These projects are produced by Dr. Xunhua Wang. If you are taking his course, you can make a *single* machine-readable copy and print a *single* copy of each page for your own reference, so long as the pages contain this copyright statement. Permission for any other use must be obtained from the author (wangxx@jmu.edu) in writing.

Project 3

Diffie-Hellman, ElGamal, and Elliptic-curve Cryptosystem

3.1 Introduction

In classroom, we have discussed Diffie-Hellman key exchange protocol, the ElGamal public-key encryption scheme and the Elliptic-curve cryptosystem (ECC). This project is about these schemes.

Note: all numbers prefixed with $0x$ are hexadecimal; other numbers are decimal. Except the numbers for the "by hand" part, **the numbers in your answer must be hexadecimal!**
(Try java.math.BigInteger.toString(16).)

For your convenience, some of the big numbers for this project can be found at
https://users.cs.jmu.edu/wangxx/web/tools/code/dhelgamalecc-bignumbers.txt

3.2 Tasks

The tasks comprise four parts.

3.2.1 Questions by hand (23 points)

The following questions must be answered by hand, unless specified otherwise. **For by-hand calculations, you may use help from a calculator, such as the Scientific Calculator on MS Windows and an online calculator.** To earn any points, you must give sufficient (but not excessive) details. Results without any intermediate steps will lead to zero points.

1. (4 points) Find **all** *primitive roots* (i.e., *generators*) of mod25. (Please note that 25 is *not* a prime number and the set in question thus only contains those numbers that are co-prime to 25.)

   You can find the definition of primitive root in our textbook. **For this task, you can develop a small computer program.**

2. (3 points) Consider a Diffie-Hellman scheme with a common prime $q = 11$ and a primitive root $g = 2$

   (a) Prove that $g = 2$ is a primitive root of 11

   (b) If user A has public key/value $Y_A = 9$, what is A's private key/value X_A?

   (c) If user B has public key/value $Y_B = 3$, what is the secret key/value K shared with A?

3. (4 points) Consider an ElGamal scheme with a common prime $q = 71$ and a primitive root $g = 7$.

   (a) If Bob has public key $Y_B = 3$ and to send Bob an encrypted message, Alice chose the random integer $k = 2$, what is the ciphertext of $m = 30$?

   (b) If Alice now chooses a different value of k so that the encoding of $m = 30$ is $C = (59, C_2)$, what is the integer C_2?

4. (12 points) Consider the following Elliptic-Curve cryptosystem: $y^2 = x^3 + 9x + 17$ mod 23 (that is $a = 9, b = 17, p = 23$), base point G $= (16, 5)$.

   (a) (3 points) If Alice's private key is $P_A = 10$ (in some books this private key may be denoted as n_A), what is her public key U_A? You must give enough details how you get the result.

   (b) (3 points) Bob gets a copy of Alice's public key U_A and he needs to encrypt a message $m = 3$ and send the ciphertext to Alice. To that end, Bob needs to map m to an ECC point P_m first. Using the method described in the slides (with two padding bits), what will P_m be for $m = 3$?

   (c) (3 points) In the encryption, if Bob picks a random value $k = 2$, what is the ciphertext C for $m = 3$?

   (d) (3 points) After receiving ciphertext C, how will Alice decrypt it? You must give detailed steps **and concrete numbers**.

3.2.2 Diffie-Hellman (10 points)

Let $p = 0x$FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A6
7CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374
FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386B
FB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55

D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670
C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC
07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA05101
5728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA
71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261
AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6
C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723
C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD
44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3
A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B
4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFF

1. (1 point) Is p a prime?
2. (2 points) Is $g_1 = 2$ a generator of finite field F_p^*? Why? (Hint: check whether $q = \frac{p-1}{2}$ is a prime or not; note that the order of an element must be a divisor of $(p-1)$. **Please study the slides to find the right checking algorithm.**)
3. (2 points) Is $g_2 = 22$ a generator of finite field F_p^*? Why?
4. (5 points) Assume that Alice and Bob share public parameters (g_1, p) (yes, it is g_1, not g_2) and they want to use the Diffie-Hellman key exchange protocol with these parameters to establish a common session key. If Alice's and Bob's private values are $a = 0x954637821$ (a hex value!) and $b = 107965234$ (a decimal value!) respectively, what will their common session key k be? A concrete number is needed. You (or your code) must also give Alice's **and** Bob's detailed steps to calculate k and the final value of k.

3.2.3 ElGamal encryption (10 points)

$p = 0x$FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67C
C74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE
1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB
5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D3
9A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C3
54E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07
A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA0510157
28E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA7
1575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261A
D2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C
770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFF
FFFFFFFFFFFF

1. (1 point) Is p a prime?
2. (2 points) Is $g_1 = 2$ a generator of F_p^*? Why? (Hint: check whether $q = \frac{p-1}{2}$ is a prime or not; note that the order of an element must be a divisor of $(p-1)$. **Please study**

the slides to find the right checking algorithm.)

3. (2 points) Is $g_2 = 31$ a generator of F_p^*? Why?

4. (5 points) Let (p, g_2) (yes, it is g_2, not g_1) be the public parameters for the ElGamal public-key encryption scheme.

   (a) (1 point) If Alice's private key is $a = 0xf9e8d7c6b5a43210$, what is her ElGamal public key?

   (b) (2 points) Bob has a copy of Alice's public key and he wants to use it to encrypt message $m = 10$. Assuming that a random value $k = 0x1234567890$ is used for ElGamal encryption, what will the ciphertext be?

   (c) (2 points) After receiving the ciphertext, how will Alice decrypt it? Detailed steps **and concrete numbers (by your program)** are required.

3.2.4 Elliptic-curve cryptosystem (20 points)

Consider the following P-384 elliptic curve: $y^2 = x^3 + ax + b \bmod p$, where $a = -3$, $b = 0xb3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef$, $p = 39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319$ (b is in hex while p is decimal).

With base point $G = (0xaa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7, 0x3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f)$, the curve has 3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3 points.

1. (5 points) If Alice's private key is $a = 0xf9e8d7c6b5a43210$, what is her ECC public key?

2. (10 points) Bob has a copy of Alice's public key and he wants to use it to encrypt message $m = 12$. Assuming that a random value $k = 0x1234567890$ is used for ECC encryption, what will the ciphertext be?

   (a) (5 points) Map m to an ECC point. Use a 20-bit padding in the mapping.

   (b) (5 points) Find the corresponding ciphertext

3. (5 points) After receiving the ciphertext, how will Alice decrypt it? Detailed steps **and concrete numbers (by your program)** are required.

3.3 Submission requirements

1. Your final submission must consist of your code and a separate report. The report should include the concrete results, in which **all integers must be in hexadecimal format.** Decimal numbers are considered wrong.
2. Screen shots showing your answers must be included in your report.