**Avinashilingam Institute for Home Science and Higher Education for Women**

**(Deemed to be University) Coimbatore-641043**

**Master's Degree Examination – November 2018**

**III – Semester**

**Class : II PG** **Time: 3 Hours**

**Major: Information Technology** **Max. marks: 60**

**17MITC16 Information Security**

**Part A** **10 x 1/2=5**

**Choose the correct answer**

1. _____ two different keys will produce two different texts.
   a) Plain text b) Encryption c) Decryption d) Ciphertext

2. Which of the following encryption algorithm takes input as the XOR of the next 6 bits of plain text and preceding ciphertext? _____.
   a) CBC(Cipher Block Chaining) b)CFB(Cipher Feedback)
   b) CTR( Counter) d) ALL the above

3. Public key cryptography is _____ involving the use of two separate keys.
   a) Symmetric b)asymmetric c) Both a & b d) None

4. The better performance could be achieved by adding _____to the exponentiation.
   a) Constant exponentiation b) Random delay c) Blinding d) RSA Algorithm

5. _____ is a method used to overwrite the selected letters of printed text.
   a) Invisible ink b) Character Mark c) Pin punctures d) None

6. The opponent simply copies a message and replays it later with_____.
   a) Mutual b) Simple replay c) Backward d) Time stamps

7. _____ is based on the use of public key cryptography and digital signature.
   a) RSA b) SMTP c) X.509 d) RFC 822

8. The Handshake protocol also defines a shared secret key that is conventional encryption of SSL payloads in _____
   a) Session identifier b)Compression Method
   b) Confidentiality d) Message integrity

9. A _____ is an example of E-mail Virus.
   a) Melissa b) Morris c) Ransom ware d)None

10. The direction in which particular services request may be initiated and allowed to flow through _____ firewall.
    a) Service Control b) User core c) Behavior control d) Direction control

## Part B 5 x 4= 20

**Answer ALL questions**

**Each answer should not exceed 200 words or one page**

11.a) What is cryptography ? Short note on Steganography. (Or)

11 b) Explain the concept of Differential and Linear cryptanalysis.

12.a) Demonstrate Euclid's Algorithm. (Or)

12.b) Summarize about the Elliptic Curve Cryptography.

13.a) Define the Concept of various Hash Functions. (Or)

13.b) Discuss about Digital Signatures in detail.

14.a) Difference between Kerberos Version 4 Vs Version 5. (Or)

14.b) Explain about Secure Electronic Transaction with example.

15.a) Define Virus. Explain the types of viruses. (Or)

15.b) Write the concept of Wireless Security fundamentals.

## Part C 5 x 7 = 35

**Answer ALL questions**

**Each answer should not exceed 600 words or three pages**

16.a) Describe the concept of Substitution Techniques. (Or)

16.b) what is encryption ? Explain Triple DES Algorithm with example.

17.a) Describe about Fermat & Euler Theorem with example. (Or)

17.b) Explain RSA Algorithm with example. Discuss about features and applications.

18.a) Discuss about the message Authentication Function in detail. (Or)

18.b) Explain about Authentication Protocol.

19.a) Explain in detail how E-Mail security can be achieved. (Or)

19.b) Illustrate IP Security and explain in detail.

20.a) Describe Intrusion. Explain Intrusion Detection. (Or)

20.b) Explain about Firewall Design Principals.