Main Examination period 2019

MTH6115: Cryptography

Duration: 2 hours

Apart from this page, you are not permitted to read the contents of this question paper until instructed to do so by an invigilator.

You should attempt ALL questions. Marks available are shown next to the questions.

Calculators are not permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.

Complete all rough work in the answer book and cross through any work that is not to be assessed.

Possession of unauthorised material at any time when under examination conditions is an assessment offence and can lead to expulsion from QMUL. Check now to ensure you do not have any unauthorised notes, mobile phones, smartwatches or unauthorised electronic devices on your person. If you do, raise your hand and give them to an invigilator immediately.

It is also an offence to have any writing of any kind on your person, including on your body. If you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms, it will be treated as being found in your possession. Unauthorised material found on your mobile phone or other electronic device will be considered the same as being in possession of paper notes. A mobile phone that causes a disruption in the exam is also an assessment offence.

Exam papers must not be removed from the examination room.

Examiners: J. N. Bray and S. Lester

We use the correspondence between the English alphabet and integers modulo 26 given by $\mathtt{A} \leftrightarrow 0, \mathtt{B} \leftrightarrow 1, \ldots, \mathtt{Z} \leftrightarrow 25$. This is given in full in the table below.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

For full marks, you will have to show all working.

Question 1. [22 marks]

(a) Describe the Cæsar shift and Vigenère cipher, either as applied to the English alphabet or to $\mathbb{Z}_n$, the integers modulo n. [**5**]

(b) In an encryption competition called Cipher Challenge you are permitted to use one of the following two methods to encrypt your message: (i) a combination of at most 3 Vigenères with each key length at most 6, or (ii) a combination of at most 2 Vigenères with each key length at most 9. Which method will you use? Justify your answer. [**5**]

(c) The following ciphertext has been encrypted using a Vigenère key of length 3.

`AHTZ IDYA EOEC LADF`

Decrypt it, given that the plaintext commences `thi`. [**8**]

(d) The Hebrew alphabet contains 22 letters. How many affine ciphers are there for this alphabet? Justify your answer. [**4**]

Question 2. [14 marks]

(a) Define what an **orthogonal array** of degree k and strength t over an alphabet $\mathscr{A}$ of size q is. [**4**]

(b) Describe the correspondence between orthogonal arrays of degree 3 and strength 2 over $\mathscr{A}$ and Latin squares with rows and columns labelled by $\mathscr{A}$. (You do not have to say what a Latin square is, but you should state the correspondence both ways round.) [**4**]

(c) The following is an orthogonal array with some entries missing.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 3 & 1 & & & & 2 & & & 1 & 0 & & & & & \end{pmatrix}$$

Write down the Latin square corresponding to the above orthogonal array, including filling in the blanks. (Order the row and column labels $0, 1, 2, 3$.) [**6**]

Question 3. [40 marks] Let n be a positive integer.

(a) Define the **Carmichael function** $\lambda(n)$ and the **Euler function** $\phi(n)$. **[6]**

(b) Determine how many positive integers there are that are less than and coprime to 30000. Find $\lambda(30000)$. **[6]**

(c) Prove, for all $n \in \mathbb{Z}^+$, that $a^{\phi(n)} \equiv 1 \pmod{n}$ whenever a is coprime to n. **[8]**

(d) Explain briefly the operation of the RSA cryptosystem. If Eve intercepts an RSA communication, which "hard" problems does she have to solve in order to break the cipher? **[8]**

(e) You are given that $N = 1147$ is the product of two (odd) primes and that $\lambda(N) = 180$. Use this information to factor N. (The marks are for the method, not the factorisation.) **[4]**

(f) Let p be a prime, and let x be an integer such that $p \nmid x$. Define the **(multiplicative) order** of x modulo p. **[3]**

(g) Determine the order of 3 modulo 31. **[5]**

Question 4. [24 marks]

(a) Define an **n-bit shift register**, and give the $\mathbb{Z}_2$-polynomial corresponding to such a shift register. Explain what it means for an n-bit shift register to be **primitive**. **[7]**

(b) You intercept the following bit string:

10111 11001 01001 10001 10101 01010 11100 11010 01010.

You have reason to believe that the message was converted into a bit string using the International Teleprinter Code, and then encrypted using a keystring derived from a 5-bit shift register. You have reason to believe that the message commences `MI`. Decrypt the message (assuming that this is the case).

The International Teleprinter Code is given in the appendix at the end of the paper. **[10]**

(c) The first 40 bits of a 5-bit shift register (not the one used above) are

10000 10110 10100 01110 11111 00100 11000 01011.

Is this shift register primitive? Justify your answer. **[2]**

(d) Let f be the polynomial corresponding to the shift register in the previous part. (We have $f(x) = x^5 + x^3 + x^2 + x + 1$.) Is f irreducible (over $\mathbb{Z}_2$)? Justify your answer. **[3]**

(e) Is the keystring in Part (c) suitable for use as a one-time-pad? Very briefly explain your answer. **[2]**

End of Paper – An appendix of 1 page follows.

A	11000
B	10011
C	01110
D	10010
E	10000
F	10110
G	01011
H	00101
I	01100
J	11010
K	11110
L	01001
M	00111
N	00110
O	00011
P	01101
Q	11101
R	01010
S	10100
T	00001
U	11100
V	01111
W	11001
X	10111
Y	10101
Z	10001
Letters	11111
Figures	11011
Line feed	01000
Carriage return	00010
Word space	00100
All space	00000

Table 1: International Teleprinter Code

End of Appendix.