Lab Assignment – 2 (20 Marks)

Execute the following Socket programs using gmp library in C or Python.

Note: Do not use predefined functions from any Library or Header file, as far as possible. Implement algorithm by your own using library functions for algorithm steps only.

Sno.	(Refer Class notes or prescribed text books)
	Symmetric Encryption (5 Marks)
Z)	Implement 2-round Feistel cipher. Suitably, choose your own function f, such that f uses your roll no last two digits in its computation. (2.5 M)
	Implement the following mode of operation for DES. Use predefined DES code. Choose suitable IV value. (2.5M)
A)	Cipher block chaining (CBC)
B)	Cipher Feedback (CFB)
C)	Output Feedback (OFB)
D)	Counter (CTR)
	Asymmetric Cryptosystem (5 Marks) **(wherever required use any suitable predefined Hash code)**
A)	OAEP construction of RSA
B)	ElGamal PKE
C)	Schnorr Signature scheme
D)	Digital Signature Standard (DSS)
	Entity Authentication (Zero Knowledge protocols) (5 Marks)
A) B)	Fiat – Shamir Protocol
C) D)	Guillou – Quisquater protocol
	Key Management (Session key distribution protocols) (5 Marks)
A) B)	Needham – Schroeder Protocol
C) D)	Otway-Rees Protocol

Programs to do:

Program Z) to be done by all.

Program A) for the students whose Rollno digit give 1 as remainder when divide it by 4.

Program B) gives 2 as remainder when divide rollno digits by 4.

Program C) whose remainder comes out to be 3.

Program D) rollno exactly divisible by 4.

i.e. if rollno is BT18CSE002 programs are – Z, SE – B, AC – B, EA – B, KM - B

Naming Convention:

Name the program as **<rollno>_<Abbreviation>_<Alphabet>_<Entity>.c or py**, where **Abbreviation** as follows, Symmetric Encryption – **SE**, Asymmetric Cryptosystem – **AC**, Entity Authentication – **EA** and Key Management (**KM**), and **Entity** can be Encryptor (**En**), Decryptor (**De**), KeyGeneration (**Kg**), Signer (**Sg**), Verifier (**Vf**), Alice (**A**), Bob (**B)**, KDC (**Kdc**).

e.g. OAEP construction of RSA programs name will be (if rollno is BT18CSE001 then) BT18CSE001_AC_A_Kg.c, BT18CSE001_AC_A_En.c and BT18CSE001_AC_A_De.c

similarly for Fiat-Shamir programs will be - BT18CSE002_AC_B_Kg.c,

INPUT to programs:

All input to the program can be through command line arguments or from some input text file. For example, for BT18CSE002_AC_A_Kg.c say its executable file name is BT18CSE002_AC_A_Kg then we test as,

$ BT18CSE002_AC_A_Kg 512 <enter>

Where $ is command prompt, 512 is input. Or store input in some Input.txt file and extract input from it.

OUTPUT of the program:

And print exact output with self-explanatory sentences (precisely). Or print your output into some text file say BT18CSE002_AC_A_Kg_output.txt

NETWORK Programming:
All programs except Key generation code should use socket programming.

Execution Convention by you:

Give the documentation of execution process used by you in separate single pdf. Can add screenshots of execution in it.

Plagiarism / Similarity percentage:

We also do plagiarism test of your programs, if similarity percentage of a program is higher than 60% then marks may be deducted.

Code Explanation Recording:

Do the minimum 2 minutes to 5 minutes recording of explaining your written code and only important steps for the **AC and KM programs**, in single video. In the video, your face needs to be visible for atleast 10sec while speaking (initially) and then show the code lines with sample small inputs and output, while explaining it.

Combined Recording should not be more than 5minutes.

*Without Recording, AC and KM programs marks will not be given.