Assignment # 1

Due Date: 27 – 01 – 12

The equation of the elliptic curve over a binary field, $F(2^m)$, is

$$y^2 + xy = x^3 + ax^2 + b$$

Write a program that does the following

- Inputs the value of m and the irreducible polynomial from the user
- Lists the generators of the multiplicative group of the binary field
- Accepts user input which specifies which of the generators should be designated g
- Inputs two integers i and j – from these a and b are respectively computed as g^i and g^j
- Lists the number of points on the EC and their coordinates
- Identifies the number of generators of the group of points on the EC and their coordinates
- Accepts user input which specifies which of the above generators should be selected
- Expresses each point as a scalar multiple of the selected generator.

This is a group assignment. All members of the group are required to ACTIVELY DISCUSS and PARTICIPATE in it.