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

BE920

No. of Printed Pages:2

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

ation : Three Hours] [Max.Marks :100]

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

MODULE I

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**

a) Write a short note on Steganography? **06**

b) Explain the Rail Fence Transposition technique with a suitable example? **06**

c) Explain the following: **08**
i. Audit Records
ii. Distributed Intrusion Detection
iii. Honeypots
iv. Rule-Based Intrusion Detection

MODULE-II

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**

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: **08**
i. Cipher Feedback
ii. Electronic Codebook

MODULE –III

Q.5 a) Write a short note on Authentication Functions?

b) Explain MD5 Algorithm with a neat diagram?

c) Explain Man-in-the-middle attack(MITM) on Diffie-Hellman's algorithm with a suitable example?

Q.6 a) Differentiate between MD5 and SHA-1 algorithm?

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

c) Write a short note on RSA security?

MODULE-IV

Q.7 a) Explain the different types of Firewall Configurations?

b) Write a Short note on IP Security?

c) Differentiate between Kerberos Version 4 and Kerberos Version 5?

Q.8 a) Differentiate between a Packet-Filtering Router and an Application-Level Gateway?

b) Explain Forward and Reverse Certificates in X.509 Authentication service?

c) Explain any three PGP functions?

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

BE920

No. of Printed Pages:02

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

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

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

MODULE – I

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

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

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

.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

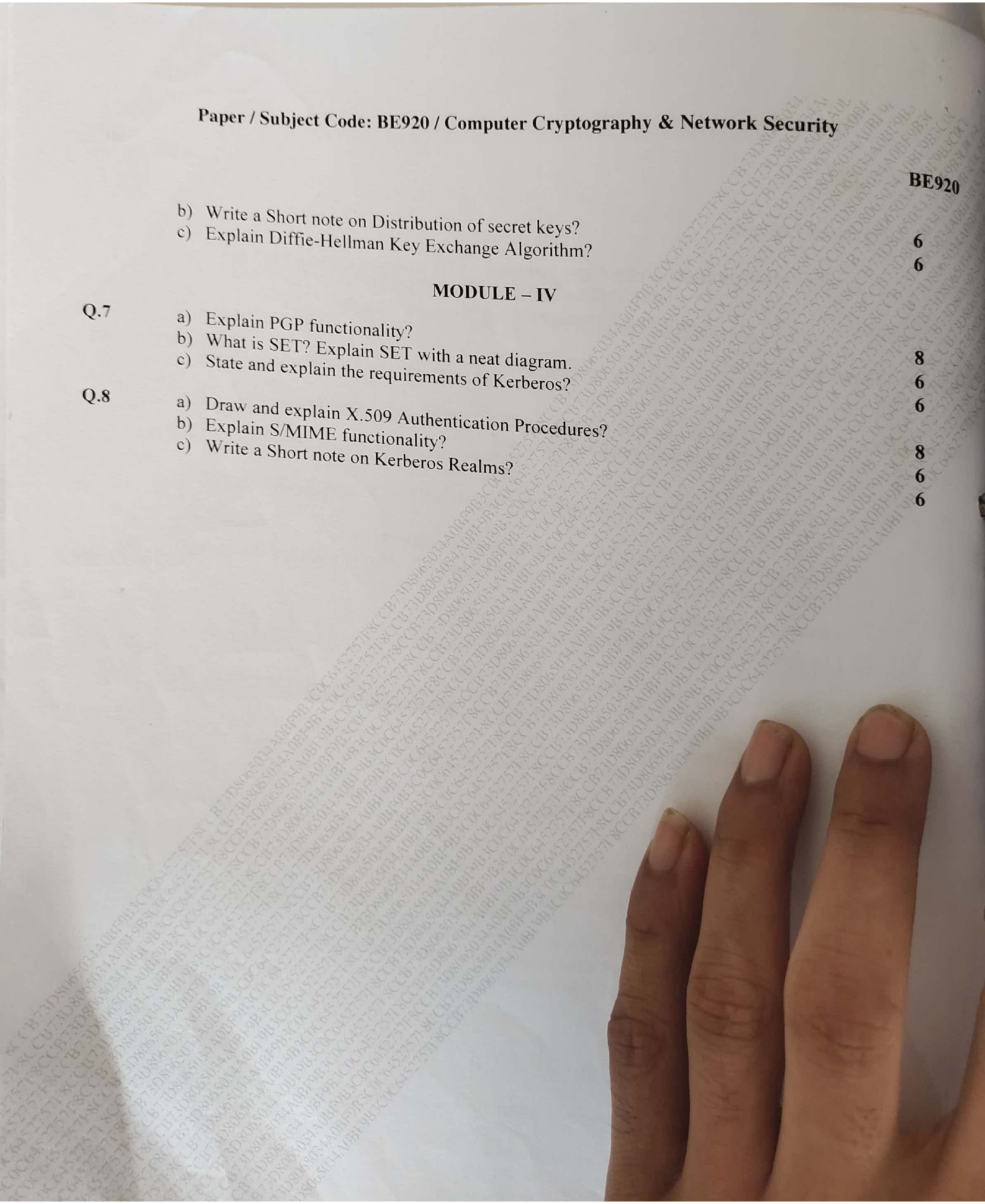
Q.6 a) Explain how MAC can provide message authentication? 8

b) 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



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.

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

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. 2015
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours | Total Marks : 100

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

Module – I

1. a) Write a note on substitution and transposition encryption techniques. 6
   b) Write a note on stegnography. 4
   c) With the help of neat diagram explain compression virus. 6
   d) Distinguish between active and passive attacks. 4

2. a) Explain digital immune system with the help of neat diagram. 6
   b) Explain the approaches to intrusion detection. 4
   c) What is a virus ? Explain the different types of viruses. 6
   d) Write a note on Audit Records. 4

Module – II

3. a) Explain a transparent key control scheme. 6
   b) Explain CBC mode of operation of DES. 4
   c) Explain how control vector scheme is used for controlling key usage. 6
   d) Write a note on avalanche effect. 4

4. a) Draw and explain Fiestel Cipher structure. 6
   b) Elaborate on the concept of hierarchy key control in key distribution in cryptographic system. 4
   c) What is Euler's totient function ? Determine $\phi(N)$ for $\phi(37)$, $\phi(35)$, $\phi(20)$, $\phi(15)$. 6
   d) Write a note on Chinese remainder theorem. 4

P.T.O.

Module – III

5. a) Explain RSA algorithm considering 2 prime numbers to be 11 and 3 determine the private public key pair. 6

   b) What is the difference between Message Authentication Code (MAC) and digital signatures ? State advantages of each. 4

   c) What is the need for public key cryptography ? Explain its principle and how it can be adapted for encryption and authentication. 6

   d) Write a note on Message digest MDS. 4

6. a) With the help of example explain Diffie Hellman key exchange. 6

   b) Explain the different techniques for distribution of public keys. 4

   c) Write a note on digital signatures. 6

   d) With the help of diagrams explain the basic uses of hash functions. 4

Module – IV

7. a) With the help of neat diagram explain x.50 g authentication service. 6

   b) Write a note on PGP. 4

   c) Explain secure electronic transaction in detail. 6

   d) What are the functions of S/MIME ? 4

8. a) Discuss the applications and limitations of firewalls. 6

   b) Write a note on certificate revocation list. 4

   c) Differentiate between version 4 and version 5 of keeberos. 6

   d) Write a note on firewall configurations. 4
