UNIVERSITY of LIMERICK

OLLSCOIL LUIMNIGH

Department of Mathematics and Statistics
Faculty of Science and Engineering

END OF SEMESTER ASSESSMENT PAPER

MODULE CODE: MA6011

SEMESTER: Autumn 2016

MODULE TITLE: Cryptographic Mathematics

DURATION OF EXAMINATION: 2 1/2 hours

LECTURER: Dr. Eberhard Mayerhofer

PERCENTAGE OF TOTAL MARKS: 70%

EXTERNAL EXAMINER: Prof. J. King

INSTRUCTIONS TO CANDIDATES:

- Answer **one** of the two questions **in Section A**.
- Answer **three** out of the four questions in **Section B**.
- At the end of the exam, please send the Sage file with solutions of section B to me (**eberhard.mayerhofer@gmail.com**).

WARNING: THIS SAMPLE IS A MINI EXAM, where I give only two choices in B, and 1 choice in A.

Section A

marks

Q.1 Recall the ElGamal Cryptosystem: Let p be a large prime, and g a primitive root modulo p. Alice typically chooses a number k and calculates

$$a = g^k \mod p$$

and publishes this a as her public key. So p, g, a are public. k is private to Alice.

Now imagine, Alice' big sister Bigalice knows about elliptic curves and therefore wants to imitate this system using elliptic curve operations, rather than operations modulo p. Complete the following steps to get this adapted cryptosystem.

- A prime p is known, and an elliptic curve $E : y^2 = x^3 + bx + c$ modulo p. Let G (taking the role of g above) be a point on E that generates the curve, that is, the points
$$G, 2G, 3G, \dots, (N-1)G, N_pG = O_E,$$
where the last point is the point at infinity, and G thus generates all all $\mathbb{F}_p$ points (the total number of points is N_p). **Bigalice picks a positive number k and computes $A = kG$.** Hence p, E, and G and one more object (**which?**) are public keys. **What is the private key here?**
- Bob's older brother Bigbob now wishes to send a message to Bigalice, using her public keys. He first identifies $m \in (0, N_p - 1)$, the message, by a point P_m on E, by setting
$$m = x \quad \text{coordinate of} \quad P_m$$
and computes the y coordinate of P_m as well (how?). [1]
- How would Bigbob encrypt this message m (via P_m?), using the elliptic curve, thus getting two points E_1, E_2 that he sends to Bigalice[2]. Hint: Translate multiplication modulo p (like bl) to addition of points (like $B + L$), and exponentiation modulo p (e.g. g^k) into multiples of points (e.g. kG).
- How can the message be decrypted by Bigalice? Why is it easier than within the original ElGamal system?

[1] In general, any message, decrypted or not, will be now identified as the x coordinate of a point on the elliptic curve. One computes with using elliptic point operations, but in the end may disregard the y coordinate, as only the x-coordinate contains information.

[2] instead of e_1, e_2 in the normal ElGamal system

Section B

Q.1 Number theory essentials.

(a) (pen and paper exercise) What is a primitive root (explain in one or two sentences). Then, find all primitive roots modulo $p = 3$. Finally, find all primitive roots modulo $p = 5$.

(b) (Sage) For large primes p, it is a difficult task to get primitive roots from scratch. However, primitive roots modulo p can be found using Sage and the routine "primitive_ root(p).". Take $p = 31$, determine with Sage the smallest primitive root modulo p, and call this number g. Then create a table of indices modulo p.

(c) For any prime p, how many different elliptic curves in Weierstrass form exist modulo p? (Hint: think of how many different coefficients modulo p you can have).

(d) Let $p = 31$, and take the elliptic curve

$$E : y^2 \equiv x^3 - 1$$

modulo p.

(i) Define this curve with Sage.

(ii) The number N_p of $\mathbb{F}_p$ points on the elliptic curve can be found with the function order(E). Determine this number!

(iii) The function E.random_ point() creates randomly a point on the curve. Denote this point P. Then calculate

$$P, \qquad 2*P, \qquad 3*P, \ldots$$

until you reach O_E, the point at infinity. Call the number of points generated this way by n. Does n divide N_p?

Warning: Every time you run the code, a new point may be generated, as it is a random one. Please make sure you freeze the generated point after generation, as otherwise your solution may conflict the results obtained when I run your code

Q.2 The RSA cryptosystem.

(a) Part I: Use Fermat factorisation to break the following RSA keys $m = pq$,

- 2442953
- 733103

Determine also for each number, the fraction

$$L/m$$

where L is number of attempts in the Fermat factorisation.Disregarding the length of digits of m, which m from the above are good choices, and why? Try to relate your answer to the figure L/m.

(b) Part Ib: One of two numbers m took longer to factorize. Apply Pollard's $p-1$ method to this number, and describe your choice of B in that method.

(c) Part II: Does Fermat factorisation work for numbers m which have more than two prime factors? (You may include a sage example, to explain your answer).

(d) Part III: Explain an RSA cryptosystem where 3 or more prime factors $p_1, \ldots, p_n$ are used for the public key $m = p_1, \ldots, p_n$. How would encryption work?How would decryption work?