HALDIA INSTITUTE OF TECHNOLOGY

(AN AUTONOMOUS INSTITUTION UNDER MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL)

Paper Code: PCC-CS 504

Paper Name: Cryptography

Time Allotted: 3 Hours   *Full Marks*: 70

The figures in the margin indicate full marks

Candidates are required to give their answers in their own words as far as practicable

Group – A

(Multiple Choice Type Questions)

Choose the correct alternatives from the followings: **15 x 1 = 15**

1. (i) To achieve reliable transport in TCP, ___________ is used to check the safe and sound arrival of data.
a) Packet   b) Buffer   [✓ c) Segment]   d) Acknowledgment

(ii) Which of the following is not applicable for IP?
a) Error reporting   b) Handle addressing conventions
[✓ c) Datagram format]   d) Packet handling conventions

(iii) In asymmetric key cryptography, the private key is kept by ___________
a) sender   [✓ b) receiver]
c) sender and receiver   d) all the connected devices to the network

(iv) Which of the following is the meaning of crypt?
a) Hidden   b) Writing   c) Copied   [✓ d) Both a and b]

(v) Which of the following principle of cryptography explains transmitted data in cannot be denied from being accepted the message received?
a) Privacy   b) Reliability   [✓ c) Non-repudiation]   d) Authentication

(vi) Which of the following is not a characteristic of a good encryption algorithm?
a) Confidentiality   b) Integrity   c) Availability   [✓ d) Authentication]

(vii) Which of the following is not a type of key agreement protocol?
a) Diffie-Hellman   b) ECDH   c) RSA   [✓ d) MQV]

(viii) Which of the following is a type of transposition cipher?
a) Caesar cipher   b) Playfair cipher   [✓ c) Rail fence cipher]   d) Vigenereciphe

(ix) How many rounds does the AES-256 perform?
a) 10   b) 12   [✓ c) 14]   d) 16

(x) _________ substitution is a process that accepts 48 bits from the XOR operation.
[✓ a) S-box]   b) P-box   c) Expansion permutations   d) Key transformation

(xi) Which encryption algorithm is used in HTTPS (Hypertext Transfer Protocol Secure)?
a) DES   [✓ b) RSA]   c) Blowfish   d) AES

(xii) Which of the following is not a characteristic of a good hash function?
a) Collision resistance   b) One-wayness   [✓ c) Reversibility]   d) Determinism

(xiii) While creating an envelope, we encrypt the ………………… with the …………… .
a) sender's private key, one time session key   b) receiver's public key, one time session key

c) one time session key, sender's private key [✓ d) one time session key, receiver's public key]

(xiv) When a hash function is used to provide message authentication, the hash function value is called to as:
a) Message Field [✓ b) Message Digest] c) Message Score d) Message Leap

(xv) Firewall is type of------
a) virus b) security threat c) worm [✓ d) none of these]

Group – B

(Short Answer Type Questions)

Attempt any three from the followings: **3 x 5 = 15**

2. (i) What is Symmetric and Asymmetric Cipher?
(ii) What are the drawbacks of Symmetric Cipher and how is it overcome in Asymmetric Cipher? 2+3

3. (i) Briefly define the Playfair cipher.
(ii) Construct a playfair matrix with the key EXAMPLE. Using this matrix encrypt the message "HIDE THE GOLD". 2+3

4. (i) What is the purpose of S-boxes in DES?
(ii) Explain the avalanche effect? 3+2

5. (i) What do you mean by primitive root of a prime number p? Is 3 a primitive root of 7?
(ii) Given p=19, q=23, and e=3 Use RSA algorithm to find n, ϕ(n) and d. 2+3

6. (i) What do you mean by digital signature?
(ii) How digital signatures can be enforced using encryptions? Illustrate with an example. 2+3

Group – C

(Long Answer Type Questions)

Attempt any four from the followings: **4 x 10 = 40**

7. (i) What is the diffusion and confusion principal?
(ii) Which one is achieved by transposition cipher and substitution cipher?
(iii) Given the plaintext"LOST IN PARADISE", compute the cipher text for
a) The Ceaser cipher with key = 5.
b) The Railfence cipher with rails = 4. 3+3+4

8. (i) Define the terms Ring, Group, Field.
(ii) Explain the various active attacks? What security mechanisms are suggested to counter attack active attacks?
(iii) What is man in the Middle Attack? 3+5+2

9. (i) Define AES Algorithm with details of one round operation.
(ii) Write short notes on IDEA algorithm. 5+5

10. (i) Explain Diffie-Hellman algorithm.
(ii) User A and B exchange the key using Diffie-Hellman algorithm. Assume α=5 q=11 XA=2 XB=3. Find the value of YA, YB and k. 5+5

11. (i) Describe SHA-1 (message digest) algorithm.
(ii) How SHA-1 is differing from MD5?
(iii) Define Hash Function in cryptographic Algorithm. 3+3+4

12. Write short notes. (Any four) 4X2.5 = 10
[✓ i) Email Security] ii) SSL Protocol [✓ iii) Hash Function]
[✓ iv) Digital Signature Algorithm] [✓ v) Steganography] vi) Firewall