MMTE-006: Cryptography

Session 1: (Uses C language)

Program 1:

Write a C program that reads a text file, and writes a text file in which

1) all the punctuation marks and other characters are removed.

2) all the letters converted to capitals

3) the output grouped in blocks of five.

Programme 2: Write a C program that encrypts(and therefore decrypts) text using an affine cipher. It should prompt for the values of a and b and use the values to encrypt/decrypt from the text in a file. It should give an error message if a is not co-prime to 26.

Programme3: Write a C program that prints all the 26 shifts if the input text.

Session 2: (Uses C language)

Program 1: Write a C program that reads from file, encrypts or decrypts the text using Vigenere cipher and writes the output to another output file specified.

Program 2: Write a program that reads a text file in which all the punctuation characters are removed and all the characters are in upper case and gives the frequency of each of the 26 characters.

Session 3: (Uses GP)

Introduction to GP.

Session 4: (Uses GP)

Intrduction to programming in GP and implementation affine and Vigenere ciphers using GP.

Session 5: (Uses GP)

Write programs in GP for the following:

1) Miller-Rabin test.

2) Finding a random irreducible polynomial of degree 20 over $\boldsymbol{Z_7}$.

3) AKS algorithm for testing primality.

Session 6: (Uses C language) Write a function in `C' that emulates an LFSR.

Session 7: (Uses GP) RSA cryptosystem using GP: Generating random primes, conversion from text to numbers and vice versa, encryption and decryption using GP

Session 8: (Uses GP) Fermat factorisation algorithm and Pohlig Hellman algorithm using GP.