BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE

BSc HONS DEGREE IN INFORMATION TECHNOLOGY

IT413 - CRYPTOGRAPHY AND NETWORK SECURITY

2 HOURS 30 MINUTES

INSTRUCTION TO CANDIDATES

Paper consists of 5 questions
Answer **all** questions
Each question carries **20 marks.** Total marks are **100.**

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

ii. How do you create a network security policy? **[5]**

b. Specify and explain the parameters that identifies the Security Association. **[5]**

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

Question 2

a. IPsec (IP security) is a suite of protocols developed to ensure the integrity, confidentiality and authentication of data communications over an IP network.

i. Explain the application of IP security. **[3]**

ii. State and explain the benefits of IP security **[3]**

b. Specify and explain the applications of the public key cryptosystem. **[6]**

c. Describe the essential steps in public key cryptosystem. **[8]**

Question 3

a. Analyse the classes of message authentication function. [6]

b. Compare MD5 and SHA algorithm. [8]

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

Question 4

a. Illustrate how a digital signature is created using DSS. [4]

b. Describe the types of attacks addressed by message authentication. [8]

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

Question 5

a. Describe the SSL Architecture in detail. [8]

b. How does IPSec offers the authentication and confidentiality services? [8]

c. Describe the purpose of salt in password protection? [6]

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