16UIT622 – CRYPTOGRAPHY AND NETWORK SECURITY

UNIT-I

K1 questions

1) Interruption attacks are also called as_____ attacks.

a)**masquerade** b)alteration c)denial of service d)replay attacks

2) Virus is a computer_____

a) file b) **program** c)database d)network

3) Ceaser cipher is an example of_____.

a. **Substitutoin cipher** b. Transposition cipher

c. Subsitution as well as transposition cipher d. None of the above

4) Cryptanalyst is a person who_____.

a. Devises cryptography solutions

b. Attempts to break cryptography solutions

c. c. None of these

d. d. Both of these

5) Conversion of cipher text into plain text is called as_____.

a) **Encryption** b) decryption c) cryptography d)crptanalyst

6) Conversion of cipher text into plain text is called as_____

a) Encryption b) **decryption** c) cryptography d)crptanalyst

7) Vernam cipher is also called as_____.

a) Rail fence technique b) **One-time pad**

c) Book cipher d) Running key cipher

8) _____ does not allow the sender of a message to refute the claim of not sending the message .

a) reputation b) un-reputaion c)in-reputation d)**non-reputation**

9) The playfair cipher is also called as_____.a) polymorphic virus
b)stealth virus

a. **Playfair square** b. Playfair circle

c. Playfair oval d. None of the above

10) An attack on cipher text wherein the attacker tries all possibilities is called as_____attack.

a. Chosen cipher text attack

a. Chosen plain text attack

c. Chosen text attack

d. **Brute-force attack**

UNIT-II

1. Expand CBC

   Cipher Block Chaining

   Chain Block Cipher

   Code Block Cipher

   Code Block Chaining

2. Block cipher technique involves encryption of ___block of text at a time.
   a. One
   b. Two
   c. Three
   d. More than 3
3. The concept of confusion and diffusion was introduced by_____
   a. Ron Rivest
   b. James will

c. Claude Shannon

d. Claude Henry

4. IDEA uses ____keys.

a) 3

b) **4**

c) 5

d) 2

5. The number of rounds in RC5 can range from

0 to _____

a) 127

b) 63

c) **255**

d) 31

6. DES is a _____ cipher.

a. Block

b. Stream

c. Both a and b

d. None

7. IDEA was launched in the year_____

a. 1980

b. 1990

c. **1991**

d. 1996

8. RC4 generate a pseudo stream of bits called as _____.

a. Key stream

b. Stream bit

c. Stream vector

d. Key vector

9. How many S-boxes are present in the blowfish algorithm?

a) 2

b) **4**

c) 6

d) 8

10. The RC5 block cipher mode is also called as _____

a. RC5 block cipher

b. RC5 CBC

c. RC5-CBC-pad

d. RC5-CTS

UNIT-III

1. Asymmetric key cryptography is also called _____
   a. **public key cryptography**
   b. private key cryptography
   c. both a and b
   d. none
2. The RSA algorithm is_____
   a. **asymmetric key algorithm**
   b. symmetric key algorithm
   c. both a and b
   d. none
3. _____cryptography solves the problem key agreement and key exchange
   a. Asymmetric key
   b. Symmetric key
   c. Both a and b
   d. None of the above
4. If any two message produces the same message digest thus violating our principal it is called _____
   a. **Collision**
   b. Diffusion
   c. Both
   d. None
5. A specific type of security attack called as _____is used to detect collisions in message digest algorithms
   a. birthday attack

b. sample attack
c. public attack
d. all the above

6. The birthday attack is most often used to attempt discover collisions in hash functions such as_____
   a. **MD5 or SHA1**
   b. RC5
   c. RC4
   d. None of the above
7. The first step in MD5 is_____
   a. **Padding**
   b. Clipping
   c. Both a and b
   d. None of the above
8. The SHA-512 algorithm takes a message of length _____
   a. **2^{128} bits**
   b. 2^{150} bits
   c. 2^{64} bits
   d. 2^{32} bits
9. The _____was developed for performing digital signatures
   a. digital signature standard (DSS)
   b. Ron Rivest
   c. Message Digest
   d. None of the above
10. The _____is public key algorithm which can be used for both digital signatures as well as encryption
    1. ElGamal technique
    2. **Message digest**
    3. Digital signature
    4. All the above

UNIT IV

1. 1. _____ is closely related to the ideas of asymmetric key cryptography.
   a. PKI

b. SKI
c. BKI
d. None of the above

2. _____ are popular standards for digital certificates and PKI.
   a. PKIX
   b. PKCS
   c. Both
   d. None of the above
3. _____ is a trusted agency that can issue digital certificates.
   a. CA
   b. PA
   c. Both
   d. None of the above
4. CA can delegate same of its tasks to this third party, called as a_____.
   a. RA
   b. CA
   c. Both
   d. None of the above
5. _____ uses the idea of certificate trust levels.

   A) X509 **B) PGP**

   C) KDC D) none of the above

6. _____ provides privacy, integrity, and authentication in e-mail.

   A) IPSec B) SSL

   C) PGP D) none of the above

7. It is desirable to revoke a certificate before it expires because
   a) the user is no longer certified by this CA
   b) the CA's certificate is assumed to be compromised
   c) the user's private key is assumed to be compromised
   d) all of the mentioned

8. CRL stands for

   a) Cipher Reusable List

b) Certificate Revocation Language

c) **Certificate Revocation List**

d) Certificate Resolution Language

9. How many functions are involved in the PKIX architectural model?

a) 3

b) 5

c) 6

d) **7**

10. Which systems use a timestamp?

i) Public-Key Certificates

ii) Public announcements

iii) Publicly available directories

iv) Public-Key authority

a) i) and ii)
b) iii) and iv)
c) **i) and iv)**
d) iv) only

UNIT V

1.Encapsulating Security Payload (ESP) belongs to which Internet Security Protocol?

a. Secure Socket Layer Protocol
b. Secure IP Protocol
c. Secure Http Protocol
d. Transport Layer Security Protocol

2.Which one of the following belongs to SSL protocol?

e. Handshake Protocol
f. Change Cipher Spec protocol
g. **Both (a) and (b)**
h. None of the above

3.The criteria which makes TLS more secure than SSL is

i. Message Authentication
j. Key material generation
k. **Both (a) and (b)**
l. None of these

5.Which security protocol is used to secure pages where users are required to submit sensitive information?

m. **Secure Socket Layer**
n. Transport Layer Security
o. Secure IP
p. Secure HTTP

5. SET is

q. **Electronic Payment System**
r. Security Protocol
s. Credit card payment
t. Internet Payment System

6.Total no. of messages used in SSL Handshake Protocol is

u. 12
v. 10
w. 8
x. 14

7. Which of the following can be used for secure exchange of email?

1. HTTPS
2. WEP
3. **S/MIME**
4. WAP

8. An HTTP connection uses port _____ whereas HTTPS uses port _____ and invokes SSL.

a) 40; 80
b) 60; 620

c) **80; 443**
d) 620; 80

9. TLS is an extension of ----------
a. HTTP B) TELNET C) SSL D)**FTP**

10.Which among them has the strongest wireless security?
a) WEP
b) WPA
c) WPA2
d) **WPA3**

16UIT622 – CRYPTOGRAPHY AND NETWORK SECURITY

K2 LEVEL

UNIT I

1) Define Cryptography.
2) Difference between plaintext and cipher text.
3) Define Caesar cipher.
4) Compare Homophonic substitution cipher and Polygram substitution cipher.
5) Define Transposition techniques.
6) Define possible types of attacks .
7) Difference between encryption and decryption .
8) Define asymmetric key.
9) Define Steganography.
10) What is mean by fabrication

UNIT II

1. Classify the algorithm types?
2. Define Initialization vector.
3. Give one usage of CFB.
4. Illustrate a security-related advantage of counter.
5. List out the encryption techniques and standards that became a part of RC4.
6. What are the disadvantages of double DES?
7. What are the CFB and OFB modes?
8. What are the different modes of operation in DES?
9. What is the most innovative feature of IDEA?
10. List the steps to produce a cipher text using a stream cipher.

UNIT III

1. State the uses of RC4
2. What is the block size used for MD5, SHA-1?
3. Which algorithm is very similar to MD5?
4. What is the practical difference between the SHA-1 and MD5?
5. What do you mean by hash function?
6. Define asymmetric key
7. Explain the steps in SHA algorithm
8. What is MAC
9. What are the disadvantages in HMAC
10. Expand SHA-1

UNIT IV

1) What is the main use case for PKI?
2) How are client certificates used in PKI?
3) What is a Certificate Authority's role in PKI?
4) What is the difference between Public Key Infrastructure and Public Key Cryptography? How are they related?
5) What is the main use case for PKI?
6) Define revocation.
7) Define Digital certificates.
8) Difference between OCPS and SCVP
9) What is RNG?
10) What is Registration Authority (RA)?

UNIT V

1) Expand TLS.
2) Expand SET.
3) What are the types of Electronic money.
4) Write any two points about security layer.
5) Define GSM.
6) Expand GSM.
7) **Define** S/MIME.
8) **Decide** why PGP generate a signature before applying compression.
9) **What** are the elements of MIME?

10)**What** is meant by SET?

16UIT622 – CRYPTOGRAPHY AND NETWORK SECURITY

K3 LEVEL

5 MARKS:

1) Explain in detail about Diffie-helman key exchange algorithm .

2) Give the short notes for possible types of attacks.

3) Explain the basics of cryptography terms.

4) Give the detail about attack in general view.

5) Which is the modified version of Caesar cipher give the details about this ?

UNIT II

1. Explain about stream cipher.
2. Explain about block cipher.
3. Write short note about CFB mode.
4. .Overview of symmetric key Cryptography.
5. How DES works? Explain it.

.

UNIT III

1. Explain an overview of Asymmetric key cryptography
2. Compare and contrast the Symmetric and Asymmetric key cryptography
3. Explain the requirements of a message digest in short
4. Compare and contrast the MD5 and SHA-1
5. Explain PKIX model in brief.

UNIT IV

1) Discuss PKI.
2) Explain the concept of digital certificates.
3) Write short note on certification Authority (CA).
4) Write short note on certificate creation steps.
5) How can we verify a Digital certificate?

UNIT V

1) Explain security in 3G.
2) Differentiate SSL and SET.
3) Summarize TSP in detail with diagrams.
4) Write about the working of SSL.
5) Explain about Email security.

16UIT622 – CRYPTOGRAPHY AND NETWORK SECURITY

K4 & K5 LEVEL

UNIT I

1.) Discuss in detail about Transposition technique.
2. 2) Explain a) Playfair cipher b) Hill cipher.
3. 3) Give short notes for Substitution techniques and its working methodology?
4. 4) Discuss : Principles of attacks
5. 5) Compare all the types of (a) virus phases and (b) classifications

UNIT II

1. Brief explain about algorithm modes.
2. Explain about DES algorithm.
3. Explain about IDEA.
4. Explain about RC5 algorithm with example.
5. Brief explain about AES algorithm.

UNIT III

1. Summarize RSA algorithm
2. Give an outline on MDS
3. Demonstrate PKCS
4. Summarize SHA-S12 with neat diagram
5. Demonstrate digital certificates

UNIT IV

1. Discuss about Digital Certificates.
2. Explain Certificate Revocation.
3. Define the following:
    a. Certificate type
    b. Roaming Certificates
    c. Attribute Certificates
4. Discuss about Public Key Cryptography Standards (PKCS).
5. Discuss about the PKIX model.

UNIT V

1. Describe Secure Socket Layer.

2) Explain Secure Electronic Transaction.

3) Explain the types of electronic money.

4) Give an outline on Email security.

5) Summarize PGP in detail with the diagram