BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE AND ENGINEERING

DEPARTMENT OF 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

Answer all questions

Question 1

a. Network attacks can be devastating, putting proprietary information into the hands of competitors, causing important data to be destroyed or compromising employees' and customers' personal information. A network security policy can limit security threats

i. Define threat and attack. **[4]**

ii. What is a network security policy and why is it important? **[2]**

iii. How do you create a network security policy? **[4]**

b. Differentiate passive attack from active attack with example. **[4]**

c. Describe the **three** key principles of security. **[6]**

Question 2

a. Briefly describe the essential ingredients of a symmetric cipher. **[10]**

b. Compare and contrast a block cipher and a stream cipher. **[4]**

c. Using an illustration, briefly explain the Caesar cipher. **[6]**

Question 3

a. Describe the essential steps in public key cryptosystem. **[6]**

b. Compare MD5 and SHA algorithm. **[8]**

c. Examine the properties of a hash function. **[6]**

Question 4

a. Describe does Diffie-Hellman key exchange achieve security? [4]

b. Illustrate how RSA method works. [8]

c. Explain **four** requirements defined for Kerberos. [8]

Question 5

a. What is traffic padding? What is its purpose? [4]

b. Outline any four limitations of SMTP. [4]

c. Distinguish between link and end-to-end encryption? [6]

d. Explain the reasons for using PGP. [6]

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