

Digital Signal Processing
(3 hours)

Total Marks: 80

- N.B. 1. Question No. 1 is compulsory
2. Attempt any **three** out of remaining
3. Assume suitable data if **necessary** and justify the assumptions
4. Figures to the **right** indicate full marks

- Q1 A Compare microprocessor with digital signal processor. 05
B State whether $x[n] = \cos(3\pi n/4)$ is an energy or power signal with proper justification. 05
C Find the cross correlation of two causal sequences $x[n] = \{2, 3, 1, 4\}$ and $y[n] = 3\delta(n-3) - 2\delta(n) + \delta(n-1) + 4\delta(n-2)$. 05
D State BIBO stability criterion for LTI systems. Test the stability of the LTI systems, whose impulse response is: $h[n] = 0.2^n u[-n] + 3^n u[-n]$. 05
- Q2 A Check whether the system $y[n] = a^n u[n]$ is:
i) Static or Dynamic 10
ii) Linear or Non-linear
iii) Causal or Non-Causal
iv) Shift variant or Shift Invariant
- B Consider analog signal $x(t) = 2 \sin 80\pi t$. If the sampling frequency is 60 Hz, find the sampled version of discrete time signal $x[n]$ also find an alias frequency corresponding to $F_s = 60$ Hz 10
- Q3 A Determine the output response of the LTI system using tabular method, whose input is:
 $x[n] = 1$; $n = 0, 1$
 $= 3$; $n = 2, 3$
 $= 0$; elsewhere
and $h[n] = \delta[n] - 2\delta[n-1] + 3\delta[n-2] - 4\delta[n-3]$. 10
B Compute DFT of sequence $x[n] = \{0, 2, 3, -1\}$. Sketch the magnitude and phase spectrum. 10
- Q4 A Explain the following properties of DFT : 10
i) Periodicity
ii) Linearity
iii) Time Shift
iv) Circular Convolution
v) Time Reversal
B Compute linear convolution of the causal sequences $x[n] = \{4, 4, 3, 3, 2, 2, 1, 1\}$ and $h[n] = \{-1, 1\}$ using overlap save method. 10

[TURN OVER]

- Q5 A In a LTI system the input $x[n] = \{1, 2, 1\}$ and impulse response is $h[n] = \{1, 3\}$. 10
 Determine the response of LTI system using radix- 2 DIT FFT method.
- B Explain Parseval's energy theorem. 10
 If IDFT $\{X(k)\} = x[n] = \{2, 1, 2, 0\}$ using DFT properties, evaluate the following:
- i) IDFT of $\{X(k-1)\}$
 - ii) IDFT of $\{X(k)$ circularly convolved with $X(k)\}$
 - iii) IDFT of $\{X(k).X(k)\}$
 - iv) Signal energy
- Q6 A Explain the significance of Carl's Correlation Coefficient Algorithm in digital signal processing. Evaluate Carl's Coefficient for two causal sequences 10
 $x[n]=\{3, 4, 7, 8\}$ and $y[n]=\{2, 1, 1, 2\}$
- B i) Compare 64 point DFT and FFT systems with respect to the number of complex additions and multiplications required. 5
 ii) Write a detailed note on biomedical applications of DSP processors. 5

Cryptography & System Security.

(Time: 3hrs)

(Marks 80)

1. Question No 1 is compulsory.
2. Attempt any three out of the remaining five questions.

- Q1. (a) Encrypt the message "Cryptography is fun" with a multiplicative cipher with key = 15. Decrypt to get back original plaintext. 05
- (b) With the help of suitable examples compare and contrast monoalphabetic ciphers and polyalphabetic ciphers? 05
- (c) What are the properties of hash functions? What is the role of a hash function in security? 05
- (d) What are the different protocols in SSL? How do the client and server establish an SSL connection 05
- Q2. (a) What is a digital certificate? How does it help to validate the authenticity of a user? Explain the X.509 certificate format. 10
- (b) With reference to DES comment on the following: 10
- i) Block size and key size
 - ii) Need for expansion permutation
 - iii) Avalanche and completeness effects
 - iv) Weak keys and semi-weak keys
 - v) Role of S-box
- Q3. (a) What are the different types of viruses and worms? How do they propagate? 10
- (b) What are the various ways for memory and address protection in Operating System? 10
- Q4. (a) Explain briefly with examples, how the following attacks occur: 10
- i) Phishing attack
 - ii) Denial of Service attack
 - iii) SQL injection attack
 - iv) Cross-site scripting attack
- (b) How is security achieved in the transport and tunnel modes of IPSec? What are security associations? 10
- Q5. (a) What are the different threats to emails? Give an algorithm to secure emails being sent from user A to user B. 10
- (b) A and B wish to use RSA to communicate securely. A chooses public key as (7,119) and B chooses public key as (13,221). Calculate their private keys. A wishes to send message $m=10$ to B. What will be the ciphertext? With what key will A encrypt the message "m" if A needs to authenticate itself to B. 10

Q6. (a) Compare and contrast (any two):

- i) Block and stream ciphers
- ii) MD-5 versus SHA
- iii) Key generation in IDEA and Blowfish

10

(b) What are the different components of an Intrusion Detection System?

10

Compare the working of signature based IDS with anomaly based IDS.

.....