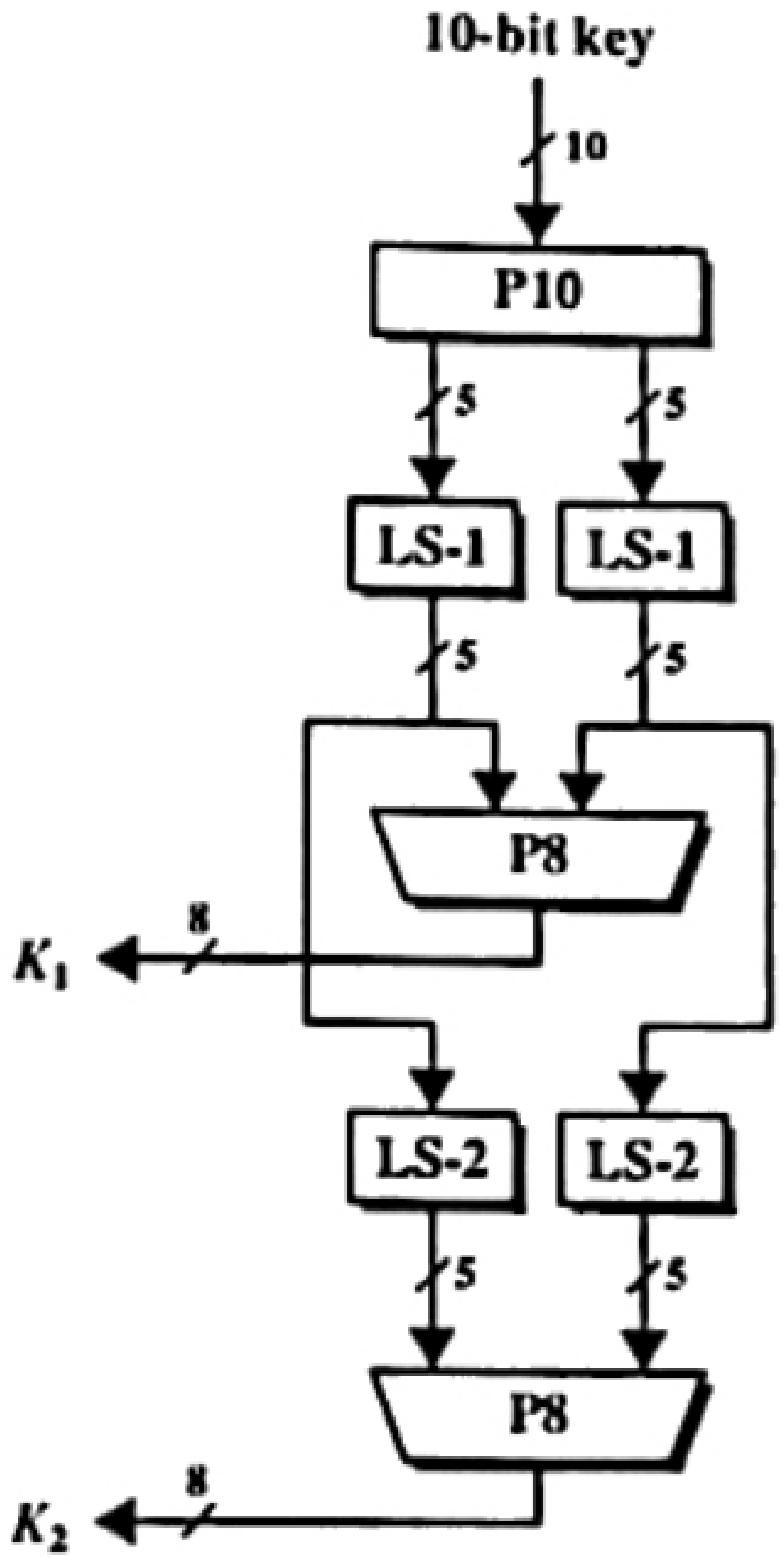
**QUESTION ONE**

(a) DES and SDES are both symmetric-key block ciphers, with DES being a widely used encryption standard in the past and SDES being a simplified variant primarily used for educational purposes. Both algorithms use a similar structure but differ in terms of block size and key size.

Given that S-DES is in use and the permutations, consider the exhibits below and answer the questions that follow:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **P10** | Input : | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | Output: | 3 | 5 | 2 | 7 | 4 | 10 | 1 | 9 | 8 | 6 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **P8** | Input : | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | Output: | 6 | 3 | 7 | 4 | 8 | 5 | 10 | 9 | | |



i. Generate the two round keys for the private key 0011010111. **[10 Marks]**

ii. Explain why DES has 16 rounds of encryption and not less or more. **[5 Marks]**

iii. Describe the 4 basic crypto primitives found in each round of DES **[10 Marks]**.

(b) Modern ciphers use different mechanisms to achieve strong encryption. Two common encryption standards in use today are 3DES and AES which use S-boxes among others to achieve their goal.

i. Given the following S-boxes, find the resultant concatenated stream of bits for an input stream of **10110111** in S-DES implementation.

$$S0 = \begin{bmatrix} 01 & 00 & 11 & 10 \\ 11 & 10 & 01 & 00 \\ 00 & 10 & 01 & 11 \\ 11 & 01 & 11 & 10 \end{bmatrix} \quad S1 = \begin{bmatrix} 00 & 01 & 10 & 11 \\ 10 & 00 & 01 & 11 \\ 11 & 00 & 01 & 00 \\ 10 & 01 & 00 & 11 \end{bmatrix}$$

**[5 Marks]**

a) Describe a trapdoor function found in asymmetric encryption and give two examples. **[5 Marks]**

b) Describe the four stages that a round undergoes in AES encryption and explain why the last round always omits one of the stages regardless of the key length. **[5 Marks]**

c) Give any five characteristic features of AES encryption. **[5 Marks]**

d) Explain why asymmetric encryption is not usually used in payload encryption. **[5 Marks]**

**(Total 50 marks)**

## SECTION B: Answer ANY TWO Questions in this section.

### QUESTION TWO

You are employed as an information security officer at a firm that has not had a security programme and policy in place. You want to find out what hosts are on the network and what services they are running before you start the documentation process.

a) Explain how you would go about the aforesaid and what tools you would use. **[5 Marks]**

b) You have found several outdated network services after your assessment in question one (a). Explain how you would go about to find the CVEs and vulnerabilities associated with these network services. **[5 Marks]**

c) The systems administrator has informed you that they use the following in their network:

- Http for their website
- Ftp for their file services
- Telnet for remote access
- SMTP for email
- Md5 for data integrity

Explain what security advice you would give in such a scenario and why, and also the alternative you would recommend to what is currently being used. **[5 Marks]**

d) You have further been informed that the company uses a proprietary application to communicate with other branch offices in other towns, but the management are not sure whether the information being transferred is secured. Explain how you would go about and what tools you would use to find out whether the information being transferred is secured. **[5 Marks]**

e) You have also found out that the network system in place does not use any access control mechanisms. You have been informed that there is money that has been allocated for an access control system that you will design but it must be multi-factor authentication. Explain what type of multi-factor authentication you would suggest and give plausible reasons. **[5 Marks]**

**(Total 25 Marks)**

## QUESTION THREE

Access control ensures that systems are used as intended. They enforce different facets of security not limited to authorization and authentication. There are many models which are used in access control with each focusing on a specific security access methodology.

a) Describe an access control matrix using a tabular matrix. **[5 Marks]**

b) With the aid of diagrams, differentiate the Bell-LaPadula (BLP) model from the Biba model in reference to access control methods. **[10 Marks]**

c) Describe the three factors of authentication giving an example in each case. **[6 Marks]**

d) Differentiate authorization from authentication as used in computer security giving two examples in each case. **[4 Marks]**

**(Total 25 Marks)**

## QUESTION FOUR

Discuss the following fundamentals of information security:

a) CIA principles ***[6 Marks]***

b) Basic operation of a Digital signature ***[4 Marks]***

c) Confusion and diffusion as used in symmetric encryption. **[5 Marks]**

d) Asymmetric encryption trapdoor function. Give two examples. ***[5 Marks]***

e) Give any 5 examples of attack vectors. **[5 Marks]**

**(Total 25 marks)**

**END OF EXAMINATION**