

GUJARAT TECHNOLOGICAL UNIVERSITY
MASTER OF COMPUTER APPLICATIONS (MCA)
Semester: IV

Subject Name: **Programming Skills – VI (FON)**
Subject Code: **640011**

List of Practicals:

- 1) Framing Techniques (Character Count, Byte Stuffing, Bit Stuffing)**
- 2) Error Detection and Correction Techniques (Single Bit Parity, Block Parity, Checksum, CRC Checksum, Hamming Code)**
Students may be asked to simulate different noise scenarios like single bit corruption, multi-bit corruption, etc, and check whether the receiver, using the given error detection/correction technique, is able to detect/correct the error.
- 3) All Data Link Layer Protocols (Protocols 1, 2, 3, 4, 5, 6 as per Main reference Book)**
Protocols 1, 2 and 3 may be asked to be implemented completely. Programs based on protocol 4, 5, and 6 may be asked in a way that a small feature like retransmission timer, or NACK or sliding window to be implemented. Entire protocol programs must not be asked for protocol 4, 5 and 6.
- 4) Cryptography (Without using Java Security/Cryptography Packages)**
Generalized Caesar Cipher, Mono-alphabetic Substitution Cipher, Transposition (Columnar) cipher, P-Box, S-Box, Product Cipher, One Time Pad.

Above programs in item no. 4 should be implemented in Java. For these programs, students need to implement the corresponding algorithms themselves in Java. Communication may be done using sockets. For that Java socket programming is to be used.

- 5) Cryptography (using Java Security/Cryptography Packages)**
Symmetric Block Ciphers:
DES (with ECB, CBC, CFM modes), 3DES (with ECB, CBC, CFM modes), AES ((with ECB, CBC, CFM modes), Stream Cipher implementation of DES, 3DES and AES

Asymmetric Ciphers: RSA

For above programs in item no. 5, cryptography and security related Java packages like java.security, java.security.interfaces, java.security.spec, etc. should be used. Students are NOT required to implement the actual logic of the cryptographic algorithm. Instead, the available security package API should be used. Communication may be done using sockets. For that Java socket programming is to be used.

Some important instructions regarding item nos. 1, 2 and 3 in the above practical list are as under:

1. These programs are intended to simulate various aspects of the functionality of LLC sub-layer protocols like flow control, error control and various ARQ. These programs have to be implemented in GNU C under Linux Platform.
2. Two separate programs namely Sender and Receiver have to be created. Both the programs communicate using the IPC mechanism FIFO or Named Pipes in Linux. The no. of named pipes required depends on the nature of the application.
3. **Bitwise operators should be used wherever applicable.** For ex; to corrupt particular bit/s in error detection /correction programs.
4. Various system calls like read(), write(), open(), delay(), etc, may be used.

Note: - The above programs will form the essential part of the term-work for this subject. Apart from above programs, presentation/seminar/ report on emerging concepts/trends in the field of computer networking may be given to students as additional term-work activity. One may prefer to use end of chapter questions as exercises to be solved as well.

Reference Books for Practical:

1. W. Richard Stevens, “Advanced Programming in Unix Environment”, Pearson Education Publications ,Second Edition (to study how system calls can be used)
2. Vijay Mukhi, “C Odyssey: Unix the open Boundless C”, BPB Publications, Paperback Edition (1992) (for learning how to read and write data using named pipes)
3. David Hook, “Beginning Cryptography with Java”, Wrox/ Wiley-Dreamtech Publications, Special Indian Edition (2005)
4. Jonathan Knudsen, “ Java Cryptography”, O’Reilly Publishers, First Edition (1998)

Accomplishments of the student after completing the Course:

1. Understand and use the process of protocols and other techniques using Java & ‘C’ under Linux environment
2. Analyze and develop protocol/algorithm to solve real problems
3. Able to implement various protocols, Framing Techniques, Error detection and correction techniques, cryptography algorithms
4. Understand working of each layer of OSI and TCP/IP Model