

BE-SEM-VII (C.B.S.G.S) EXTC - Data compae. and encryption
 Data compression and encryption
 Q.P. Code : 788901
 21/12/16

(3 Hours)

[Total Marks : 80

- N.B. : (1) Question No.1 is Compulsory.
 (2) Attempt **any three** questions out of remaining questions.
 (3) Assume suitable data wherever necessary.

1. Answer in brief. (Any Four) 20
 - (a) Explain different redundancies in data and how they are used for data compression. Also give evaluation parameters for compression techniques.
 - (b) What are the goals of cryptographic systems? Describe various attacks compromising these goals.
 - (c) State Fermat's Little Theorem, Euler's Theorem in modular arithmetic. What is Euler's Totient function? Compute $\Phi(37)$, $\Phi(35)$, and $\Phi(75)$.
 - (d) Give an example of each:
 - Substitution cipher
 - Transposition cipher
 - Stream cipher
 - Block cipher
 - (e) Explain extended Euclid's algorithm, and compute multiplicative inverse of 7 modulo-160.
2. (a) Explain the principle of arithmetic coding. Hence generate a decimal tag for the sequence: **SWISS_ MISS**. Also decode the decimal tag. 10
 - (b) What are the advantages of minimum variance Huffman codes over normal Huffman codes? Design a minimum variance Huffman code on the source with alphabet $A=\{a_1, a_2, a_3, a_4, a_5\}$ with respective probabilities $\{0.25, 0.2, 0.15, 0.3, 0.1\}$. 10
3. (a) Explain lossy and lossless schemes for image compression. Give an overview of JPEG-2000. 10
 - (b) Explain Frequency masking, Temporal masking with respect to audio compression. Also explain how an MP-III encoder works. 10

125-1

TURN OVER

Q.P. Code : 788901

2

4. (a) Compute the encrypted and decrypted text using RSA algorithm for the plaintext 88. Public key is $(n, e) = (187, 7)$. 10
- (b) Perform LZ-78 compression on the following string and find the compression ratio. 100011110101111000111110001111 10
5. (a) Explain Triple-DES with two keys and the "Meet-in-the-middle-attack". 10
- (b) Consider a Diffie-Hellman scheme with a common prime $q=11$ and a primitive root $\alpha=2$. 10
- (i) Show that 2 is primitive root of 11.
- (ii) If user A has public key $Y_A=9$, what is A's private key X_A ?
- (iii) If user B has public key $Y_B=3$, what is the shared secret key K?
6. Write short notes on (Any Four). 20
- (a) Digital Signatures
- (b) H.264. Video coding standard
- (c) Ethical Hacking
- (d) Digital Immune Systems
- (e) Elliptic curves for cryptography

125-2