Department of Electronics & Telecommunication Engineering

Data Compression & Encryption

Sem V (CBCGS-H)

Mock Question Paper

1. A Huffman encoder takes a set of characters with fixed length and produces a set of characters of (1M)
   a. Fixed Length
   b. Constant Length
   c. Random Length
   d. Variable Length

2. What is RLE compressed output for the input 'ABBCCCDDDDEEEEE'? (2M)
   a. A1B2C3D4E5
   b. 122333444455555
   c. a1b2c3d4e5
   d. E5D4C3B2A1

3. A source emits letters from the alphabet A = {m, n , o , p , q} with probabilities p(m) = p(n) = 0.2, p(o) = 0.4, p(p) = p(q) = 0.1. Calculate the entropy of the source. (2M)
   a. 2.2 bits/symbol
   b. 2.12 bits/symbol
   c. 1.5 bits/symbol
   d. 2.5 bits/symbol

4. The unit of information is (1M)
   a. Nats
   b. Bits
   c. Decits
   d. Digits

5. The basic idea behind Huffman coding is to (1M)
   a. expand data by using fewer bits to encode more frequently occurring characters
   b. compress data by using fewer bits to encode fewer frequently occurring characters
   c. compress data by using more bits to encode more frequently occurring characters
   d. compress data by using fewer bits to encode more frequently occurring characters

6. In dictionary techniques for data compaction, which approach of building dictionary is used for the prior knowledge of probability of the frequently occurring patterns? (1M)
   a. Static Dictionary
   b. Adaptive Dictionary
   c. Both Static and Adaptive Dictionary
   d. Neither static nor adaptive dictionary

7. If the Search buffer in LZ77 is a b a b r a r then decode the sequence for the token <3,5,C(d)> (2M)
   a. rarrrr
   b. rarrrd
   c. rarrad
   d. raraad

8. A sequence is encoded using the LZW algorithm and the initial dictionary is: 1. a, 2. space, 3. r, 4. t. The output of the LZW encoder is the following sequence 3, 1, 4, 6, 8, 4. Decode the sequence. (2M)
   a. ratatatt
   b. ratatata
   c. ratatttt
   d. rattata

9. Down sampling is to make a digital image file smaller by (1M)
   a. Removing Pixels
   b. Adding Pixels
   c. Removing Noise
   d. Adding Noise

10. In a typical picture, most pixels will be (1M)
    a. Very similar to their neighbours
    b. Very different from their neighbours
    c. Equal in value
    d. Bright

11. The best visual compression quality is achieved using (1M)
    a. Fourier Transform
    b. Wavelets
    c. Discrete Cosine Transform
    d. Discrete Sine Transform

12. Digitizing the coordinates of image is called (1M)
    a. Sampling
    b. Quantization
    c. Framing
    d. Coding

13. If frames are displayed on screen fast enough, we get an impression of (1M)
    a. Signals
    b. Motion
    c. Packets
    d. Bits
14. Block size in block preparation step of JPEG compression is (1M)
    a. 4 x 4
    b. 8 x 8
    c. 16 x 16
    d. 64 x 64

15. Which of the following is not a compression technique? (1M)
    a. MPEG
    b. JPEG
    c. Supervised Coding
    d. Run Length Coding

16. In the coding redundancy technique, we use (1M)
    a. Fixed length code
    b. Random length code
    c. Variable length code
    d. Constant length code

17. Suppose we want to transmit a 512 x 512, 8-bits-per-pixel image over a 9600 bits per second line. How much time it takes to transmit the entire image? (2M)
    a. 60 sec
    b. 219 sec
    c. 200 sec
    d. 120 sec

18. The size of an image before compression is 2Mb and its size after compression is 500 Kb. The compression ratio of the said compression technique is (2M)
    a. 4:1

b. 2:1
c. 16:1
d. 1:1

19. An asymmetric-key (or public-key) cipher uses (1M)
a. 1 key
b. 2 keys
c. 3 keys
d. 4 keys

20. Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not (1M)
a. Authenticated
b. Confidential
c. Joined
d. Separate

21. We are provided the plain text "SUN". You need to convert the given plain text into ciphertext under the Caesar cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 2? (2M)
a. UWP
b. VXQ
c. TVO
d. NUS

22. Shift cipher is sometimes referred to as the (1M)
a. Asymmetric Cipher
b. Substitution Cipher
c. Block Cipher
d. Caesar Cipher

23. DES stands for (1M)
a. Data Encryption Subscription
b. Data Encryption Solutions
c. Data Encryption Standard
d. Digital Encryption Standard

24. In Cryptography, original message, before being transformed, is called (1M)

a. Simple Text
b. Plain Text
c. Cipher Text
d. Coded Text

25. In Asymmetric-Key Cryptography, although RSA can be used to encrypt and decrypt actual messages, it is very slow if message is (1M)
a. Short
b. Long
c. Flat
d. Thin

26. In symmetric key cryptography, key used by sender and receiver is (1M)
a. Shared between the sender and receiver
b. Unique
c. Different
d. Shared publicly

27. The value of the following Euler's Totient function ϕ(231) is (2M)
a. 60
b. 213
c. 230
d. 123

28. Consider a function: f(n) = number of elements in the set {a: 0 <= a < n and gcd(a,n) = 1}. What is this function? (1M)
a. Primitive
b. Totient
c. Primary
d. Secondary

29. The inverse of 49 mod 37 is (2M)
a. 31
b. 23
c. 22
d. 34

30. In cryptography, the order of the letters in a message is rearranged by (1M)

a. Transpositional Cipher
b. Substitution Cipher
c. Caesar Cipher
d. Both Transpositional and Substitution Cipher

31. Which is the largest disadvantage of the symmetric Encryption? (1M)
a. More complex and therefore more time-consuming calculations.
b. Problem of the secure transmission of the Secret Key
c. Less secure encryption function.
d. Isn't used any more

32. Asymmetric Encryption: Why can a message encrypted with the Public Key only be decrypted with the receiver's appropriate Private Key?
a. Not true, the message can also be decrypted with the Public Key
b. A so called "one-way function with back door" is applied for the encryption
c. The Public Key contains a special function which is used to encrypt the message, and which can only be reversed by the appropriate Private Key
d. The encrypted message contains the function for decryption which identifies the Private Key

33. DES is a type of (1M)
a. Caesar Cipher
b. Block Cipher
c. Stream Cipher
d. Bit Cipher

34. Which one of the following uses a 128bit round key to encrypt the data using XOR and use it in reverse to decrypt it? (1M)
a. Round key algorithm
b. Public key algorithm
c. Advanced Encryption Standard
d. Asymmetric key algorithm

35. Cryptanalysis is used (1M)
a. To increase the speed
b. To find security flaws in a cryptography scheme
c. To encrypt the data
d. To decrypt the data

36. Cryptographic hash function takes an arbitrary block of data and returns (1M)
a. Random sized bit string

b. Variable sized bit string
c. Fixed size bit string
d. Bit string of the same size as that of the input

37. The input block length in AES is: (1M)
    a. 56 bits
    b. 64 bits
    c. 128 bits
    d. 512 bits

38. SSL provides _________. (1M)
    a. Message Integrity
    b. Confidentiality
    c. Compression
    d. Integrity, Confidentiality, and compression

39. Which one of the following is not a higher-layer SSL protocol? (1M)
    a. Alert Protocol
    b. Alarm Protocol
    c. Handshake Protocol
    d. Change Cipher Spec Protocol

40. Which of the following is not an element/field of the X.509 certificates? (1M)
    a. Issuer Name
    b. Serial Modifier
    c. Issuer unique Identifier
    d. Signature