1 1 N

UNIVERSITY OF BUEA
FACULTY OF ENGINEERING AND TECHNOLOGY
SECOND SEMESTER EXAMINATIONS

MONTH: July
YEAR: 2014

COURSE INSTRUCTOR: SONE EKONDE
COURSE CODE & NUMBER: CEF 406
COURSE TITLE: Information Systems and Network Security

DATE: 16/07/14
TIME ALLOWED: 3 HOURS

TIME: 11.30 – 14.30
CREDIT VALUE: 4

INSTRUCTION: Answer ANY THREE questions. Each question carries 25 marks

QUESTION 1 (25 marks)

A) Describe the following digital signature algorithm

i) RSA digital signature algorithm

ii) Elliptic curve digital signature algorithm (ECDSA).

Your description should include:

- Key generation
- Signature generation
- Signature verification

4 15
100 1111

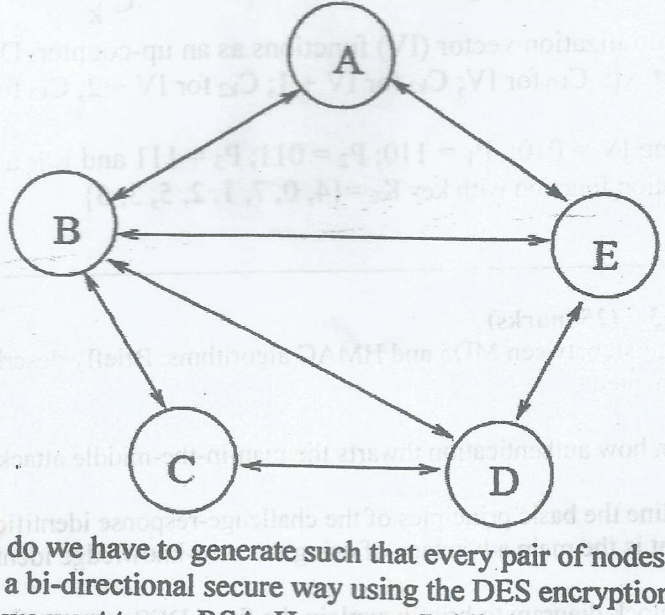
Use artificial parameters (primes) in the table below to illustrate your answer

- For the RSA scheme, consider a hexadecimal message, m = 4F
- For ECDSA scheme, consider the hash function of the message, h(m) = 10 and the elliptic curve equation, $y^2 = x^3 + x + 6$

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	263	269	271	277	281	283
293	307	311	313	317	331	337	347	349	353

(15 marks)

B) Suppose that we have the following network nodes A, B, C, D and E



i) How many keys do we have to generate such that every pair of nodes can communicate in a bi-directional secure way using the DES encryption algorithm?

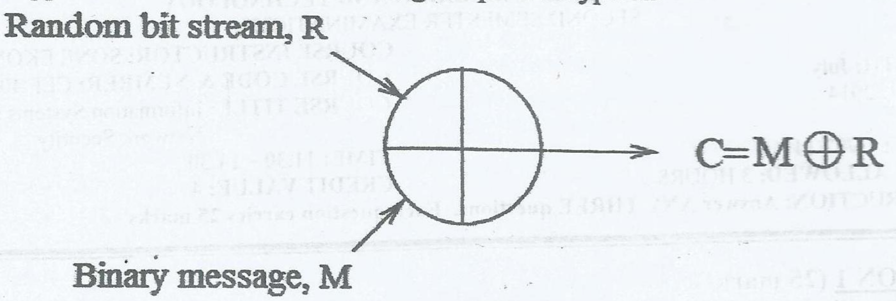
ii) Instead of DES, we want to use RSA. How many Public keys do we need such that every pair of nodes can now communicate in a safe way?

(10 marks)

180 13x180

QUESTION 2 (25 marks)

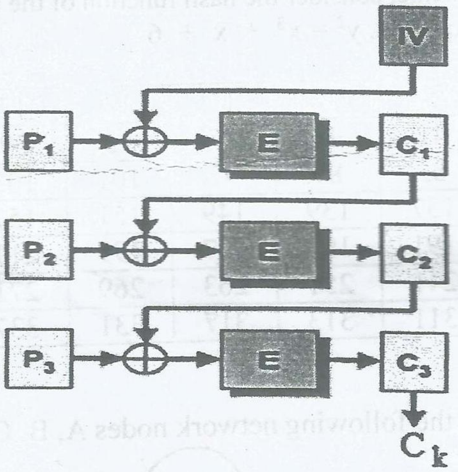
A) **Suppose that we use the following simple encryption**



A language has only two words: A = 111 and B = 0000. Two sentences in the language are encrypted with the same random binary sequence R. The first sentence S1 is encrypted as 011101101001000111001 and the second sentence S2 is encrypted as 011010110110100111110. Find good candidates for the original sentences.

(10 marks)

B) **CCMP (Counter mode with Cipher block chaining Message authentication code Protocol) forms the basis of WPA2 (WiFi Protected Access 2) used in wireless network security. Consider a simplified implementation as follows**



The initialization vector (IV) functions as an up-counter. Derive the following ciphertext: C_{k0} for IV; C_{k1} for IV + 1; C_{k2} for IV + 2; C_{k3} for IV + 3.

Assume IV = 010; P_1 = 110; P_2 = 011; P_3 = 111 and E is a 3-bit block cipher encryption function with key K_E ={4, 0, 7, 1, 2, 5, 3, 6}

(15 marks)

QUESTION 3 (25 marks)

A) **Distinguish between MD5 and HMAC algorithms. Briefly describe how each is implemented**

(10 marks)

B) **Explain how authentication thwarts the man-in-the-middle attack** **(5 marks)**

C) **i) Outline the basic principles of the challenge-response identification protocol**
ii) What is the main advantage of using the zero-knowledge identification protocol?

(5 marks)

D) **Use a block diagram to briefly explain the fixed DES-encrypted password algorithm**

(5 marks)

101

QUESTION 4 (25 marks)

A) PGP (Pretty Good Privacy) is a complete email security package which uses a block cipher called IDEA (International Data Encryption Algorithm). Use a block diagram to explain how PGP works

(8 marks)

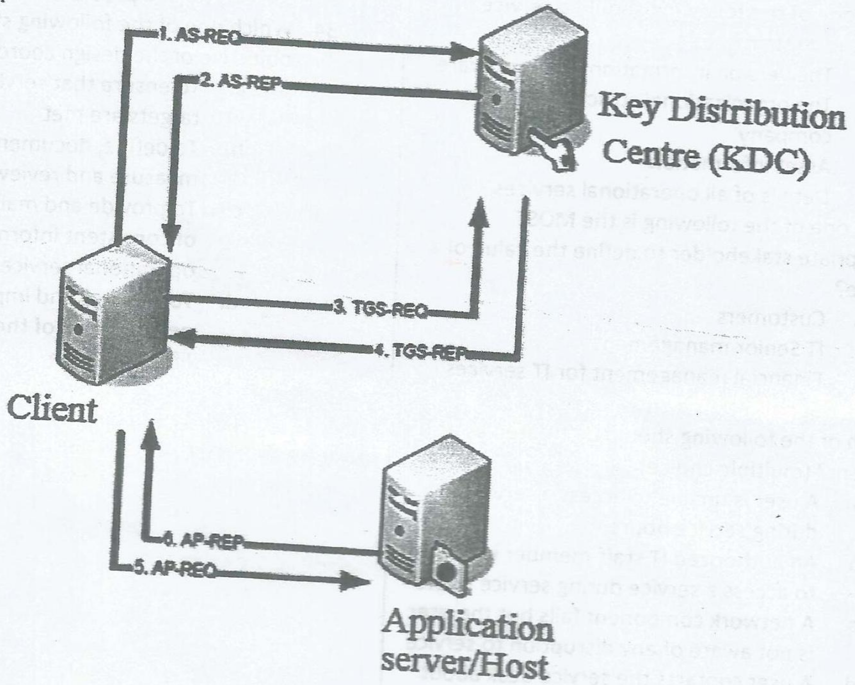
B) Explain the transport layer security (TLS) handshake process

(5 marks)

C) Give the two modes of operation of IPsec. Hence draw the packet structure for the two modes to ensure privacy service.

(5 marks)

D) Kerberos is an authentication service designed to allow clients to access in a secure manner over a network. The standard is X.509 authentication service which is used in many protocols such as Internet Protocol (IP) Security. Use the diagram below to explain how the X.509 authentication service works by clearly outlining the processes labelled 1, 2, 3, 4, 5, and 6.



(7 marks)