|| Jai Sri Gurudev ||

SRI ADICHUNCHANAGIRI SHIKSHANA TRUST ®

ADICHUNCHANAGIRI INSTITUTE OF TECHNOLOGY

(Affiliated to VTU, Belagavi | Approved by AICTE, New Delhi | Recognized by Govt. of Karnataka)

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

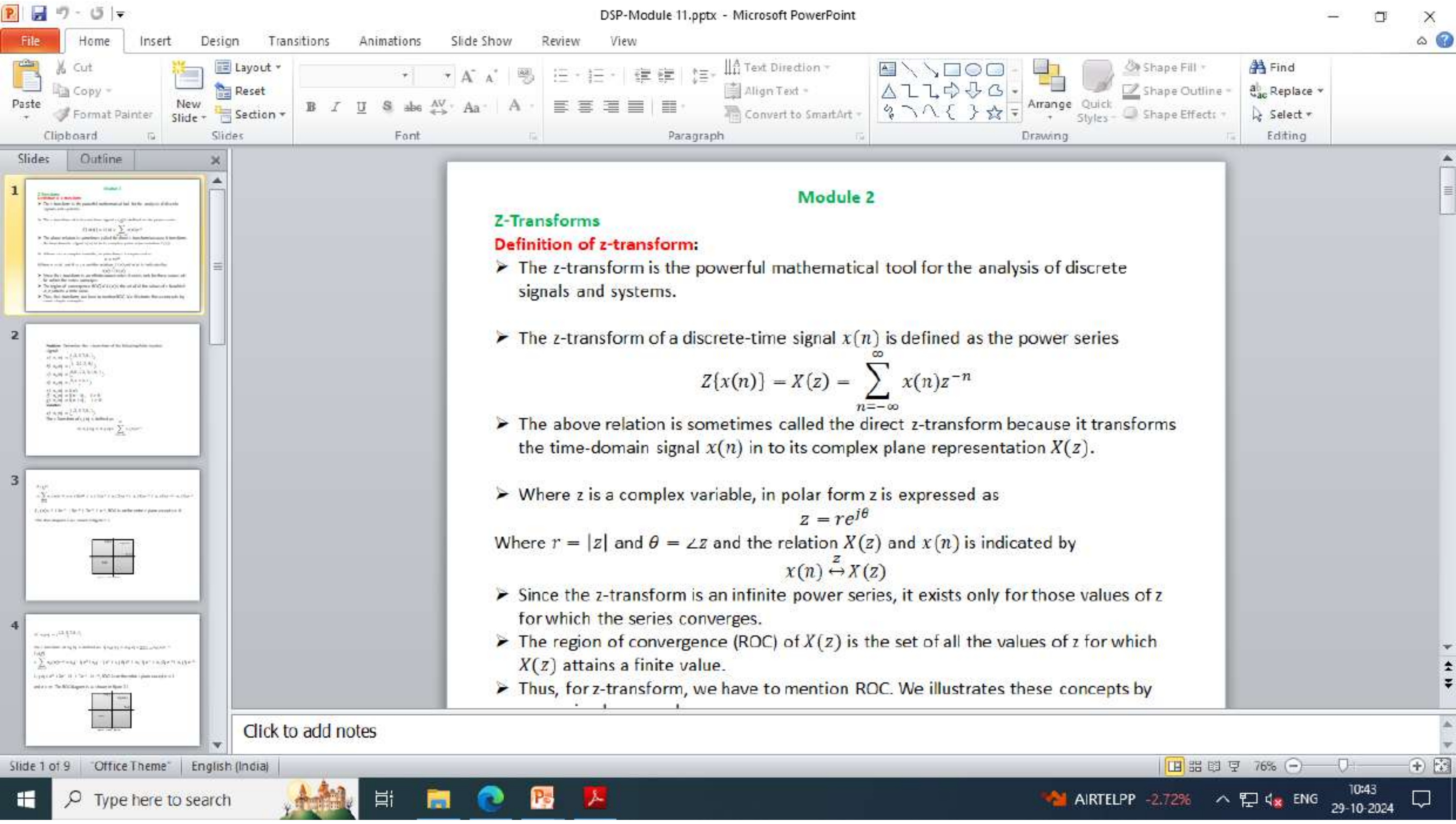
CHIKKAMAGALURU - 577 102

(Accredited by NBA and NAAC)

Teachers use ICT enabled tools for effective teaching-learning process.

SL NO	Experimental learning	Participative learning	Problem solving	subject	Faculty	Date of conduction	No of students
1	PPT			Digital signal processing	Dr Harish M S	20-09-2024	65
2		QUIZ		Cryptography	Divya G S	30-03-2024	65

Professor & Head
Dept. of Electronics & Communication Er...
Adichunchanagiri Institute of Technology,
Chikmagalur - 577 102



Module 2

Z-Transforms

Definition of z-transform:

- The z-transform is the powerful mathematical tool for the analysis of discrete signals and systems.

- The z-transform of a discrete-time signal $x(n)$ is defined as the power series

$$Z\{x(n)\} = X(z) = \sum_{n=-\infty}^{\infty} x(n) z^{-n}$$

- The above relation is sometimes called the direct z-transform because it transforms the time-domain signal $x(n)$ in to its complex plane representation $X(z)$.

- Where z is a complex variable, in polar form z is expressed as

$$z = re^{j\theta}$$

Where $r = |z|$ and $\theta = \angle z$ and the relation $X(z)$ and $x(n)$ is indicated by

$$x(n) \overset{z}{\leftrightarrow} X(z)$$

- Since the z-transform is an infinite power series, it exists only for those values of z for which the series converges.
- The region of convergence (ROC) of $X(z)$ is the set of all the values of z for which $X(z)$ attains a finite value.
- Thus, for z-transform, we have to mention ROC. We illustrates these concepts by

Dept. of ECE, A I T, Chikkamagaluru
Subject: Digital Communication (21EC51)
Quiz

Semester: 5 **Date: 11 March 2024**
Max Marks: 20 **Time: 10:30 AM – 11:00 AM**

Answer all the questions in one word

1. Minimum distance between the two signal points in QAM constellation is _______.
   a) $2\sqrt{E_0}$ b) $\sqrt{E_0}$ c) $\sqrt{\frac{E_0}{2}}$ d) $4\sqrt{E_0}$

2. Match the following

Digital Modulation Technique	Average Probability of Symbol Error	
a) Binary PSK	1. $\frac{1}{2}e^{-\frac{E_b}{N_0}}$	a - ______
b) Binary FSK	2. $2Q(\sqrt{\frac{2E_b}{N_0}})$	b - ______
c) QPSK	3. $Q(\sqrt{\frac{2E_b}{N_0}})$	c - ______
d) DPSK	4. $Q(\sqrt{\frac{E_b}{N_0}})$	d - ______

3. __________ is the non coherent mode of binary phase shift keying.
   a)QPSK b)DPSK c)QAM d)BFSK

4. The energy of the orthonormal basis functions is ____________
   a) 0 b) Unity c) infinity d) Not defined

5. The correlator consists of ___________
   a) Multiplier, detector b) Integrator, detector c) multiplier, integrator d) Adder, Integrator

6. The matched filter impulse response is matched to __________________
   a) Channel b) basis function c) input signal d) output signal

7. Nyquist condition for zero ISI
   a) x(nT) = 0, n=0 b)x(nT) = 1, n=0 c) x(nT) = 0, n=0, n=1 d) x(nT) = 1, n=1, n=2

8. The maximum likelihood decision rule is to choose the message point which is
   a) Exactly equal to the received signal point, b) closest to the received signal point
   c) independent of received signal point d) All the above

9. In spread spectrum technique, the multiple users are assigned
   a) Same spectrum and same PN code b) Same spectrum and different PN code
   c) Different spectrum and different PN code d) Different spectrum and same PN code

10. The period of a PN sequence produced by a linear m stage shift register cannot exceed ___ symbols.
    a) 2m b) m c) 2^m d) 2^m -1

11. Institute of Electrical and Electronics Engineers (IEEE) 802.11 Direct Sequence Spread Spectrum (DSSS) uses the data rate of
a) 1 or 2 Mbps b) 6 to 54 Mbps c) 5.5 and 11 Mbps d) 2 and 54 Mbps

12. An $(\mathcal{E}_b/I_0)_{\text{dB}}$ = 10 dB is required to achieve reliable communication. What is the processing gain that is necessary to provide an interference margin of 20 dB?
a)1 b)10 c) 100 d) 1000

13. For a sure event, the amount of information is equal to _______
a) 0 b) 1 c) > 1 d) < 1

14. Calculate the entropy of source with a symbol set containing 64 symbols each with a probability 1/64.
a) 64 bits/symbol b) 6 bits/symbol c) 4 bits/symbol d) 1 bit/symbol

15. ____________ is the process by which the output of the information source is converted into a binary sequence.
a) Source encoding b) Source decoding c) Redundancy d) Modulation

16. The transmission errors due to white Gaussian noise are called as ____________
a) Gaussian errors b) Burst errors c) Random Errors d) Linear errors

17. The code in which codewords consists of message bits and parity bits separately is called _______
a) Block Codes b) Systematic Codes c) Non-systematic Codes d) Hamming code

18. For a (6,4) block code where n = 6, k = 4 and d_{min} = 3, how many errors can be corrected by this code?
a) 1 b) 2 c) 3 d) 4

19. In Linear Block code if R=110110 & E=010000, calculate transmitted code
a) 110110 b) 000110 c) 100110 d) 010000

20. While representing the convolutional code by (n,k,m), what does 'm' signify or represent in it?
a) Coded bits b) Message bits c) Memory order d) All of the above

################################

Marks Scored

____

20

NAME of the STUDENT: ________________________________

SEM: 5^{TH} **SEC :**____________

USN: _______________________

Signature of the Faculty

ADICHUNCHANAGIRI INSTITUTE OF TECHNOLOGY

(Affiliated to Visvesvaraya Technological University, Belagavi)
Chikkamagaluru, Karnataka, India-577102

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

Continuous Internal Evaluation: QUIZ

Date: 30 March 2024	Course Title **: CRYPTOGRAPHY (21EC642)**	Marks: 20
Timing : 9 -10 am	Answer ALL the questions	Duration : 1 HOUR

PART A

Each question carries one mark

1. Which of the following is the meaning of crypt?
a. Hidden b. Writing c. Copied d. Both a and b

2. Jim has encrypted his company's confidential files using a secret key. Attacker John tries to decipher those files without knowing the key, what is this process called?
a. Cryptography b. Cryptanalysis c. Decryption d. None of the above

3. Which of the following are the components of crypto system?
a. Plain text b. Cipher text c. Keys d.All of the above

4. Which of the following is the other name of symmentric key cryptography?
a. Private key b. Secret key c. Ideal key d. Both a and b

5. Find an integer x that satisfies the equation 5x ≡ 3 (mod 11).
a. 2 b. 3 c.5 d.1

6. Determine : 11 mod -5.
a. -4 b. -1 c. 1 d.4

7. Given integers a and b, multiplicative inverse exists if and only if gcd(a,b) =
a. a b. 1 c. b d.None

8. Which of the following cipher techniques involves matrix operations in their algorithms of encryption and decryption?
a. Hill Cipher b.Playfair Cipher c. Both a &b d.None of the above

9. With symmetric key algorithms, the ____ key is used for the encryption and decryption of data.
a. Different b. Same c. Both a & b d. None of the above

10. Which of the following is a type of attack on encryption that tries every possible key combination?
a.Brute force attack b.Dictionary attack c.Collision attack d.Rainbow table attack

11. The theorems that play important roles in public-key cryptography are
a. Fermat's theorem b. Euler's theorem c. Euclidean theorem d. Both a &b

12. Using the Euler's totient function, determine $\phi(253)$.
a. 200 b.209 c.220 d.252

13. What are the two keys that are used in asymmetric key cryptography?
a. Secret key and private key b. Private key and public key
c.Public key and secured key d. Secured key and private key

14. Jim and Joe decide to use Diffie-Hellman method. If they are not authenticated to each other, what type of security attack can be expected?
a. Man-in-the-middle attack b. Brute force attack c. Plain text attack d. Cipheronly attack

15. How many rounds does 128 bits in AES requires?
a. 10 b.12 c.14 d.15

16. 128 bits plain text form of AES has __ bytes.
a. 12 b.14 c.16 d.18

17. Amongst which of the following is / are true with reference to the rounds in AES –
a.Byte Substitution b.Shift Row c.Mix Column and Key Addition d.All of the above

18. The full-form of RSA in the RSA encryption technique
a.Round Security Algorithm b. Rivest, Shamir, Adleman
c.Robert, Shamir, Addie d.None of the above

19. Data encryption standard is a block cipher and encrypts data in blocks of size of _____ each.
a. 16 bits b. 64bits c.128 bits d.32 bits

20. The ____________ method provides a one-time session key for two parties.
a. Diffie-Hellman b.RSA c. AES d. DES

PART B
Each question carries two mark

1. Find the gcd(3399, 1563).
   a. 2 b.3 c.5 d.1
2. The value of 3^{51} mod 5 is
   a. 2 b.1 c.3 d.4
3. Find the multiplicative inverse of 13 mod32 using extended Euclidean algorithm.
   a. 6 b.3 c.13 d.5
4. Find the GCD of the polynomials $f(x) = x^2+x+1$ and $g(x) = x^4+x^3+1$
   a. x^2+1 b. $x+1$ c. 1 d.x
5. Construct a Playfair cipher for a key “DIODE” and encrypt the message “semiconductor”.
   a. TOLOFIKERHSESW c. UPLPEKMFQEUNSW
   b. OTOLFIKERHESSW d.TOLOIFEKHRSESW
6. Using the Vigenère cipher, encrypt the word “explanation” using the key *leg*.
   a. AWSDRGYHJIL b.CWETUJBNOLH c.PBVWETLXOZR
7. Decrypt the following cipher text with a key of 3 using Caesar cipher : “L olnh wr zhdu kdwv”.

   a. I like to wear hats b. I love to wear hats

   c. I like to wear band d. I love to wear band
8. Calculate the determinant mod 26 of $\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$
   a. -121 b. 17 c.9 d.4
9. Determine the inverse mod 26 of the matrix $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$
   a. $\begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix}$ b. $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}$ c. $\begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix}$ d. $\begin{bmatrix} 161 & -92 \\ -115 & 9 \end{bmatrix}$

10. Using RSA, if p=13, q=5 and e=7, the value of d and private key are
    a.4, PR(7,48) b.7,PR(7,48) c. 7,PR(7,65) d.4,PR(7,65)

################################

Faculty In charge Name and Signature	DIVYA G S
Student name	
USN	
Semester & Section	6^{TH} A
Marks Scored	20

Name: ______________________________ **USN:**_________________________

ROUGH WORK