Semester II Examinations 2013/2014

Exam Code(s)	3BA1,4BCS1, 1OA1,1EM1, 1MF1/3BME1,3BMS2,4BME1,4BS3,4BS4
Exam(s)	3rd & 4th Arts, Overseas, Masters of Software Design & Development 4th Science, 3rd, 4th Maths & Education 3rd Mathematical Science
Module(s)	**Cryptography**
Module Code(s)	MA492, MA545 and CS402
Paper No	1
Repeat Paper	NO
External Examiner(s)	Dr. C. Campbell
Internal Examiners	Prof. Dr. G. Pfeiffer, Dr. A. Rahm (Course Co-ordinator)
Instructions:	**Answer all four questions.** Do not use red ink or red pencils.
Duration	**2 Hours**
No. of Pages	4 pages (incl. cover page) - 4 questions
Disciplines	Mathematics
Requirements:	
Release to Library:	Yes
Statistical Tables/ Log Tables:	Optional
Other Materials	non-programmable calculators permitted

Recalls from the lectures.

For characteristic of $\mathbb{F}_q$ not 2 or 3, the polynomial $x^3 + ax + b$ has multiple zeroes in $\mathbb{F}_q$ if and only if $4a^3 + 27b^2 \equiv 0$ in $\mathbb{F}_q$. Addition formulas for points on elliptic curves are provided on the last page.

1. Imagine you are working in the headquarters of a bank, and have to transmit an urgent message to the Chief Executive Officer (CEO). On your emailed question "Where are you?", your CEO requests you to use classical Diffie–Hellmann key exchange, in order to preserve the confidentiality of the communication. Use the following alphabet over $\mathbb{Z}/47\mathbb{Z}$:

_	A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z	.	?	'
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

0	1	2	3	4	5	6	7	8	9	#	!	$	%	&
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

;	:
45	46

   (a) Fix $g = 5$ as a generator of $(\mathbb{Z}/47\mathbb{Z})^*$. Choose your private secret key to be $sk_A = 6$. Compute your public key $g^{sk_A} \mod 47$.

   (b) You receive the public key 31 from your CEO. Compute the common secret key.

   (c) Which of the elements $23, 24, 25, 26$ of $(\mathbb{Z}/47\mathbb{Z})^*$ is the decryption key matching the common secret key?

   (d) Decrypt the secret message

   P0ZJ

   where the 0 is a zero and shall not be confused with the letter O.

   (e) Use the common secret key and your own public key to find out if your CEO's private secret key is 2, 3, or 5.

2. Upon your question "IN_WHICH_RESOURCE_SHALL_WE_INVEST?", your CEO considers that the encryption used above was not secure enough given the confidentiality of the communication, and so he decides to switch to classical RSA encryption for his answer.

   So the answer that you receive back, is encrypted with the public key of the bank headquarters, (modulus $N = 55$, encryption key $e = 27$). You have access to the prime factors of N, namely $p = 5$ and $q = 11$. Compute the Euler totient $\phi(N)$.
   In the safe drawer, you find three secret keys: 7, 5 and 3.

   Which is the one that fits the public key of the bank headquarters?

   Use it to decrypt the message from your CEO,

   Erq

   Use the following alphabet:

_	A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	P	Q	R	S	T	U	V	W	X	Y	Z	.	?	’
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
	p	q	r	s	t	u	v	w	x	y				
	45	46	47	48	49	50	51	52	53	54				

3. (a) Check that the equation $y^2 = x^3 + 3x + 2$ defines an elliptic curve over $\mathbb{F}_5$.

   (b) Compute the set of all points on the curve specified in Paragraph (a).

   (c) Find the order of at least one point computed in Paragraph (b). That point shall not itself be the horizon.
   Please turn over.

Question 3, continued.

(d) Using your insights from Paragraphs (b) and (c), and computing the orders of more points if necessary, determine the group structure of the elliptic curve defined in Paragraph (a).

4. Suppose that you want to establish a secure communication channel with Bob, based on an elliptic curve variant of the Diffie–Hellmann key exchange. Choose the prime number $p := 37$, the parameter $a := 1$ and the point $(x, y) := (1, 1)$.

   (a) Find an equation $y^2 = x^3 + ax + b$ over $\mathbb{F}_{37}$ with $a = 1$ such that $(1, 1)$ is a solution. Check that this gives you an elliptic curve.

   (b) Pick $s := 3$ as your secret number. Compute your public key: The point $pk_A := s \cdot (1, 1)$ on the elliptic curve. Check that it lies on the elliptic curve before you send the coordinates to Bob.

   (c) Bob sends you his public key: The point $(13, -10)$. Multiply it with your secret number s and obtain the coordinates constituting the common secret key of you and Bob. Check that the coordinates lie on the elliptic curve.

Addition formulas for elliptic curves $y^2 = x^3 + ax + b$ of characteristic not 2 or 3:

- Adding $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ with $x_1 \neq x_2$: $P + Q = (x_3, y_3)$,

$$\text{where } x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

  and $y_3 = -y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3)$.

- Adding $P = (x_1, y_1)$ to itself : $2P = (x_3, y_3)$,

$$\text{where } x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

  and $y_3 = -y_1 + \frac{3x_1^2 + a}{2y_1}(x_1 - x_3)$.