COM 5336 ASSIGNMENT #4

DUE BY 11:59PM 5/16/2017 (Tue)

10% penalty applies to 1-day late submissions received between 0:00 AM 5/17 and 11:59PM 5/17.
No submission will be accepted after 0:00 AM 5/18/2017

Objective

Implement the General Elliptic Curve Group over prime fields GF(p) and use it to implement the EC-ElGamal cryptosystem.

Description

General elliptic curve group over a prime field GF(p) can be specified as E: $y^2=x^3+ax+b$ with point G. Let n=ord(G). The general elliptic curve group can be uniquely determined by the quintuple (p,a,b,G,n). In this assignment, we fix the following parameters.

```
p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFF
a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 7FFFFFFC
b = 1C97BEFC 54BD7A8B 65ACF89F 81D4D4AD C565FA45
Gx = 4A96B568 8EF57328 46646989 68C38BB9 13CBFC82
Gy = 23A62855 3168947D 59DCC912 04235137 7AC5FB32
n = 01000000 00000000 000001F4 C8F927AE D3CA7522 57
```

The objective of this assignment is to implement EC-ElGamal. Note that you need to represent the plaintext as a point on the curve and there is no guarantee that, given any x-coordinate, you can always find a y (as a solution) such that (x,y) is on the curve. This can be achieved by using **8 don't-care bits in the x-coordinate**, as shown in the Data Embedding Method below.

```
<Data Embedding Method>
Input: (m-8)-bit binary data M
Output: Point (Mx,My) on the elliptic curve
Mx = append(d,00)
while (Mx not on curve)
   increment Mx
compute y (s.t. y%2 == 1)
return (Mx,My)
```

You should look at the following two documents. www.secg.org/collateral/sec1_final.pdf and www.secg.org/collateral/sec2_final.pdf. Look at section 2.3 in sec1_final.pdf to see how point at infinity is represented and how point compression is done. Look at sec2_final.pdf for parameter samples.

3 Test Cases (Input shown in bold face)

```
<EC-ElGamal encryption>
Plaintext M = 2923BE84 E16CD6AE 529049F1 F1BBE9EB B3A6DB
Pa = 03 9994C5C1 6070EE87 8F89A614 3CE865AC 2EC7EC5D
nk = A61F035A 7D093825 1F5DD4CB FC96F545 3B130D89
Mx = 2923BE84 E16CD6AE 529049F1 F1BBE9EB B3A6DB01
My = A38CC9D2 3D61B446 A4F51B2C 8DA6BC6F C5CA2BAC
Cm = {Pk,Pb} = { 3D5A5C8A 80799494 624E741A 0119804F F707A2AB
, 3C83F7C5 2185D5AC BE561718 80995F59 1DFE5C3C }

<EC-ElGamal decryption>
Pk = 02 3D5A5C8A 80799494 624E741A 0119804F F707A2AB
Pb = 02 3C83F7C5 2185D5AC BE561718 80995F59 1DFE5C3C
na = 3C870C3E 99245E0D 1C06B747 DEB3124D C843BB8B
Plaintext = 2923BE84 E16CD6AE 529049F1 F1BBE9EB B3A6DB
```

```
<EC-ElGamal encryption>
Plaintext M = 110BA66C C954BE96 3A7831D9 D9A3D1D3 9B8EC3
Pa = 02 7AB13D6D 69847A9C CE9A84E5 DB1BDDD8 7F11F38C
nk = 8E07EB42 65F1200D 0745BCB3 E47EDD2D 23FBF571
Mx = 110BA66C C954BE96 3A7831D9 D9A3D1D3 9B8EC301
My = F4CBB301 B518D7D4 67E542D0 40AC6029 F7833135
Cm = {Pk,Pb} = {7AF4ED0D 220D9482 424E72FE 5A375C6B FC2B0743
, 015A7D66 7CDA436F 401E6156 9109D753 ECD1F0B1 }

<EC-ElGamal decryption>
Pk = 02 7AF4ED0D 220D9482 424E72FE 5A375C6B FC2B0743
Pb = 03 015A7D66 7CDA436F 401E6156 9109D753 ECD1F0B1
na = 246FF426 810C46F5 04EE9F2F C69BFA35 B02BA373
Plaintext = 110BA66C C954BE96 3A7831D9 D9A3D1D3 9B8EC3
```

```
<EC-ElGamal encryption>
Plaintext M = E1DB763C 99248E66 0A4801A9 A973A1A3 6B5E93
Pa = 03 7E3966DF 631F4871 3E61F0B7 0E1B5F77 C8A5B41B
nk = 5ED7BB12 35C1F0DD D7158C83 B44EADFD F3CBC541
Mx = E1DB763C 99248E66 0A4801A9 A973A1A3 6B5E9302
My = 7E4AB41E 02090D89 7192EAE4 960E6A4E F1CFAF27
Cm = {Pk,Pb} = { 782C00A6 44071320 B2E424C4 05AFF3CE 68387585
, 2F35CEA2 0391E5DA AD0E63FF 64A0947E 9F13A568 }

<EC-ElGamal decryption>
Pk = 03 782C00A6 44071320 B2E424C4 05AFF3CE 68387585
Pb = 03 2F35CEA2 0391E5DA AD0E63FF 64A0947E 9F13A568
na = F43FC4F6 51DC16C5 D4BE6FFF 966BCA05 80FB7343
Plaintext = E1DB763C 99248E66 0A4801A9 A973A1A3 6B5E93
```

Grading

Your program MUST BE compatible with Dev C/C++ or GNU C/C++ compilers. If you are using other compilers, please make sure your final program is compatible. **You will get no points if your program is not compilable using the abovementioned compilers.** If your program is compilable but the result is not completely correct, you'll still get partial credits. Your program should be well-commented, well-structured, and easy to understand. You may lose up to 30% of points if you fail to do so.

Submission

Put all your source codes in a folder containing main functions, function implementations, class definitions, or compilation instructions (if any). Compress them as a single zip file. DO NOT submit executable files. Name your zip file as your student ID number (i.e. 100012345.zip). Submit your source code on iLMS at http://lms.nthu.edu.tw.