BINDURA UNIVERSITY OF SCIENCE EDUCATION
FACULTY OF SCIENCE AND ENGINEERING
DEPARTMENT COMPUTER SCIENCE
BSc HONS DEGREE IN INFORMATION TECHNOLOGY

COURSE CODE IT413: CRYPTOGRAPHY AND NETWORK SECURITY

DURATION: 2 HOURS 30 MINUTES TOTAL MARKS: 100

INSTRUCTIONS TO CANDIDATES

Paper consists of 5 questions
Answer all questions.
Each question carries 20 marks.



---

Question 1

a. Explain the following in action of information security and highlight how you would apply to an internet shopping scenario.
   i. Prevention [2]
   ii. Detection [2]
   iii. Reaction [2]

b. Laws, policies, and technical controls are all examples of deterrents measures to unethical and illegal behavior. What are three conditions that can make these measures a success? [6]

c. State and explain the elements of Publicly Available Directory. [8]

Question 2

a. Explain how public key cryptography may be used for identification. [5]

b. Studies have shown that on-line banking services have become primary targets of cyber-attacks. Phishing, password database theft, Man-in-the-Middle attack, Man-in-the-Browser attack, key logging and pharming are among the top threats identified in on-line banking services among others.
   i. Describe how a man-in-the-middle attack may be performed on a Wi-Fi network and the consequences of such an attack. [10]

ii. Explain how a man-in-the-middle attack on a Wi-Fi network can be defeated. [5]

## Question 3

a. Explain why a stream cipher fails to protect message integrity. [6]

b. Describe how a one-way hash function may be used for message authentication. [6]

c. Compare MD5 and SHA algorithm. [8]

## Question 4

a. A Feistel cipher is used in the DES algorithm. Describe the operation of a Feistel cipher. [5]

b. Briefly describe **three** modes of operation of DES. [7]

c. Explain the **four** main stages in AES operation. [8]

## Question 5

a. Outline the steps involved in SSL record protocol. [4]

b. Explain the design goals of firewalls. [6]

c. Explain any **three** services provided by PGP. [6]

d. Why is salt in password protection needed? [4]

**********END OF PAPER**********