Paper / Subject Code: BE920 / Computer Cryptography & Network Security

BE920

Total No. of Printed Pages:02

B.E. (Information Technology) Semester - VIII (Revised Course 2007-08)
EXAMINATION NOV/DEC 2019 16-17
Computer Cryptography & Network Security

[Duration Three Hours] **[Max. Marks: 100]**

Instructions: 1) Answer **any five** questions with atleast **one** from **each** Module.
2) **All** questions carry **equal** marks.

MODULE – I

Q.1 a) Differentiate between Passive attacks and Active attacks? **6**
b) Using Hill Cipher encrypt the plaintext "SUMMER". Also explain the decryption process. Use the Key $\begin{vmatrix} 3 & 3 \\ 2 & 5 \end{vmatrix}$ **8**
c) List and Explain the different types of viruses? **6**

Q.2 a) With an example explain the structure of a virus? **6**
b) Explain The following : **8**
i. Playfair Cipher
ii. Columnar Transposition
c) Explain any two Security services defined by X.800 OSI Security Architecture? **6**

MODULE – II

Q.3 a) Explain Triple DES with 3 keys? State it's advantages over DES. **8**
b) Using Euclidean algorithm find the GCD of (1785,546) ? **6**
c) Compare Link Encryption with End-to-End Encryption? **6**

Q.4 a) State and explain Extended Euclid algorithm with an example? **6**
b) With a neat diagram explain Decentralized Key Distribution Scheme? **6**
c) Explain the following Block Cipher modes of operation: **8**
i. Electronic Codebook
ii. Output Feedback

MODULE – III

Q.5 a) Perform encryption and decryption using RSA algorithm for the following p=7, q=11, e=17 and M=88? **8**
b) Explain MD5 Algorithm with a neat diagram? **6**
c) Write a short note on Distribution of Public keys? **6**

Q.6 a) Explain how MAC can provide message authentication? **8**

B

b) Write a Short note on Distribution of secret keys? 6
c) Explain Diffie-Hellman Key Exchange Algorithm? 6

MODULE – IV

Q.7
a) Explain PGP functionality? 8
b) What is SET? Explain SET with a neat diagram. 6
c) State and explain the requirements of Kerberos? 6

Q.8
a) Draw and explain X.509 Authentication Procedures? 8
b) Explain S/MIME functionality? 6
c) Write a Short note on Kerberos Realms? 6

Paper / Subject Code: BE920 / Computer Cryptography & Network Security

BE920

tal No. of Printed Pages:2

B.E.(Information Technology) Semester - VIII (Revised Course 2007-08)
EXAMINATION MAY/JUNE 2019
Computer Cryptography & Network Security

uration : Three Hours] **[Max.Marks :100]**

structions:
1. Answer **any five** questions with atleast **one** from **each** Module.
2. **All** questions carry **equal** marks.

MODULE I

.1	a)	With an Example explain substitution using Caesar Cipher. Perform Brute-Force Cryptanalysis on the calculated ciphertext?	06
	b)	Explain the two approaches to Intrusion Detection?	08
	c)	Explain the working of a One-Time Pad? Also state its advantages and disadvantages.	06
.2	a)	Write a short note on Steganography?	06
	b)	Explain the Rail Fence Transposition technique with a suitable example?	06
	c)	Explain the following: i. Audit Records ii. Distributed Intrusion Detection iii. Honeypots iv. Rule-Based Intrusion Detection	08

MODULE-II

.3	a)	Explain Double DES? Also Explain meet in the middle attack.	08
	b)	Using Euclidean algorithm find the GCD of (888,54)?	06
	c)	Draw and explain the working of S-Boxes in DES.	06
.4	a)	Explain how the Multiplicative inverse of a number is calculated using Extended Euclid algorithm?	06
	b)	Draw and explain a single round in the Data Encryption Standard algorithm?	06
	c)	Explain the following Block Cipher modes of operation: i. Cipher Feedback ii. Electronic Codebook	08

A0F8AADAF690B62888FAA9AD44E27634

MODULE –III

Q.5	a)	Write a short note on Authentication Functions?	06
	b)	Explain MD5 Algorithm with a neat diagram?	06
	c)	Explain Man-in-the-middle attack(MITM) on Diffie-Hellman's algorithm with a suitable example?	08
Q.6	a)	Differentiate between MD5 and SHA-1 algorithm?	06
	b)	Explain any four ways in which a hash code can be used to provide authentication?	08
	c)	Write a short note on RSA security?	06

MODULE-IV

Q.7	a)	Explain the different types of Firewall Configurations?	08
	b)	Write a Short note on IP Security?	06
	c)	Differentiate between Kerberos Version 4 and Kerberos Version 5?	06
Q.8	a)	Differentiate between a Packet-Filtering Router and an Application-Level Gateway?	08
	b)	Explain Forward and Reverse Certificates in X.509 Authentication service?	06
	c)	Explain any three PGP functions?	06

A0F8AADAF690B62888FAA9AD44E27634

IT 8-2 (RC) 2007 – 08

B.E. (IT) (Semester – VIII) (RC 2007-08) Examination, Nov./Dec. 2018
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours | Total Marks : 100

Instructions : *1) Answer **any five** questions with at least **one** from **each** Module.*

*2) **All** questions carry **equal** marks.*

MODULE – I

1. a) Elaborate on the X.800 security services. 8

   b) Explain the symmetric cipher model with a suitable diagram. 6

   c) With examples, explain substitution cipher and transposition cipher. 6

2. a) Compare statistical anomaly detection and rule based intrusion detection technique. 8

   b) Write a short note on password selection strategies. 6

   c) What is a virus ? Describe the phases in the lifetime of a virus. 6

MODULE – II

3. a) Explain the Chinese remainder theorem. 6

   b) With the help of diagram explain the working of DES algorithm. 8

   c) Explain the terms : Diffusion and Confusion in cryptographic systems. 6

4. a) Discuss the strengths of the DES algorithm. Compare the DES and S-DES algorithms. 8

   b) State Fermat's and Euler's Theorems. Find $\varphi(15)$, $\varphi(7)$, $\varphi(41)$. 6

   c) Explain Hierarchical key control in key distribution in cryptographic systems. 6

P.T.O.

IT 8-2 (RC) 2007 – 08

MODULE – III

5. a) Explain the scenario of secret key distribution with confidentiality and authentication. 6

   b) Perform encryption and decryption using RSA algorithm given p = 11 q = 3 e = 7 and message m = 7. 8

   c) Define hash function. What are the requirements for a hash function ? 6

6. a) Explain how confidentiality and authentication can be achieved using message authentication codes. 6

   b) Explain the MD5 processing of a single 512 bit block. 6

   c) Explain Diffie-Hellman key exchange using suitable example. 8

MODULE – IV

7. a) Explain the Kerberos authentication application. 8

   b) Describe some of the principle services provided by PGP. 6

   c) Write a note on firewalls and the types of firewall. 6

8. a) Describe IPSec along with the services provided. 8

   b) Elaborate on the SMIME functionality. 6

   c) Mention the steps involved in the SSL Record Protocol Transmission. 6

22-5-18

46

IT 8 – 2 (RC)

B.E. (IT) (Semester – VIII) (RC) (2007-08) Examination, May/June 2018
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours

Total Marks : 100

Instructions : *1) Answer **any five** questions with atleast **one** from **each** Module.*
*2) **All** questions carry **equal** marks.*

MODULE – I

1. a) What is cryptanalysis ? Explain different types of attacks on encrypted messages. **6**
   b) With the help of suitable examples, explain active and passive attacks. **6**
   c) What is a virus ? List and explain the different types of viruses. **8**

2. a) With a diagram, describe a digital immune system. **6**
   b) Briefly describe the use of Honeypots. What is the purpose of salt in the Unix password management system ? **6**
   c) Explain Hill Cipher to encrypt the plaintext "MISSION". Also explain the decryption process. Use the key $\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$. **8**

MODULE – II

3. a) Differentiate between double DES and triple DES. **6**
   b) Discuss some of the potential location for confidentiality attacks. **6**
   c) Describe the cipher block chaining mode and cipher feedback modes of operation of DES. **8**

4. a) Explain the application of discrete logarithm in cryptographic systems. **6**
   b) Compare link to link and end to end encryption with appropriate diagrams. **8**
   c) Explain the parameters to be considered while designing Fiestel network. What is the difference between a session key and a master key ? **6**

P.T.O.

IT 8 – 2 (RC)

MODULE – III

5. a) Explain the Encryption, Decryption and key generation process in the RSA algorithm. Also discuss the approaches to attack the algorithm. 8

   b) What are the properties a digital signature should have ? Discuss applications of digital signatures. 6

   c) With neat diagrams explain the basic uses of Hash functions. 6

6. a) Perform encryption and decryption using the RSA algorithm for the following p = 7 q = 11 e = 17 and M = 9. 8

   b) Given prime number to be 23, its primitive root $\alpha = 5$, private key $X_A = 6$ and $X_B = 15$, carry out Diffie – Hellman key exchange. 8

   c) What is the role of compression function in a hash function ? 4

MODULE – IV

7. a) Describe the Kerberos authentication application. 8

   b) Explain S/MIME functionality. 6

   c) Explain the various IPSec services. 6

8. a) Explain the X.509 certificate format. Where is it used ? 8

   b) Discuss firewall characteristics and limitations. 6

   c) Explain some of the key features of SET. 6

21-11-17

IT 8 – 2 (RC)

B.E. (IT) (Semester – VIII) (RC) Examination, Nov./Dec. 2017
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours

Total Marks : 100

Instructions: *1) Answer **any five** questions with at least **one** from **each** Module.*

*2) **All** questions carry **equal** marks.*

MODULE – I

1. a) Compare and contrast different types of security attacks. **4**

   b) Explain Playfair cipher. If user have to send message "GOOD LUCK" using keyword "ENCODE", what will be cipher text transmitted using Playfair cipher. Also verify decrypted message. **6**

   c) With the help of neat diagram, explain digital immune system. **5**

   d) Define following terms: **5**

      i) Data Integrity

      ii) Non Repudiation.

2. a) Explain different transposition techniques for encryption with suitable example. **8**

   b) What is steganography ? Explain some steganography techniques. **6**

   c) List and explain different intrusion detection techniques. **6**

MODULE – II

3. a) With suitable diagram, explain simplified DES scheme. **8**

   b) Explain the terms diffusion and confusion in cryptographic systems. **6**

   c) Using Chinese Remainder Theorem solve : **6**

      $x \bmod 37 = 11$

      $x \bmod 49 = 42$

P.T.O.

4. a) Compare Cipher feedback mode and output feedback mode of operation of DES. 8

   b) Explain how keys are distributed in different scenario and what difficulties needs to be addressed in key distribution. 6

   c) Differentiate between end to end and link encryption. 6

MODULE – III

5. a) What are principle elements of public key cryptosystem ? Explain in detail. 6

   b) Perform encryption and decryption using RSA algorithm. $p = 7, q = 11, e = 17$ and message m= 'I'. 8

   c) State similarity and differences between MD5 and SHA – 1. 6

6. a) Explain creation and use of a digital signature. 6

   b) Explain how confidentiality and authentication can be achieved using Message Authentication Codes. 6

   c) Explain Diffie-Hellman key exchange algorithm with suitable example. 8

MODULE – IV

7. a) How is an X.509 certificate revoked ? 4

   b) Describe some of the principle services provided by PGP. 6

   c) Differentiate between Kerberos version 4 and Kerberos version 5. 6

   d) List the applications of IPSec. 4

8. a) Write short note on S/MIME. 6

   b) Explain key features of secure electronic transaction. 8

   c) Describe different types of firewall with neat diagram. 6

23/5/17

IT 8 – 2(RC)

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

Duration : 3 Hours

Total Marks : 100

Instructions : 1) Answer any five questions with atleast one from each Module.
2) All questions carry equal marks.

MODULE – I

1. a) Explain different types of messages on encrypted messages. 6
   b) With the help of suitable example, explain different transposition techniques. 8
   c) What is the difference between statistical anomaly detection and rule based intrusion detection. 6

2. a) Classify malicious programs and briefly explain them. 6
   b) Explain with suitable example one time pad technique of encryption. 5
   c) Differentiate between steganography and cryptography. 4
   d) Describe symmetric cipher model with suitable diagram. 5

MODULE – II

3. a) Explain automatic key distribution for connection oriented protocol. 6
   b) Which are potential location for confidentiality attacks ? Explain. 6
   c) Describe different modes of operation of DES. 8

4. a) Explain application of discrete logarithm in cryptographic system. 6
   b) Differentiate between Double DES and Triple DES. 6
   c) Write note on : i) Traffic confidentiality ii) Testing for primality 4
   d) Explain the parameters to be considered while designing Fiestel network. 4

P.T.O.

MODULE – III

5. a) Explain the scenario of secret key distribution with confidentiality and authentication. 8

   b) Describe various approaches to attack RSA algorithm. 6

   c) Define hash function. What are the requirements for a hash function ? 6

6. a) Distinguish between direct and arbitrated digital signature. 6

   b) Explain the MD5 processing of a single 512 bit block. 6

   c) Given prime number to be 23, its primitive root $\alpha = 5$, private key $X_A = 6$ and $X_B = 15$, carry out Diffie-Hellman key exchange. 8

MODULE – IV

7. a) Write short note on Kerberos. 8

   b) Explain how key management is done in IPSec. 6

   c) What steps are involved in SSL recent protocol transmission ? 6

8. a) Explain any two transaction type supported by SET. 6

   b) Explain techniques that firewalls use to control access and enforce the site security policy. 4

   c) Compare MIME and S/MIME. 4

   d) Describe general format of PGP message. 6

IT 8 – 2 (RC)

B.E. (IT) (Semester – VIII) (RC) Examination, Nov./Dec. 2016
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours

Total Marks : 100

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

MODULE – I

1. a) Explain different security services defined in X.800. 6
   b) Explain the model for network security. 4
   c) Explain the working of play fair cipher with the help of example. 6
   d) Write a note on steganography. 4
2. a) With the help of diagram explain distributed intrusion detection architecture. 6
   b) What do you mean by audit record ? Explain different types of audit records. 4
   c) Write a note on : 6
      a) Trapdoor
      b) Logic bomb
      c) Trojan horse.
   d) List and explain different password managing techniques. 4

MODULE – II

3. a) Explain briefly different block cipher modes of operation. 6
   b) Explain link versus end-to-end encryption. 4
   c) What is Eulers totient function. Solve the following using Euler totient function. 6
      a) $\phi(37)$
      b) $\phi(15)$
      c) $\phi(21)$
      d) $\phi(25)$
   d) Explain the role of substitution box in DES. 4

P.T.O.

4. a) With the help of neat diagram explain DES. 6
   b) Explain triple DES with two and three keys. 4
   c) Write a note on key distribution. Explain the different ways of key distribution. 6
   d) Write a note on Avalanche effect. 4

MODULE – III

5. a) Explain RSA algorithm. Perform encryption, decryption for p = 11 and q = 3 and e = 3 for message = 7. 6
   b) Compare MD5 and SHA-1. 4
   c) With the help of neat diagram explain digital signature. 6
   d) With the help of diagram explain how MAC can be used to achieve confidentiality and authentication. 4

6. a) Explain MD5 algorithm in detail. 6
   b) Explain basic uses of Hash functions. 4
   c) Explain diffie-Hellman key exchange algorithm. 6
   d) Explain the 3 classes of functions used to produce authenticator. 4

MODULE – IV

7. a) Explain simple authentication dialogue of kerberos. 6
   b) What are the benefits of IPsec ? 4
   c) With the help of diagram explain different types of firewall. 6
   d) Write a note on certificate revocation. 4

8. a) With the help of diagram explain X·509 certificate format. 6
   b) Write a note on SSL. 4
   c) What do you mean by SET. Explain the transaction involved in SET. 6
   d) Write a note on PGP. 4

IT 8-2 (RC)

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

Duration : 3 Hours Total Marks : 100

Instructions : 1) Answer **five** questions in all selecting atleast **one** question from each Module.
2) Assume **missing** data **if** any.

Module – I

1. a) Elaborate on any 8, X 800 security services. 8
   b) With examples, describe the following multi-letter ciphers. 8
      i) Playfair ii) Hill Cipher.
   c) Compare and differentiate nature audit records and detection specific audit records. 4
2. a) Briefly explain the Rule Based Intrusion detection techniques. 6
   b) Describe some of the issues in the design of a distributed Intrusion detection system. With an example, explain the architecture of a distributed IDS. 8
   c) Define a virus. Describe the various phases in the lifetime of a virus. 6

Module – II

3. a) Elaborate on some of the design features of the Feistel Cipher structure. 6
   b) State the advantages of the counter block cipher mode of operation. 4
   c) Compare Link to link and end to end encryption placement techniques. 8
   d) State Fermats and Eulers theorem. 2
4. a) Provide a brief overview of discrete logarithms in public key algorithms. 6
   b) What is a product cipher ? Clearly explain the concept of diffusion and confusion in cryptographic systems. 6
   c) For a user workstation in a typical business environment, list potential locations for confidentiality attacks. 6
   d) What do you mean by Avalanche effect ? Does DES exhibit it ? 2

P.T.O.

Module – III

5. a) Explain the RSA algorithm. Considering the 2 prime numbers to be 11 and 3, determine the private public key pair. 8

   b) Explain the public key authority and public key certificates techniques for distribution of public keys. 8

   c) What is a primitive root ? How is it calculated ? Is 2 a primitive root of 11. Justify your answer. 4

6. a) Elaborate on any 2 approaches to producing message authentication. 8

   b) Users A and B use the Diffie Helman key exchange technique with a common prime q = 71 and a primitive root $\alpha = 7$. 10

      i) If user A has private key $X_A = 5$, what is A's public key Y_A ?

      ii) If user B has private key $X_B = 12$, what is B's public key Y_B ?

      iii) What is the shared secret key ?

   c) Define a Oneway Hash function. Where is it used ? 2

Module – IV

7. a) Elaborate on Kerberos as an authentication service. 8

   b) With a diagram, explain the X.509 authentication service. 6

   c) Write a short note on S/MIME. 6

8. a) Describe any 2 services provided by PGP. 8

   b) Briefly describe the sequence of events that are required for a secure electronic transaction to purchase an item online. 6

   c) Discuss the applications and limitations of firewalls. 6

IT 8 – 2 (RC)

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

Duration: 3 Hours | Total Marks: 100

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

MODULE – I

1. a) Explain the different security services defined in X.800. **6**
   b) Explain the following techniques with example : **4**
      a) Caesar cipher
      b) Rail fence.
   c) Explain the model for network security. **4**
   d) Explain the working of playfair cipher with the help of example. **6**

2. a) Explain the various intrusion detection techniques. **6**
   b) Write a short note on virus. **4**
   c) With the help of neat diagram explain digital immune system. **6**
   d) Write a short note on following malicious programs : **4**
      a) Trap doors
      b) Logic bombs.

MODULE – II

3. a) With the help of neat diagram explain DES. **6**
   b) Compare link encryption and end to end encryption. **4**
   c) Explain briefly different block cipher modes of operation. **6**
   d) Explain the parameters to be considered while designing fiestel network. **4**

4. a) Explain triple DES with 2 keys. **6**
   b) What is the purpose of S-box ? How does it work ? **4**
   c) Explain a transparent key control scheme. **6**
   d) State Fermat's and Euler's theorems. **4**

P.T.O.

MODULE – III

5. a) With the help of example explain RSA algorithm. 6

   b) Explain the 3 classes of functions used to produce authenticator. 4

   c) Explain the following techniques for distribution of public keys : 6

      i) Public key authority

      ii) Public key certificates.

   d) With the help of diagram explain how MAC can be used to achieve confidentiality and authentication. 4

6. a) With the help of neat diagram explain digital signatures. 6

   b) What are the requirements for a hash functions ? Explain one basic use of hash functions. 4

   c) Explain Diffie Hellman key exchange algorithm. 6

   d) Compare MD5 and SHA-1. 4

MODULE – IV

7. a) Describe the sequence of message exchange in keeberos. 6

   b) What are the applications of IP Sec ? 4

   c) How both confidentiality and authentication can be achieved using PGP ? 6

   d) Write a note on S/MIME. 4

8. a) Draw and explain different types of firewall. 6

   b) Compare keeberos ver.4 and keeberos ver.5. 4

   c) Describe the participants of SET with a neat diagram. 6

   d) Write a note on SSL. 4

B - 682

[Total No. of Questions : 8]

(Pages : 02)

IT 8-2 (RC)

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

Duration : 3 Hours

Total Marks : 100

Instructions : 1) Attempt any five questions by selecting at least one question from each Module.

2) Make suitable assumptions if required.

MODULE - I

Q1) a) Explain different types of active and passive attacks. [6]

b) With the help of example explain Hill cipher. [7]

c) Write a short note on steganography. [5]

d) Define Security Mechanism. [2]

Q2) a) What is Intruder? Explain different classes of Intruder. [4]

b) Explain different types of viruses. Also explain structure of virus. [6]

c) With the help of neat diagram explain steps involved in digital Immune system. [5]

d) Write a short note on audit record. [5]

MODULE - II

Q3) a) Explain Single Round of DES Algorithm. [6]

b) What is confusion and diffusion? [4]

c) What is the difference between stream cipher and block cipher. [3]

d) Explain briefly different block cipher modes of operation. [7]

Q4) a) What are the potential locations for confidentiality attacks? How link encryption and end-to-end encryption is used to overcome these attacks? Explain with neat diagrams. [8]

b) With the help of neat diagram explain different steps occur in between KDC, Initiator A and Responder B in key distribution scenario using symmetric Encryption. [6]

c) State [6]

i) Formats Theorem ii) Eulers Theorem

iii) Chinese Remainder Theorem.

P.T.O.

MODULE - III

Q5) a) Explain how authentication and confidentiality is achieved using public key cryptography? [4]

b) Explain how distribution of secret keys using public key cryptography is achieved? [5]

c) Explain Man - in - the - middle attack in Diffie Hellman key exchange algorithm. [4]

d) Explain RSA algorithm with the help of an example. Also state different attacks on RSA algorithm. [7]

Q6) a) Draw and explain Internal and External error control mechanisms using symmetric encryption. Why these mechanisms are used? [6]

b) What is Hash Function? Draw and explain basic uses of Hash function. [8]

c) Draw and explain signing and verifying functions used in Digital signature algorithm. [6]

MODULE - IV

Q7) a) Draw and explain X.50g certificate format. [5]

b) Differentiate between Kerberos version 4 and version 5. [5]

c) Explain different services provided by PGP. [7]

d) What is the functionality of S/MIME? [3]

Q8) a) Write a short note on IPSec. [5]

b) Explain various participants involved in SET. [5]

c) Explain any two Firewall configurations. [5]

d) Write a short note on SSL. [5]

❄❄❄

IT 8 – 2 (RC)

B.E. (IT) (Semester – VIII) (RC) Examination, May/June 2014
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours | Total Marks : 100

Instructions : *1) Attempt **any five** questions selecting atleast **one** question from **each** Module.*
*2) Figures to the **right** indicate **full** marks.*
*3) **Make** suitable assumptions **if required.***

MODULE – I

1. a) Explain various cryptanalytic attacks on encrypted messages based on the amount of information known to the cryptanalyst. **6**
   b) Explain play fair Cipher with the help of an example. **6**
   c) Explain authentication and data integrity security services defined in X-800. **5**
   d) What is Rail fence technique ? **3**

2. a) Explain Rule-based Intrusion detection system. **5**
   b) Explain Logic for a compression virus in detail. **6**
   c) Write a short note on worms. **5**
   d) Explain in brief Generic Decryption Technology. **4**

MODULE – II

3. a) With the help of diagram explain Triple DES in detail. **6**
   b) Explain briefly different Block Cipher modes of operation. **8**
   c) Explain Feistel Cipher structure. **6**

4. a) Write a short note on Front-End Processor. **5**
   b) What is convert channel ? How traffic analysis attack is overcome in link encryption approach ? **6**
   c) Define Fermat's theorem and Euler's theorem. **4**
   d) Write a short note on Chinese Remainder Theorem. **5**

P.T.O.

MODULE – III

5. a) Explain working of RSA algorithm with the help of an example. Also list different possible attacks on RSA. 7

   b) Explain in detail working of Digital Signature Algorithm. 7

   c) State different methods to distribute public keys. Explain any two. 6

6. a) Explain working of Diffie-Hellman Algorithm. Also state and explain disadvantage of this algorithm. 7

   b) Explain how both authentication and secrecy is achieved using public-key cryptosystem. Also state and explain different applications of public-key cryptosystem. 8

   c) Compare MD5 and SHA. 5

16

MODULE – IV

7. a) Explain X-509 certificate format in detail. 6

   b) Compare Kerberos Version-4 and Version-5 in context to environmental shortcomings. 6

   c) List different services provided by PGP. Explain any three. 8

8. a) What is Bastion Host ? Explain different configurations of firewall. 7

   b) Write a short note on SSL. 5

   c) What are applications of IPSec ? 4

   d) Explain in brief functions of S/MIME. 4