KENYA METHODIST UNIVERSITY

END OF TRIMESTER EXAM APRIL 2008

FACULTY	**:**	**SCIENCE AND SOCIAL STUDIES**
DEPARTMENT	**:**	**COMPUTER INFORMATION SCIENCE**
COURSE CODE	**:**	**COMP 445**
COURSE TITLE	**:**	**INFORMATION SYSTEMS SECURITY**

Total Marks (60)

TIME: 2 ½ HOURS

INSTRUCTIONS

Answer all questions in SECTION A and ANY ONE question in SECTION B
The VIGENERE TABLE is attached for any relevant questions.

SECTION A – Answer ALL questions (30 marks)

1. Define the following terms
   a. Nonrepudiation
   b. Computationally secure
   c. Group
   d. Trap-door one-way function
   e. Honeypot

(5 marks)

2. What is the difference between a block cipher and a stream cipher?

(2 marks)

3.
   a. Construct a Playfair matrix with the key *largest.* (1 mark)
   b. Using the Playfair matrix from **a.)** encrypt this message:

      Must see you over Cadogan West. Coming at once. (3 marks)

4. Prove the following
   a. [(a mod n) – (b mod n) mod n] = (a-b) mod n

(3 marks)

5. What is the difference between Rijndael and AES? (2 marks)
6. What is the difference between a session and a master key? (2 marks)

7. Perform encryption and decryption using the RSA algorithm, for the following:

   a. p = 3; q = 11, e = 7; M = 5
   b. p = 17; q = 31, e = 7; M = 2. (6 marks)

8. What is the difference between statistical randomness and predictability. (2 marks)

9. Describe the role that zombies play in distributed denial of service attacks. (4 marks)

SECTION B – Answer ANY ONE question

Question 1 – 30 marks

1. What is a DDos? (2 marks)

2. How does behavior-blocking software work? (2 marks)

3. A taxicab was involved in a fatal hit-and-run accident at night. Two cab companies, the Green and the Blue, operate in the city. You are told that

- 85% of the cabs in the city are Green and 15% are Blue.
- A witness identified the cab as Blue.

The court tested the reliability of the witness under the same circumstances that existed on the night of the accident and concluded that the witness was correct in identifying the color of the cab 80% of the time. What is the probability that the cab involved in the incident was Blue rather than Green? (6 marks)

5. A phonetic password generator picks two segments randomly from each six-letter password. The form of each segment is CVC (consonant, vowel, consonant), where V = <a,e,i,o,u> and C = $\overline{V}$. (8 marks)

   a. What is the total password population?
   b. What is the probability of an adversary guessing a password correctly?

6. What is the difference between an SSL connection and an SSL session?

(2 marks)

7. Consider the following threats to Web security and describe how each is countered by a particular feature of SSL. (10 marks)

a. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.
b. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.

Question 2 – 30 marks

1. List four general categories of schemes for the distribution of public keys.

(4 marks)

2. Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root $\alpha = 7$.
   a. If user A has private key $X_A = 5$, what is A's public key Y_A?
   b. If user B has private key $X_B = 12$, what is B's public key Y_B?
   c. What is the shared secret key? (9 marks)

3. In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M? (4 marks)

4. In the RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

(5marks)

5. What should be the maximum period obtainable from the following generator?
   $X_{n+1} = (aX_n) \bmod 2^4$
   a. What should be the value of a?
   b. What restrictions are required on the seed? (6 marks)

6. What problem was Kerberos designed to address? (2 marks)

Question 3 – 30 marks

1. Using the extended Euclidean algorithm, find the multiplicative inverse of
   a. 1234 mod 4321 (4 marks)
2. Explain the avalanche effect. (4 marks)
3. This problem provides a numerical example of encryption using a one-round version of DES. We start with the same bit pattern for the key K and the plaintext, namely:

in hexadecimal notation:	0 1 2 3 4 5 6 7 8 9 A B C D E F
in binary notation:	0000 0001 0010 0011 0100 0101 0110 0111
	1000 1001 1010 1011 0100 1101 1110 1111

a. Derive K_1, the first-round subkey.
b. Derive L_0, R_0. (8 marks)

Use the following information:

a. A bit rotation of 1

b. Permutation choice 1 for key

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

c. Permutation choice 2 for key

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

d. Initial permutation for plaintext

(a) Initial Permutation (IP)							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

4. Decipher the message MWALO LIAIW WTGBH JNTAK QZJKA ADAWS SKQKU AYARN CSODN IIAES OQKJY B using the Hill cipher with the inverse key $\begin{pmatrix} 2 & 23 \\ 21 & 7 \end{pmatrix}$ Show your calculations and the result. (8 marks)

5. Using the Vigenère cipher, encrypt the word "explanation" using the key *leg*.

(4 marks)

6. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher? (2 marks)