Queen Mary
University of London

Main Examination period 2018

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.

Only non-programmable calculators that have been approved from the college list of non-programmable calculators are permitted in this examination. Please state on your answer book the name and type of machine used.

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 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 shall 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: W.H.Mannan, B. Noohi

All keys, plaintext and ciphertext will be given in SMALL CAPS, without quotation marks. We use the standard conversion:

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

When working modulo n, $T_r(u)$ will denote $u^r \in \mathbb{Z}/n\mathbb{Z}$.

For full marks show all working.

Question 1. [**20 marks**]

(a) Encrypt the word CAN using the affine cipher: $f(x) \equiv 5x - 3 \mod 26$. [**4**]

(b) Alice uses the encryption function $g(x) \equiv 4x - 8 \mod 26$ to communicate with Bob (so he knows that she uses g as her encryption function). Alice requests Bob to bring her a can, encrypting the word CAN with the encryption function g.

What might he bring her instead of a can and what feature of the function g would have created this confusion? [**6**]

(c) The affine cipher $h(x) \equiv 509x - 83 \mod 1023$ is used to encrypt a message. Find the function which would be used to decrypt the message. [**5**]

(d) The following ciphertext has been encrypted using an affine cipher. Assume the second most frequent letter in the plaintext is M. Make an educated guess for the most frequent letter in the plaintext. Hence find the decryption function and decrypt the message.

ZBBU ZB KBOB [**5**]

Question 2. [20 marks]
In all substitution tables the columns correspond to key entries and the rows correspond to plaintext entries.

(a) Encrypt the plaintext CAT with the key TCG using the substitution table S:

$S =$

	A	C	G	T
A	T	G	C	A
C	A	C	A	T
G	G	A	C	G
T	C	T	G	C

[**3**]

(b) Give an example of a plaintext message, which when encrypted with key TCG and substitution table S, cannot be decrypted even by the intended recipient (who is in possession of both the key and substitution table). [**3**]

(c) The substitution table T is given by:

$T =$

	A	C	G	T
A	T	T	T	G
C	G	C	A	T
G	A	A	C	A
T	C	G	G	C

[**3**]

What feature of T means the problem in (b) will not occur?

(d) A plaintext message M is encrypted using substitution table T. Initially you know that:

$$\mathbb{P}(M = \text{TAT}) = 0.1, \qquad \mathbb{P}(M = \text{GAG}) = 0.3, \qquad \mathbb{P}(M = \text{ACT}) = 0.6.$$

You intercept the ciphertext CTC. Modify the above probabilities accordingly. [**6**]

(e) In addition to your answer to (c), what further feature must a substitution table have in order to be a Latin square? What is the advantage of having this feature? Name the theorem that states that Latin squares have this advantage. [**5**]

Question 3. [**22 marks**]

(a) A shift register is described by the polynomial $x^3 + x^2 + 1$. Starting with initial configuration 001 calculate the key generated by this register. Is the shift register primitive? [**6**]

(b) Calculate the number of runs of 0's and the number of runs of 1's of each length in this key. Also calculate the out of phase autocorrelations of each shift and the in phase autocorrelation. With reference to these numbers, determine which of Golomb's postulates this key satisfies. [**8**]

(c) State a theorem which would have told you immediately which of Golomb's postulates this key satisfies, without performing the calculations in (b). [**2**]

(d) In a key generated by a primitive n-bit shift register, how many runs of 1's of length $n - 1$ are there? Explain your answer without using any results that you do not prove. [**6**]

Question 4. [**16 marks**] For full marks any methods you use should have fast (polynomial time) implementations on a classical computer.

(a) Bob is using RSA cryptography with public key ($n = 2035153$, $e = 11$). Eve hides a camera in Bob's home and catches him typing in his private key $d = 1283$. She then intercepts the encrypted number $T_e(x) \equiv 5 \mod 2035153$. Decrypt this to find x. [**8**]

(b) Bob finds the camera and realises that Eve has seen him type in his private key. He then switches his public key to $e' = 13$. Show that this is a mistake by computing his new private key (do not worry about the size of your answer, as long as it works). [**8**]

Question 5. [**22 marks**]

(a) A publicly known prime number p is fixed. Alice has a secret number a. Write down a linear equation in x which guarantees that T_x is the inverse of T_a. Name the method needed to find x by solving this equation. [**6**]

(b) Bob also has a secret number b and T_y is the inverse of T_b.

Alice wishes to secretly communicate a number $m \mod p$ to Bob. Let $m_0, m_4 = m$, and let m_1, m_2, m_3 be numbers they exchange publicly in that order. So first m_1 is sent publicly, then m_2, then m_3.

For $i = 1, 2, 3, 4$ write down:

- Which of the functions T_a, T_b, T_x, T_y is applied to m_{i-1} to get m_i,
- Who is applying the function,
- Which direction (if any) m_i is sent ('Alice to Bob' or 'Bob to Alice'). [**8**]

(c) Eve sees all the numbers being sent publicly. Suppose now it is publicly known that m is a primitive generator modulo p. If Eve invented a fast algorithm for solving the discrete logarithm problem, how could she break the encryption and find m? [**8**]

End of Paper.