www.makaut.com

ENGINEERING & MANAGEMENT EXAMINATIONS, APRIL – 2009

DATA COMPRESSION & CRYPTOGRAPHY

SEMESTER - 8

Time : 3 Hours] [Full Marks : 70

GROUP – A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for the following : 10 × 1 = 10

i) If the principle of ..... to be ensured, the contents of a message must not be modified while in transit.

a) confidentiality b) authentication

c) integrity d) access control. ☐

ii) The ..... attack is related to confidentiality.

a) interception b) fabrication

c) modification d) interruption. ☐

iii) 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. ☐

www.makaut.com

www.makaut.com

iv) Biometric authentication works on the basis of

a) human characteristics b) passwords

c) seed d) random challenge. ☐

v) DOS attacks are caused by

a) alternation b) authentication

c) fabrication d) replay attacks. ☐

vi) When two different messages digests have the same value, it is called as

a) attack b) collision

c) hash d) none of these. ☐

vii) Lossy image simplification is based on ..... operation.

a) DCT b) CCIT

c) ISO d) DMS. ☐

viii) Typical lossless compression for manual image is

a) 3 : 1 b) 4 : 1

c) 2 : 1 d) 4 : 3. ☐

ix) Symmetric key cryptography is ..... asymmetric key cryptography.

a) always slower than b) of the same speed as

c) faster than d) usually slower than. ☐

x) If *A* and *B* want to communicate securely with each other, *B* must not know

a) *A*'s private key b) *A*'s public key

c) *B*'s private key d) *B*'s public key. ☐

www.makaut.com

www.makaut.com

GROUP – B

(Short Answer Type Questions)

Answer any *three* of the following. 3 × 5 = 15

2. a) When an encryption algorithm is said to be computationally secure ?

   b) What are the different types of attacks on computer and network systems ? 2 + 3

3. Differentiate between lossless and lossy compression techniques with suitable example. What broad types of multimedia data are each most suited to ?

4. Show how you would encode the following token stream using run length encoding :

   ABC000AAB00000000DEFAB00000.

   What is the compression ratio obtained ?

5. Explain DOS attack. What are IP sniffing and IP spoofing ? 3 + 2

6. What are the typical contents of Digital Certificate ? Discuss Key exchange protocol. 3 + 2

7. For the following symbols whose probability of occurrence is given along with the symbol, calculate Huffman codes. Find also the average code length.

Symbols	***Probability***
A	0·2
B	0·3
C	0·4
D	0·05
E	0·05

www.makaut.com

www.makaut.com

GROUP – C

(Long Answer Type Questions)

Answer any *three* of the following. 3 × 15 = 45

8. a) Is it possible to combine symmetric key and asymmetric key cryptography so that better of the two can be combined ? 5

   b) Write short notes on the following : 2 × 5 = 10

      i) Digital signature

      ii) Message digest.

9. What is Transform Coding ? Briefly describe. Suppose eight characters have a distribution :

   A : (1), B : (1), C : (1), D : (2), E : (3), F : (5), G : (5), H : (10)

   a) Draw a Huffman tree for this distribution.

   b) What is the average no. of bits needed for each pixel using Huffman Coding ?

10. Briefly describe the following dictionary based coding :

    a) LZW compression algorithm

    b) LZW DeCompression Algorithm with example.

11. a) Explain active attack and passive attack with example. 5

    b) Describe briefly DES algorithm. 7

    c) Explain Verman cipher. 3

www.makaut.com

www.makaut.com

12. a) Differentiate between Fixed Length Coding and Variable Length Coding with suitable example. 4

b) What is entropy of a source ? Estimate the entropy of the following source which generates the symbol as following :

1 1 1 2 2 1 1 3 3 4 4 4 1 1 1 1 + 5

c) Discuss the concept of Run Length Encoding. 5

END

www.makaut.com