8E4014

Roll No. : ______________________ Total Printed Pages : 4

8E4014

B. Tech. (Sem. VIII) (Main/Back) Examination, April/May - 2011
Computer
8CS1 Information System and Securities

Time : **3** Hours] [Total Marks : **80**
[Min. Passing Marks : **24**

*Attempt any **five questions**, selecting **one question** from **each unit**. All questions carry **equal** marks. (Schematic diagrams must be shown wherever necessary.) Any data you feel missing suitably be assumed and stated clearly, Units of quantities used/calculated must be stated clearly.*

Use of following supporting material is permitted during examination. *(Mentioned in form No. 205)*

1. Nil 2. Nil

UNIT - I

1 (a) In column A, given are the security services whereas column B. Lists the security mechanisms. Prepare a table showing which mechanism(s) provide each service.

Column A	**Column B**
Peer Entity Authentication	Encipherment
Date origin Authentication	Digital signatures
Access Control	Authentication
Confidentiality	Traffic padding
Traffic flow confidentiality	Routing control
Data integrity	Notarization
Non. repidration	Message authentication
Availability	File permissions (as in unix)

More than one mechanism may provide the requested service. **6**

~~(b)~~ List the machanism(s) employed to thwart the following attacks :

(i) Release of message contents.

(ii) Traffic analysis

(iii) Marquerade

(iv) Replay

(v) Modification of messages

(vi) Denial of service.

Also explain each attack in not more than two sentences each.

3+3=6

(c) Explain the various types of cryptanolytic attacks and arrange these attacks in increasing complexity order.

4

OR

1 (a) In Braytair cipher, the key is "MONARCHY". Encipher the word "PLAINTEXT BOOK" using the system.

8

(b) A host connects to an AIM network, sets up a logical connection to another host and is prepared to transfer data to that host. The data is in the form of packets.

The user is to devise a suitable encryption system whether to use link encryption or end-to-end encryption or both. Suggest a suitable encryption scheme and analyze the solution against possible threats.

4+4=8

UNIT - II

2 (a) If x_1, x_2 and x_3 are three consecutive numbers, one of them is divisible by 3. Prove it.

4

(b) Using the Eucledean algorithm, find (i) gcd (3076, 1776) and (ii) express gcd as a linear combination of 3076 and 1776.

4

(c) Prove that no prime of the form 4n+3 can be expressed as sum of two squares.

4

(d) let $a \equiv b \,\mathrm{mod}(m)$ and $c \equiv d \,\mathrm{mod}(m)$ then (i) $a+c \equiv (b+d)\,\mathrm{mod}(m)$ and (ii) $ac \equiv bd \,\mathrm{mod}(m)$. Prove.

4

OR

2 (a) Find the reminder when 16^{53} is divided by 7. Use the properties of congruences.

5

(b) Product of 4 consecutive integers is divisible by 12. Prove it.

5

(c) Find the reminder when 245^{1040} is divided by 18.

3

(d) Show that Diffie – Hellman key exchange algorithm results in the same key.

3

UNIT - III

3 (a) Explain the terms (i) external error control and (ii) internal error control in messages. Draw neat diagrams to illustrate the two. Also compare the two schemes.

2+3+1=6

(b) Level of effort for brute force attack on a MAC algorithm is min (2^k, 2^n) where k is length of key and n is the length of MAC. Justify the statement.

10

OR

3 Given below a scheme for distribution of secret key using KDC.

Message No.	*From – to*	*Message*
1	$A \rightarrow KDC$	$ID_A \Vert ID_B$
2	$KDC \rightarrow A$	$E\left(k_a, \left[k_s \Vert ID_B \Vert T \Vert E\left(K_b, \left[k_s \Vert ID_A \Vert T\right]\right)\right]\right)$
3	$A \rightarrow B$	$E\left(k_b, \left[k_s \Vert ID_A \Vert T\right]\right)$
4	$B \rightarrow A$	$E\left(k_s, N_1\right)$
5	$A \rightarrow B$	$E\left(K_s, f\left(N_1\right)\right)$

Where E(K,M) repressents encryption of M using K as key. Analyze the above algorithm against replay attack. Suggest remedy if found to be vulnerable against replay attack.

16

UNIT - IV

4 (a) In PGP, a user is allowed to home multiple public key/private key pair and can use any pair for communication at any time. Explain the method of communicating to the receiver which pair has been used for encryption. Also draw general format of a PGP message as sent by a sendor.

6+4=10

(b) What is the role of cerificate revocation list in X·509 authentication service ? – Explain.

6

OR

4 (a) Explain the technical deficiencies in kerberose 4. How these were removed in version 5 ? – Discuss.

6

(b) What purpose(s) are served by employing X·509. (i) One way (ii) two-way and (iii) three way authentication procedures. Also draw suitable diagrams for the three procedures with details of messages exchanged.

4+6=10

UNIT - V

5 (a) How IPsec benefits in emproving security of routing applications ? – Discuss.

6

(b) Explain the procedures used in IPsec for protection against

(i) Replay attack

(ii) Message modification.

Draw suitable digrams.

5+5=10

OR

5 (a) In ISAKMP, cookies are exchanged for prevention against clagging attacks, list the basic requirements required to be satisfied by cookie generation method.

6

(b) Write short notes on the following :

(i) Handshake protocol (SSL)

(ii) Trusted systems.

5+5=10