COMP 8 – 2 (RC)

B.E. (Computer) (Semester – VIII) (RC)
Examination, November/December 2017
COMPUTER CRYPTOGRAPHY & NETWORK SECURITY

Duration : 3 Hours

Total Marks : 100

Instructions : 1) Answer **any five** questions selecting at least **one** from **each** Module.
2) Make necessary assumptions if **required**. Clearly state **any** such assumptions made.
3) Draw diagrams **wherever** necessary.

MODULE – I

1. a) What are the two general approaches of attacking a cipher ? Explain. 6
   b) Kelly has intercepted the cipher text "UVACLYFZLJBYL". Show she can use a brute force attack to break the cipher. 6
   c) Using vigenere Cipher encrypt the word "cryptography" using the key "house". 6
   d) What is steganography ? Explain any one technique. 2

2. a) Explain in detail Single round of DES with the help of necessary diagram . 8
   b) Explain any two operations of Block Cipher modes. 8
   c) What is meet in the middle attack ? Explain. 4

MODULE – II

3. a) What is Euler's totient function $\phi(N)$? Compute $\phi(N)$ for $\phi(13)$, $\phi(10)$, $\phi(240)$, $\phi(49)$. 6
   b) Explain the Miller Rabin Algorithm and check if the number 561, 27, 61 pass the Miller Rabin test. 8
   c) Explain RSA algorithm with an example. 6

P.T.O.

COMP 8 – 2 (RC)

B.E. (Computer) (Semester – VIII) (RC) Examination, May/June 2017
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours | Total Marks : 100

Instructions : 1) Answer **any five** questions selecting at least **one** from **each** Module.
2) Make necessary assumptions **if** required. Clearly state **any** such assumptions made.
3) Draw diagrams **wherever** necessary.

MODULE – I

1. a) Define security attack. Also explain different types of security attacks. 6

b) Alice meets bob and says Rjjy rj ts ymi xfggfym. Bi bnqq inxhzxx ymj uqfs. If she is using Caesar cipher, what is she trying to convey ? 6

c) Assuming that the following cipher is generated using monoalphabetic cipher, perform cryptanalysis to decrypt and recover the plain text. 6

GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS, DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU', MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKS FO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.

d) What is steganography ? Explain any one technique. 2

P.T.O.

2. a) Explain in detail DES algorithm with the help of necessary diagram. 10
   b) List and explain the advantages of the Block Cipher Counter (CTR) mode. 5
   c) Write a short note on Triple DES. 5

MODULE – II

3. a) What is Euler's totient function $\phi(N)$? Compute $\phi(N)$ for $\phi(13)$, $\phi(10)$, $\phi(240)$, $\phi(49)$. 8
   b) With the help of a pseudo code explain the Miller Rabin Algorithm. 6
   c) In a public key system using RSA you intercept ciphertext C = 11 to a user whose public key e = 23 and n = 187 what is the plain text M. 6

4. a) Explain Internal and External error Control using Symmetric encryption for message authentication. 5
   b) State and explain the Diffie Hellman Key exchange algorithm, prove the same if Alice and Bob want to exchange a key and they agree on the numbers n = 11 and g = 7, Alice chooses the random number x = 3 and Bob independently chooses the value of y = 6. 8
   c) Explain how public key cryptosystem be used for both authentication and confidentiality. 4
   d) Explain the properties of a Hash Function. 3

MODULE – III

5. a) What are the properties of a Digital Signature ? Explain different approaches for generating Digital Signature Algorithm. 8
   b) Explain Kerberos version 4 authentication dialogue with a neat diagram. 6
   c) What is chain of certificates ? Give examples how X.509 certificate is revoked ? 6

6. a) With reference to kerberos what is a realm ? Explain. 6
   b) Explain general format of PGP message reception from A to B. 8
   c) What are the applications and benefits of IP Sec ? 6

MODULE – IV

7. a) What are different web traffic security approaches ? Also draw and explain SSL Architecture. 8

   b) List and briefly define the principal categories of SET participants. 6

   c) Explain architecture of Distributed Intrusion Detection. 6

8. a) List different advanced Anti-virus techniques. Explain any two. 8

   b) How password are stored in UNIX ? Explain. 6

   c) List different types of Fire wall. Explain any two. 6

COMP 8 – 2 (RC)

B.E. (Computer) (Semester – VIII) (RC) Examination, Nov./Dec. 2016

COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours

Total Marks : 100

Instructions : *1) Answer **any five** questions selecting atleast **one** from **each** Module.*

*2) Make necessary assumptions if required. **Clearly** state **any** such assumptions made.*

*3) Draw diagrams **wherever** necessary.*

MODULE – I

1. a) What are the two general approaches to attacking a cipher ? Explain. 5
   b) Explain the differences between reversible and irreversible mapping. 4
   c) Explain the working of S-boxes in DES Algorithm. 5
   d) Explain any three security services. 6

2. a) List characteristics of Blowfish Algorithm. Also explain sub-key and S-box generation in Blowfish. 6
   b) For a user workstation in a typical business environment, list and explain potential locations for confidentiality attack. 5
   c) Explain two drawbacks of double DES. 5
   d) Briefly explain PRNG and TRNG. 4

MODULE – II

3. a) With the help of pseudocode, explain Miller-Rabin Algorithm. 5
   b) What are the requirements of public key cryptography ? 5
   c) Explain chosen ciphertext attack on RSA Algorithm. 5
   d) Explain working of public-key authority scheme to distribute public keys. 5

P.T.O.

4. a) Define primitive root of a prime number. Also give examples to prove. 6
   i) Given number is a primitive root of a prime number.
   ii) Given number is not a primitive root of a prime number.
   b) What are the requirements for HASH function ? 4
   c) Explain working of MD5 processing of a single 512-bit block. 5
   d) Explain how MAC is used for Message authentication. 5

MODULE – III

5. a) What are the properties of digital signature ? Explain different approaches for generating digital signatures. 6
   b) Explain version – 4 Message exchanges in a full service kerberos environment. 5
   c) Explain X. 509 certificate format. 5
   d) What do you mean by forward certificate and reverse certificate ? 4

6. a) What are the differences between version – 4 and version – 5 of kerberos ? 5
   b) Explain general format of PGP Message (from A to B). 5
   c) Explain different MIME content types. 5
   d) What are the applications and benefits of IP Sec ? 5

MODULE – IV

7. a) What are audit records ? Explain. 5
   b) List and briefly define the principal categories of SET participants. 5
   c) Explain SSL record protocol operation. 5
   d) What is a dual signature and what is its purpose ? 5

8. a) How passwords are stored in UNIX ? Explain. 5
   b) Explain how generic decryption technology is used as an advanced antivirus technique. 5
   c) Explain Packet – Filtering Router. 5
   d) Explain screened – subnet firewall configuration. 5

COMP 8 – 2 (RC)

B.E. (Computer) (Semester – VIII) (RC) Examination, May/June 2016
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours

Max. Marks : 100

Note : *1) Answer **any five** questions selecting at least **one** question from **each** Module.*
*2) Make suitable assumption if **required**. Clearly state any such assumption made.*
*3) Draw diagram **wherever** necessary.*

Module – I

1. a) Consider the block diagram of two round DES is as shown in Figure 1. 12

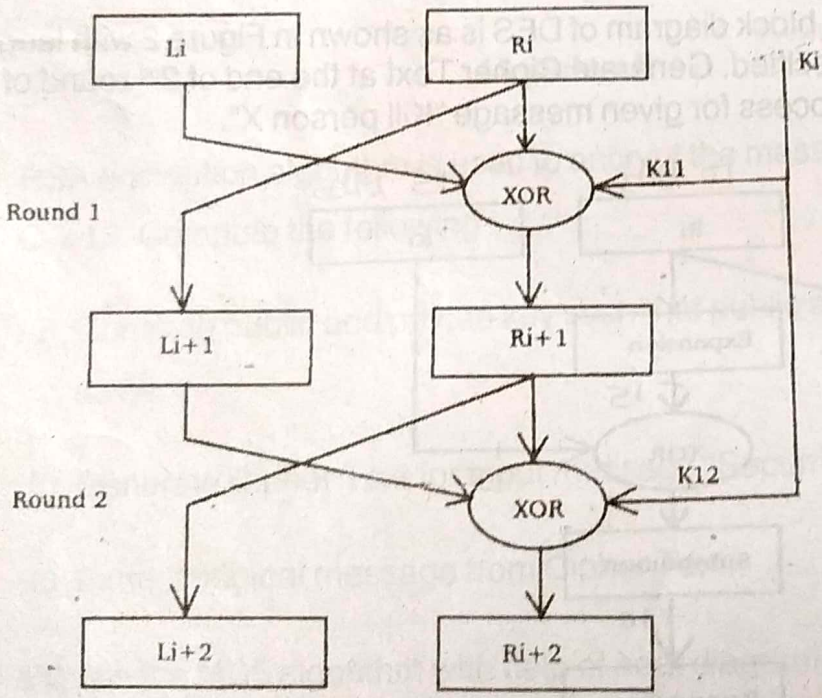

Figure 1

P.T.O.

The Triple DES encryption function is defined as follows :

$C = E2\,(E1(E2(Message, K1), K2), K3)$ ---------- Equation 1

Where E1, E2 and E3 are the encryption function of Two round DES as shown in Figure 1 Generate the cipher text using triple DES encryption function defined in Equation 1. The input message to be encrypted is "Person Should Die" and keys are defined as follows :

K1 = 0111 0001 where K1 is divided into K11 = 0111 and K12 = 0001

K2 = 1100 1011 where K2 is divided into K11 = 1100 and K12 = 1011

K3 = 0111 1010 where K3 is divided into K11 = 0111 and K12 = 1010

b) What is Hill Cipher ? Generate cipher text and extract original message from cipher text using Hill Cipher method. The input message is "Make Mission Successful" and key matrix of hill cipher is given as below : 8

$$K = \begin{bmatrix} 4 & 7 \\ 1 & -1 \end{bmatrix}$$

2. a) What is DES ? The block diagram of DES is as shown in Figure 2 with length of each block is specified. Generate Cipher Text at the end of 2nd round of DES Encryption process for given message "Kill person X". 12

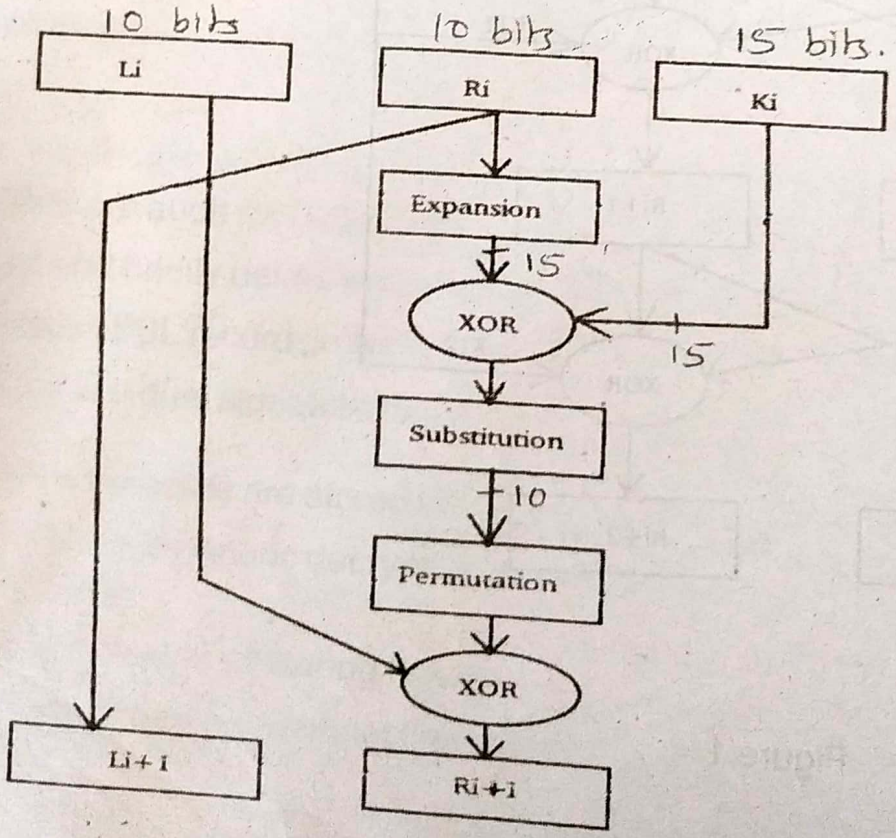

Figure 2

Substitution Logic : The first bit is representing row and second bit is representing column.

$$S_1 = \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix}, S_2 = \begin{bmatrix} 0 & 1 \\ 3 & 2 \end{bmatrix}, S_3 = \begin{bmatrix} 0 & 3 \\ 1 & 2 \end{bmatrix}, S_4 = \begin{bmatrix} 2 & 0 \\ 1 & 3 \end{bmatrix}, S_5 = \begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix}$$

Expansion

$$\begin{bmatrix} m_5 | m_1 & m_2 & m_3 & m_4 | m_2 \\ m_7 | m_9 & m_{10} & 0 & 0 | m_4 \\ 0 | m_5 & m_6 & m_7 & m_8 | m_6 \end{bmatrix}$$

Permutation

$$\begin{bmatrix} m_4 & m_5 & m_1 & m_2 & m_3 \\ m_9 & m_{10} & m_6 & m_7 & m_8 \end{bmatrix}$$

b) What is Playfair Cipher. Generate cipher text using playfair cipher for input message "All should be benefitted" with "Random" as key. 8

Module – II

3. a) RSA encryption algorithm is used to encrypt the message and let P = 11 and Q = 13. Compute the following :

   i) Compute public and private key such that public and private keys are not same.

   ii) Generate Cipher Text for input message "Security is very High".

   iii) Extract original message from Cipher Text. 12

   b) Explain the MD5 algorithm with help of neat diagram. 8

4. a) The block diagram of modified Secure Hash Algorithm (SHA) is as shown in the Figure 3. The length of A, B, C and D block is 6 bit long. Generate hash function at the end of 2rd iteration for the given input message "Security System is Weak" using modified SHA algorithm.

COMP 8 – 2 (RC)

Assume Initial Value of A, B, C, D and E as follows :

A = 110101, B = 100110, C = 101010, D = 111000, E = 110011

K1 = 101010, K2 = 010101.

12

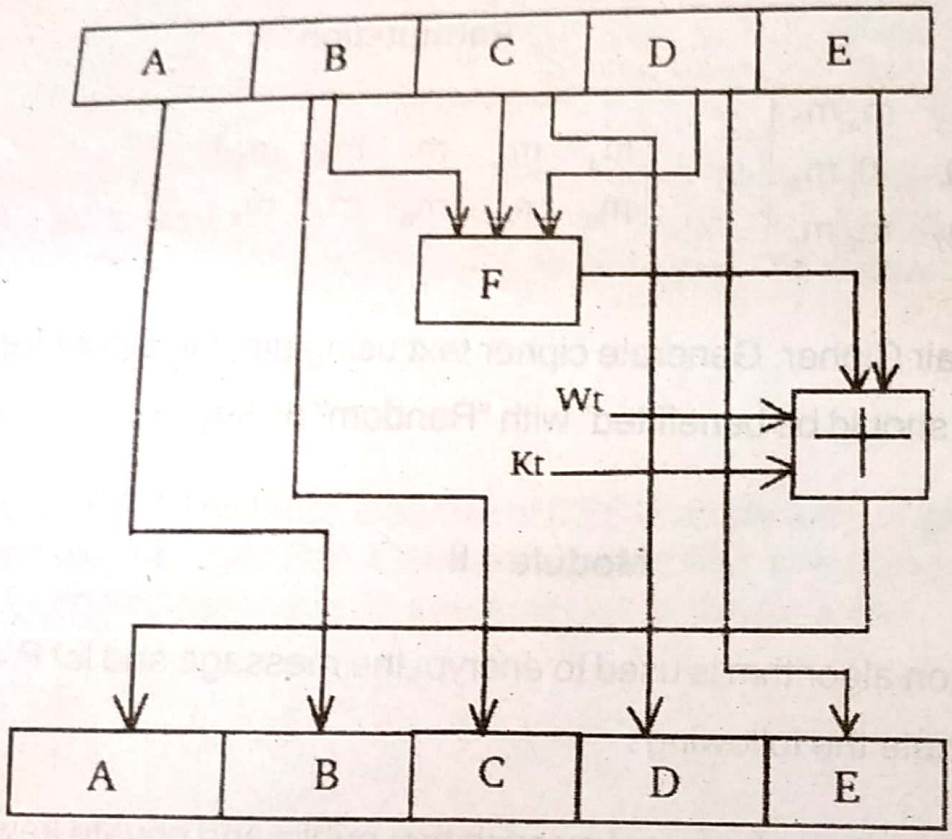

Figure 3

The function f is defined as follows :

$F_1 = (B \wedge C) \vee (B \wedge \text{not } D)$

$F_2 = (B \wedge \text{not } C) \wedge (B \wedge D)$

$F_3 = (\text{not } B \wedge C) \vee (\text{not } B \wedge D)$

$F_4 = (B \wedge \text{not } C) \vee (B \wedge D)$

b) What is the significance of key in cryptography ? What is the main constraint on selecting key of asymmetric cryptography algorithm ?

c) What is significance of Modulo operator in Cryptography ?

Module – III

5. a) What is Digital Signature ? Consider the block diagram as shown in Figure 4, which represents hash function of digital signature. Generate hash function at end of 2nd iteration and digital signature for the input message "Goa State is beautiful". Assume suitable public and private key. 12

Assume Initial Value of A, B, C and D as follows :

A = 101010, B = 110110, C = 101101, D = 111000

S1, S2 and S3 are single left shift operator.

M_i represents message vector.

⊞ represents addition modulo 63.

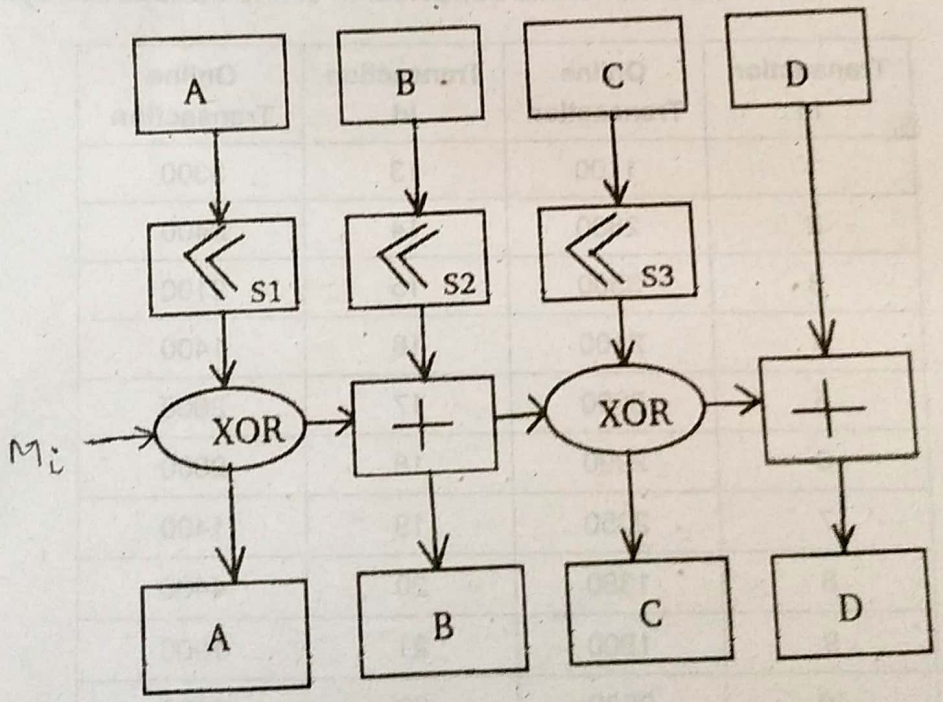

Figure 4

b) Explain different X.509 Authentication procedures. 8

COMP 8 – 2 (RC)

6. a) What are the weakness of exiting mail servers ? Discuss. Proposed a Model to make Mail Server Highly Secured application for communication. 8

b) Draw a neat diagram of IPSec authentication header. Explain Anti-Replay service in authentication header. 6

c) Explain the IP Security Architecture in detail. 6

Module – IV

7. a) Why Https protocol is strong protocol for communication ? Explain in detail. 10

b) What is virus ? How to develop virus software ? Write a code in any language to show simple virus application. 10

8. a) Online transaction executed by different peoples are recorded as shown in the Table 1. 12

i) How to detect abnormal behaviour in online transaction using statistical method ?

ii) How Statistical method and Probabilistic methods can be combined together to detect abnormal behaviour in online transaction ? Propose a model to detect abnormal behaviour in online transaction system.

Transaction Id	Online Transaction	Transaction Id	Online Transaction
1	1100	13	3300
2	2800	14	2400
3	3500	15	2100
4	2100	16	1400
5	3900	17	2600
6	2990	18	2800
7	2050	19	1400
8	1380	20	4400
9	1800	21	1900
10	3500	22	5000
11	2800	23	3100
12	2900	24	2000

Table 1

b) Why malicious software are dangerous ? How to detect and prevent malicious software from getting installed on a system ? 8

COMP 8 – 2 (RC)

B.E. (Computer) (Semester – VIII) (RC) Examination, Nov./Dec. 2015
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours

Total Marks : 100

Instructions : 1) Answer **any five** questions selecting atleast **one** from **each** Module.
2) Make necessary assumptions **if required**. **Clearly** state **any** such assumptions made.
3) **Draw** diagrams wherever **necessary**.

MODULE – I

1. a) What are the characteristics of cryptography ? Also briefly explain any three cryptanalytic attacks. 6
   b) Explain how sub-keys are generated in simplified DES. 5
   c) What is Avalanche effect ? 3
   d) Explain in detail single round of DES algorithm. 6

2. a) For a user workstation in a typical business environment, list and explain potential locations for confidentiality attacks. 5
   b) List and explain advantages of Block Cipher counter (CTR) mode. 5
   c) Explain Blowfish Encryption and decryption process. 6
   d) Briefly explain decentralised key distribution approach. 4

MODULE – II

3. a) Explain timing attack and chosen ciphertext attack on RSA algorithm. 6
   b) With the help of pseudocode explain Miller-Rabin Algorithm. 5
   c) Diffie-Hellman key exchange protocol is vulnerable to which attack ? Justify your answer. 5
   d) Briefly explain Hybrid scheme to distribute secret keys using PKC. 4

4. a) Explain how opponent carry out Birthday attack ? How to prevent this attack ? 5
   b) Explain different applications of MAC. 5
   c) Explain in detail working of MD5 Algorithm. 7
   d) What is strong collision resistance ? 3

P.T.O.

MODULE – III

5. a) What is a chain of certificates ? Give example. How X.509 certificate is revoked ? 5

b) Explain kerberos version – 4 message exchange for service request in another Realm. 6

c) What is difference between direct and arbitrated digital signatures ? 4

d) Explain signing function of DSS Algorithm. 5

6. a) What are the differences between version – 4 and version – 5 of kerberos ? 5

b) What are the five principal services provided by PGP ? Explain any three. 6

c) What are the benefits of IPSec ? 4

d) Explain different MIME transfer encoding techniques. 5

MODULE – IV

7. a) Explain architecture for distributed Intrusion Detection. 5

b) Explain how purchase request is sent by card holder to Merchant in SET ? 6

c) How passwords are stored in UNIX ? Explain. 5

d) List and briefly define classes of intruders. 4

8. a) List different advanced Anti-virus techniques. Explain any two. 7

b) What are the characteristics of Bastion host ? 4

c) What is the difference between an Access control list and a capability ticket. 4

d) Explain Packet Filtering Router. 5

COMP 8 – 2 (RC)

B.E. (Computer) (Semester – VIII) (RC) Examination, May/June 2015
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours

Total Marks : 100

Instructions : 1) *Answer **any five** questions selecting at least **one** from **each** Module.*
2) *Make necessary assumptions **if required**. Clearly state **any** such **assumptions made**.*
3) *Draw diagrams **wherever** necessary.*

MODULE – I

1. a) List and briefly explain categories of active attacks. 4
   b) What is steganography ? List and briefly explain various techniques used in it. What are the drawbacks of steganography ? 6
   c) What is the difference between diffusion and confusion ? 4
   d) Explain in detail single round of DES Algorithm. 6
2. a) What is Meet-in-the middle attack ? Explain. 4
   b) List characteristics of Blowfish algorithm. Also explain in detail sub-key and S-Box generation in Blowfish. 6
   c) What is the difference between session key and master key ? Explain key-distribution scenario between KDC, Initiator and Responder. 6
   d) Briefly explain Blum Blum Shub Generator. 4

MODULE – II

3. a) State Euler's theorem and Fermat's theorem. 4
   b) Determine which of the following integers pass the Miller Rabins Primality test ?
   29, 221. 5
   c) Explain different approaches to attack RSA algorithm mathematically. What are different suggestions made by Algorithm inventors to counter this attack ? 5
   d) Briefly explain different methods for distribution of secret keys using public-key cryptography. 6

P.T.O.

4. a) Explain Internal and External Error Control using symmetric encryption for Message Authentication. 5

b) Explain any four ways in which a hash code can be used to provide message authentication. 6

c) Explain in detail working of MD5 Algorithm. 7

d) What is weak collision resistance ? 2

MODULE – III

5. a) Explain X.509 certificate format ? How this certificates are revoked ? 7

b) Explain different arbitrated digital signature techniques. 5

c) Explain version-4 message exchanges in a full-service Kerberos environment. Also give any three differences between kerberos version-4 and version-5. 8

6. a) Explain any three principal services provided by PGP. 6

b) Explain different X.509 Authentication procedures. 6

c) Explain IPSec ESP format. 5

d) What is the importance of key-ID in PGP ? 3

MODULE – IV

7. a) Explain working of SSL Handshake protocol. 6

b) Explain construction of Dual signature in SET. 5

c) Explain architecture for Distributed Intrusion Detection. 5

d) What is a Honeypot ? Explain. 4

8. a) What is a virus ? What are the phases of virus ? With the help of code explain general structure of virus . 6

b) What is Digital Immune System ? Explain. 5

c) List different types of Firewalls. Explain any two. 6

d) What is Bastion Host ? 3

COMP 8 – 2 (RC)

B.E. (Computer) (Semester – VIII) (RC) Examination, Nov./Dec. 2015
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours

Total Marks : 100

Instructions : 1) *Answer* ***any five*** *questions selecting atleast* ***one*** *from* ***each*** *Module.*
2) *Make necessary assumptions* ***if required***. ***Clearly*** *state* ***any*** *such assumptions made.*
3) ***Draw*** *diagrams wherever* ***necessary***.

MODULE – I

1. a) What are the characteristics of cryptography ? Also briefly explain any three cryptanalytic attacks. **6**

   b) Explain how sub-keys are generated in simplified DES. **5**

   c) What is Avalanche effect ? **3**

   d) Explain in detail single round of DES algorithm. **6**

2. a) For a user workstation in a typical business environment, list and explain potential locations for confidentiality attacks. **5**

   b) List and explain advantages of Block Cipher counter (CTR) mode. **5**

   c) Explain Blowfish Encryption and decryption process. **6**

   d) Briefly explain decentralised key distribution approach. **4**

MODULE – II

3. a) Explain timing attack and chosen ciphertext attack on RSA algorithm. **6**

   b) With the help of pseudocode explain Miller-Rabin Algorithm. **5**

   c) Diffie-Hellman key exchange protocol is vulnerable to which attack ? Justify your answer. **5**

   d) Briefly explain Hybrid scheme to distribute secret keys using PKC. **4**

4. a) Explain how opponent carry out Birthday attack ? How to prevent this attack ? **5**

   b) Explain different applications of MAC. **5**

   c) Explain in detail working of MD5 Algorithm. **7**

   d) What is strong collision resistance ? **3**

P.T.O.

MODULE – III

5. a) What is a chain of certificates ? Give example. How X.509 certificate is revoked ? 5

   b) Explain kerberos version – 4 message exchange for service request in another Realm. 6

   c) What is difference between direct and arbitrated digital signatures ? 4

   d) Explain signing function of DSS Algorithm. 5

6. a) What are the differences between version – 4 and version – 5 of kerberos ? 5

   b) What are the five principal services provided by PGP ? Explain any three. 6

   c) What are the benefits of IPSec ? 4

   d) Explain different MIME transfer encoding techniques. 5

MODULE – IV

7. a) Explain architecture for distributed Intrusion Detection. 5

   b) Explain how purchase request is sent by card holder to Merchant in SET ? 6

   c) How passwords are stored in UNIX ? Explain. 5

   d) List and briefly define classes of intruders. 4

8. a) List different advanced Anti-virus techniques. Explain any two. 7

   b) What are the characteristics of Bastion host ? 4

   c) What is the difference between an Access control list and a capability ticket. 4

   d) Explain Packet Filtering Router. 5

COMP 8 – 2 (RC)

B.E. (Comp.) (Semester – VIII) (RC) Examination, May/June 2014

COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours | Total Marks : 100

Instructions: *1) Figures to the **right** indicate **full** marks.*

*2) Answer **any 5** questions, selecting at least **one** question from **each** Module.*

*3) Make necessary assumptions **if required.***

MODULE – I

1. a) What is security attack ? With the help of examples explain different types of active attacks. **6**

   b) Encrypt the message "paymoremoney" using the Hill cipher with the key given below. Show the calculations and the result. **7**

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

   c) Explain how sub-key generation is done in S-DES. **5**

   d) What do you mean by Stream Cipher ? **2**

2. a) Explain in detail single round of DES algorithm. **6**

   b) Briefly explain the characteristics and drawbacks of Blowfish Algorithm. **5**

   c) Explain working of front-end processor function. **4**

   d) What are the characteristics of random numbers ? Also explain TRNGs. **5**

MODULE – II

3. a) Define Fermats theorem and Eulers theorem. **5**

   b) List all steps of Miller-Rabin algorithm. Also give two examples. **6**

   c) What are the applications of public-key cryptosystem ? Explain. **5**

   d) Briefly explain any two counter measures for RSA-timing attack. **4**

P.T.O.

4. a) Explain in detail MD5 algorithm. 5
   b) Explain different methods to distribute secret keys using public-key cryptography. 5
   c) Explain Man-in-the-Middle attack in Diffie-Hellman key exchange protocol. 3
   d) What is the difference between MAC and a one way hash function ?

MODULE – III

5. a) What are the requirements of digital signature ? 4
   b) Explain digital signature algorithm. 6
   c) Explain working of Kerberos V4 protocol. 6
   d) Explain symmetric encryption approach in context to one-way authentication. 4

6. a) Explain in detail X.509 certificate format. 6
   b) List different services provided by PGP. Explain working of any three. 7
   c) Explain different types of MIME transfer encodings. 4
   d) List any three benefits of IP Sec. 3

MODULE – IV

7. a) Explain SSL record protocol and Alert protocol. 6
   b) Explain significance of dual signature in SET. 5
   c) Explain in detail statistical anomaly detection. 6
   d) What is Honeypot ? 3

8. a) Explain UNIX password scheme. 5
   b) Explain different phases of virus. Also explain structure of a simple virus. 6
   c) Explain digital immune system. 5
   d) What are the characteristics of Bastion host ? 4

COMP 8 – 2 (RC)

B.E. (Comp.) (Semester – VIII) (RC) Examination, Nov./Dec. 2013
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours | Total Marks : 100

Instructions : *1) Answer **any 5** questions, selecting at least **one** question from **each** Module.*
*2) Make necessary assumptions **if required**.*
*3) Draw diagrams **wherever** necessary.*

MODULE – 1

1. a) Explain simplified DES algorithm with neat diagrams. 8

   b) Briefly explain the different types of cryptanalytic attacks based on what is known to the attacker. 8

   c) What is traffic padding ? Why is it used ? 4

2. a) Explain the design parameters of the Fristel Cipher. 6

   b) Differentiate between monoalphabetic and polyalphabetic ciphers. Illustrate with examples. 8

   c) Explain the basic principle of the rotor machine. 6

MODULE – 2

3. a) Perform encryption and decryption using the RSA algorithm.

   P = 5, q = 11, e = 9, M = PLAN. 8

   b) Explain the man in the middle attack in Deffie Hellman key exchange. 7

   c) What type of attacks are addressed by message authentication. 5

4. a) Briefly discuss the various attacks on RSA. 7

   b) Explain SHA – 512 processing of a single 1024 Bit Block. 6

   c) Users A and B use the Deffie Hellman key exchange technique with a common prime q = 71 and a primitive root $\alpha = 7$.

   i) If user A has private key $X_A = 10$. What is A's public key Y_A ?

   ii) If user B has private key $X_B = 14$. What is B's public key Y_B ?

   iii) What is the shared key ? 7

P.T.O.

MODULE – 3

5. a) With the help of a neat diagram explain the general format of PGP message. 7

   b) List and explain the arbitrated digital signature techniques. 6

   c) Explain the environmental and technical shortcomings of Kerberos Ver 4. 7

6. a) What is forward and reverse certificate ? Explain. 5

   b) Explain the process of PGP message generation. 7

   c) What is S/M/ME ? What are its functions ? 4

   d) Explain the IPsec authentication header. 4

MODULE – 4

7. a) What is a firewall ? Explain the different types of firewalls. 6

   b) What is the difference between rule-based anamoly detection and rule based penetration identification ? 6

   c) List and explain the principal categories of SET participants. 6

   d) What is a polymorphic virus ? 2

8. a) State the SSL handshake protocol message types along with their parameters. 6

   b) Write short notes on : (6×2=12)

      i) Distributed intrusion detection.

      ii) Stateful inspection firewalls.

   c) What are honeypots ? 2

B.E. (Comp.) (Semester – VIII) (RC) Examination, June 2013
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours Total Marks : 100

Instructions : 1) *Answer **any 5** questions, selecting at least **one** question from **each** Module.*
2) *Make **necessary** assumptions **if** required.*
3) ***Draw** diagrams **wherever** necessary.*

Module – 1

1. a) List and explain the different categories of security mechanisms. 7

   b) Encrypt the message "ATTACK IS TODAY" using Hill Cipher with key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext. 8

   c) With the help of a neat diagram explain cipher feedback mode. 5

2. a) Explain the S-DES key generation algorithm, given key 0111111101 generate subkeys. 8

   b) What are pseudo random numbers ? Briefly explain any two methods for generating the same. 8

   c) What is steganography ? Explain any two techniques used in it. 4

Module – 2

3. a) Determine which of the following integers pass the Miller Rabins primarility test ? 195, 397, 97. 7

   b) Briefly explain the requirements of public key cryptography. 6

   c) List and briefly explain the four schemes for the distribution of public keys. 7

4. a) Differentiate between MAC and a one way hash function. 4

   b) With the help of a neat diagram explain the MD 5 algorithm. 8

   c) In a public key system using RSA, you intercept ciphertext C = 10 sent to a user whose public key e = 5, n = 35. What is the plaintext M ? 6

   d) Calculate $\phi(231)$. 2

P.T.O.

Module – 3

5. a) What is the difference between direct and arbitrated digital signature ? 4
   b) Differentiate between Kerberos Ver 4 and Ver 5. 6
   c) How can a X 509 certificate be revoked ? 4
   d) What are the five principal services provided by PGP ? 6

6. a) Explain in brief the five new header fields defined in MIME. 6
   b) With reference to Kerberos, what is a realm ? Explain. 6
   c) List the benefits of IPsec. 5
   d) What is R 64 conversion ? 3

Module – 4

7. a) With the help of a neat diagram explain purchase request sent by card holder to merchant in SET. 7
   b) What is a virus ? Enumerate on the different types of viruses. 7
   c) What is the difference between an access control list and a capability ticket ? 6

8. a) Draw and explain the digital immune system. 7
   b) What is a dual signature ? What is its purpose ? 5
   c) What is a circuit level gateway ? Explain with the help of an example. 6
   d) List and define the three classes of intenders. 2

B.E. (Computer) (Semester – VIII) (RC) Examination, May/June 2012
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours | Total Marks : 100

Instructions : 1) Answer **any five** questions selecting atleast **one** from **each** Module.
2) Make **necessary** assumptions if required. Clearly state **any such** assumptions made.
3) Draw diagrams **wherever** necessary.

MODULE – I

1. a) Define Security Attack. Also explain different types of Security attacks. 6

   b) What is Steganography ? Explain various techniques used in it. Also state its disadvantages. 6

   c) Draw and explain Feistel Cipher Structure. 6

   d) Construct a Playfair Matrix with the key LARGEST. 2

2. a) What is Double DES. State and explain drawbacks of it. How these drawbacks can be overcame ? 8

   b) Draw and explain key distribution Scenario between KDC, Initiator and responder. 5

   c) What is the use of Random Number ? List different methods of PRNG generation. Explain any one method. 7

MODULE – II

3. a) Explain Euclid's Algorithm with the help of an example. Also state Fermat's theorem. 6

   b) Draw and explain how secrecy can be achieved using Public-Key Cryptosystem. State and explain in brief use of the public key cryptosystem. 6

   c) Describe RSA algorithm with an example. Show working of each step in detail. 8

P.T.O.

4. a) Explain different categories of schemes for the distribution of public keys. 8

   b) In context to authentication function explain Internal and External Error Control for Symmetric Encryption. 5

   c) Explain in detail working of MD5 message digest algorithm. 7

MODULE – III

5. a) What requirements should a digital signature satisfy ? Explain different Arbitrated digital signature techniques. 7

   b) Draw and explain X.509 format of digital certificate. How and when this certificate is revoked ? 7

   c) Explain Kerberos Version 4 authentication dialogue with neat diagram. 6

6. a) List and explain different principal services provided by PGP. 7

   b) List and explain different MIME Transfer encodings for message bodies. What are different functions of S/MIME ? Explain. 7

   c) Draw and explain IPSec ESP format. 6

MODULE – IV

7. a) Define SSL session and SSL connection. List and briefly define the parameters that define SSL session state and connection state. 7

   b) List and briefly define the principal categories of SET participants. Also discuss the importance of Dual signature in SET. 7

   c) Write a short note on Statistical Anomaly detection. 6

8 a) Explain virus structure with the help of an example. Also explain different types of viruses.

   b) Explain how Generic Decryption Technology is used as an advanced antivirus technique.

   c) Describe Packet-filter firewall. Also discuss weaknesses and appropriate countermeasures of it.

B - 07

[Total No. of Questions : 8] (Pages : 02)

COMP 8-2 (RC)

B.E. (Computer) (Semester - VIII) (RC) Examination, Nov. - 2011
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours **Total Marks : 100**

Instructions : 1) Answer any five questions selecting at least one from each module.
2) Make necessary assumptions if required. Clearly state any such assumptions made.
3) Draw diagrams wherever necessary.

MODULE - I

Q1) a) Draw and explain a model for Network security. [6]

b) What is a transposition cipher? Discuss any two techniques. [6]

c) Explain in detail DES algorithm with the help of necessary diagrams. [8]

Q2) a) List and explain advantages of CTR (counter) mode. [5]

b) Write a short note on Triple - DES. [5]

c) With the help of pseudocode explain Blum - Blum shub generator. [5]

d) What is steganography? Explain various techniques used in it. [5]

MODULE - II

Q3) a) State Fermat's Theorem and Euler's Theorem. [5]

b) Explain how public key cryptosystem used for both authentication and confidentiality. [5]

c) Explain Diffie - Hellman key exchange algorithm with the help of an - example. Also explain Man-in-the Middle attack. [7]

d) What is the difference between MAC and one - way hash function. [3]

Q4) a) Explain Secure Hash Algorithm with the help of neat diagrams. [7]

b) Explain RSA algorithm with an example. Also discuss any two attacks on RSA algorithm. [8]

c) Draw and explain how public key distribution is achieved with public key authority? What is the disadvantage of this method? [5]

P.T.O.

MODULE - III

Q5) a) What is digital signature? Draw and explain digital signature algorithm. [7]

b) Differentiate between kerberos Version - 4 and Version - 5. [6]

c) Explain different services provided by PGP with the help of neat diagrams. [7]

Q6) a) Write a short note on S/MIME functionality. [5]

b) What are the benefits of IPSec? [4]

c) Draw and explain IPSec ESP format. [5]

d) Explain Oa kley key Determination protocol. [6]

MODULE - IV

Q7) a) What are different web traffic security approaches? Also draw and explain SSL architecture. [7]

b) Draw and explain how merchant verifies customer purchase request in SET. [6]

c) List and explain different approaches for Instrusion detection. [7]

Q8) a) Explain working of Digital Immune System. [5]

b) Write short notes on [4 × 2 = 8]

i) Worm

ii) Trapdoor

c) With the help of neat diagrams explain different Firewall configurations. [7]

❄❄❄

G - 1172 (Pages : 02)

Total No. of Questions : 8]

COMP 8-2 (RC)

B.E. (Computer) (Semester - VIII) Examination, May/June 2011

COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours Total Marks : 100

Instructions : 1) Answer any five questions selecting at least one question from each module.

2) Make necessary assumptions if required. Clearly state any such assumptions made.

3) Draw diagrams wherever necessary.

MODULE - I

Q1) a) List and explain categories of security services. [6]

b) Explain playfair cipher with the help of an example. [6]

c) What is one-time pad scheme? What are its difficulties? [5]

d) What is the difference between stream cipher and block cipher? [3]

Q2) a) Explain triple DES with two keys. Also explain known-plaintext attack on triple DES. [6]

b) Differentiate between link versus End-to-End Encryption. [4]

c) What are the uses of random numbers? Explain any two methods to generate PRNG. [7]

d) What is the difference between session key and master key? [3]

MODULE - II

Q3) a) What is Euler's Totient Function $\phi(N)$? Compute $\phi(N)$ for $\phi(37)$, $\phi(35)$, $\phi(42)$, $\phi(20)$. [6]

b) Explain timing attack and chosen ciphertext attack on RSA Algorithm. [6]

c) State and explain different methods to distribute public keys. [8]

Q4) a) Explain how message authentication and confidentiality can be achieved using MAC? In what situations MAC can be used? [6]

b) Explain Diffie-Hellman key exchange algorithm with an example. [6]

c) Explain secure Hash Algorithm with the help of neat diagrams. [8]

P.T.O.

wherever necessary.

G - 1172

MODULE - III

Q5) a) What is the difference between direct and arbitrated digital signature. [4]

b) Draw and explain signing function for digital signature algorithm. [5]

c) Explain overview of kerberos with necessary diagram. [7]

d) What is forward and Reverse Certificate? [4]

Q6) a) Draw and explain general format of PGP message. [5]

b) Explain in brief five new header fields defined in MIME. [5]

c) Draw and explain IPSec Authentication Header. [5]

d) Draw and explain IPSec ESP Format. [5]

MODULE - IV

Q7) a) What steps are involved in the SSL Record Protocol transmission? [6]

b) With the help of neat diagram explain purchase request sent by cardholder to Merchant in SET. [6]

c) What are classes of Intruder? [3]

d) Draw and explain Unix password scheme. [5]

Q8) a) What are different phases of virus? Also explain virus structure. [6]

b) Draw and explain Digital Immune System. [6]

c) Draw and explain different types of Firewall. [8]

❖❖❖❖

COMP 8 (E IV) 2 (NC)

B.E. (Comp.) (Semester – VIII) Examination, May/June 2010
CRYPTOGRAPHY AND NETWORK SECURITY (E – IV)

Duration: 3 Hours

Total Marks : 100

Instructions : 1) *Answer* ***any five*** *questions by selecting at least* ***one*** *question from* ***each*** *Module.*
2) *Make suitable assumption* ***if required.***

MODULE – I

1. a) Describe a model for network security which is required for two principals to securely exchange messages. **6**

b) Explain working of Hill cipher with the help of an example. **7**

c) Describe the simplified DES Algorithm. **7**

2. a) Explain single round of IDEA. **7**

b) Differentiate between Link Versus End-to-End encryption. **5**

c) What are the characteristics of Random numbers ? Explain any two methods for PRNG. **8**

MODULE – II

3. a) Explain how secracy and authentication is achieved with the help of public-key cryptosystem. **6**

b) Explain distribution of public keys using public key certificate. **6**

c) Define Fermat's theorem. **2**

d) What is Euler's Totient Function $\phi(N)$? Using properties of $\phi(N)$ compute $\phi(13)$, $\phi(16)$, $\phi(35)$. **6**

4. a) Draw and explain different variety of ways in which a hash code can be used to provide message Authentication. **8**

b) What is digital signature ? What are the requirement for a digital signature. **6**

c) Draw and explain how verification is done at receiver in digital signature algorithm. **6**

P.T.O.

MODULE – III

5. a) Explain the exchanges that are required in Kerberos inter-realm environment. 6

   b) Explain the authentication procedures for X.509 directory authentication service. 4

   c) What is functionality provided by S/MIME ? 3

   d) Explain the different services provided by PGP. 7

6. a) Explain the PGP message format and key rings. 6

   b) What is Oakley key determination protocol ? Describe its features. 6

   c) Draw a neat diagram of IPSec authentication header. Explain Anti-Replay service in authentication header. 8

MODULE – IV

7. a) Give a brief overview of SET. 6

   b) Explain SSL architecture. Write a note on handshake protocol used in it. 8

   c) Discuss important techniques used for Intrusion detection. 6

8. a) What are different types of firewalls ? Explain. 8

   b) Explain Data Access Control. 5

   c) What is Digital Immune system ? Explain with the help of necessary diagram. 5

   d) Differentiate between virus and worm. 2

---

4. a) Define primitive root of a prime number. Also give examples to prove.
   i) Given number is a primitive root of a prime number.
   ii) Given number is not a primitive root of a prime number. 6
   b) What are the requirements for HASH function ? 4
   c) Explain working of MD5 processing of a single 512-bit block. 5
   d) Explain how MAC is used for Message authentication. 5

MODULE – III

5. a) What are the properties of digital signature ? Explain different approaches for generating digital signatures. 6
   b) Explain version – 4 Message exchanges in a full service kerberos environment. 5
   c) Explain X. 509 certificate format. 5
   d) What do you mean by forward certificate and reverse certificate ? 4

6. a) What are the differences between version – 4 and version – 5 of kerberos ? 5
   b) Explain general format of PGP Message (from A to B). 5
   c) Explain different MIME content types. 5
   d) What are the applications and benefits of IP Sec ? 5

MODULE – IV

7. a) What are audit records ? Explain. 5
   b) List and briefly define the principal categories of SET participants. 5
   c) Explain SSL record protocol operation. 5
   d) What is a dual signature and what is its purpose ? 5

8. a) How passwords are stored in UNIX ? Explain. 5
   b) Explain how generic decryption technology is used as an advanced antivirus technique. 5
   c) Explain Packet – Filtering Router. 5
   d) Explain screened – subnet firewall configuration. 5