G7907 **Pages 3**

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Scheme for Valuation/Answer Key

Scheme of evaluation (marks in brackets) and answers of problems/key

SEVENTH SEMESTER B.TECH DEGREE EXAMINATION, DECEMBER 2018

Course Code: CS409

Course Name: CRYPTOGRAPHY AND NETWORK SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks. Marks

1 Definition - (1.5 +1.5), example - (.5 + .5) (4)

2 C = (p+20) mod 26 – 1, nbcmcmuhyrylwcmy - 3 (4)

3 Reason – 2 marks, advantage -1, disadvantage - 1 (4)

4 Key Generation - private key(Random) (4)

Public Key - based on the private key(multiplicative inverse (2 marks)

Encryption of message using public key - 2 Marks

5 GCD(1970, 1066)= 2. (4)

Any method can be adopted to find gcd like Euclid's Algorithm, Extended Euclid's Algorithm etc (4 Marks)

6 Hash value of the message should be encrypted by private key of the sender - 4 (4)

7 Private key ring can be viewed as a table in which each row represents one of the public/private key pairs owned by user. Each row contains the entries: Timestamp, KeyID, public key, private key, USER ID (at least four fields – each 1 mark) (4)

8 (4)

1. Enveloped data (1 mark)
2. Signed data (1 mark)
3. Clear-signed data (1 mark)
4. Signed and enveloped data (1 mark)

9 The alert protocol is used to alert status changes to the peer. The primary use of this protocol is to report the cause of failure. Status changes include error condition like invalid message received or message cannot be decrypted, connection has closed. (4 Marks) (4)

10

- Tunneling involves allowing private network communications to be sent across a public network, such as the Internet.
- As the packets move through the tunnel, they are encrypted and

encapsulated into another IP packet

- Encapsulation allows the packets to arrive at their proper destination. At the final destination, de-capsulation and decryption occur (4 marks)

PART B

Answer any two full questions, each carries 9 marks.

11 a) The answer will vary based on the playfair matrix used. (like normally i/j combined.) (5)

Marks can be given for the correct answer based on the chosen playfair matrix by following the rules for encryption

Playfair matrix- 2 marks

Encryption - 3 Marks

b) Key generation schedule (4)

i. Input Key

ii. Permuted choice one (PC-1)

iii. Permuted choice two (PC-2)

iv. Schedule of Left Shifts (One mark each)

12 a) Initialization 1 mark (4)

Initial permutation of S 1 mark

Stream generation 1 mark

Diagram 1 mark

b) Algorithm 2 marks (5)

Diagram 2 marks

Explanation 1 mark

13 a) C = KP mod 26 – 1 mark, problem solution – 3 mark, Answer = ZXXD (4)

b) S box creation steps (5)

Initialization 1 mark

Map each byte to its multiplicative inverse 1 mark

Applying transformation to each bit - 3 marks

PART C

Answer any two full questions, each carries 9 marks.

14 a) $\phi(n)$ –the number of positive integers less than n and relatively prime to n 1 mark (5)

$\phi(pq) = (p-1)(q-1)$, proof 4marks

If the students have tried to illustrate through an example, 2 marks can be given.

b) Algorithm – 4 marks (4)

15 Steps – 3 marks, compression function and explanation – 3 marks, diagrams – 3 marks (9)

16 a) Security requirements – 8 points, 0.5 marks each (4)

b) Key generation – 2 marks, encryption/decryption – 3 marks (5)

PART D

Answer any two full questions, each carries 12 marks.

17 a) Block diagram or flow chart for generating message for transmission – 2 marks, its explanation – 2 marks (8)

Block diagram or flow chart for reception of message – 2 marks, its explanation – 2 marks

b) (4)

1. IPSec Protocol(AH or ESP) and mode of protocol(transport or tunnel) - 1 mark
2. Authentication algorithm and its key - 1/2 mark
3. Encryption algorithm, its key and initialization vector – 1/2 mark
4. Sequence number counter – 1/2 mark
5. Anti replay window – 1/2 mark
6. Life time of SA – 1/2 mark

Path MTU – 1/2 mark

18 a) SET components – 2 marks, dual signature – 2 marks, Payment processing – 4 marks (8)

b) Any four differences – 1 marks each. (4)

19 a) Sequence numbering with sliding receiver window in AS and ESP is designed to thwart replay attacks (3 marks each) (6)

b) Handshake protocol steps – 4 marks, diagram – 2 marks (6)

****