Queen Mary
University of London

Main Examination period 2017

MTH6115 / MTH6115P: 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 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: B. Noohi

Question 1. [16 marks]

(a) In Cipher Challenge, one of the submissions was encrypted using the Vigènere key `XYABT` followed by a Caesar shift of 13. One of the students managed to crack this cipher by finding both the Vigènere key `XYABT` and the shift of 13. How did I find out that they had cheated? **[4]**

(b) The following ciphertext has been encrypted using the affine map $x \mapsto 25x + 6 \pmod{26}$. Decrypt it.

`ISMPG TOKCP YOESP PCEN` **[6]**

(c) How many substitution ciphers on the English alphabet are there that encrypt each of the following letters to itself: `d`, `s`, and `t`? How many of them are affine? Justify your answers. **[6]**

Question 2. [18 marks]

(a) Define what an *orthogonal array* of degree k and strength t over an alphabet $\mathcal{A} = \{a_1, \ldots, a_q\}$ of size q is. **[4]**

(b) Find the adjugate of the following Latin square on the alphabet $\mathcal{A} = \{1, 2, 3, 4\}$.

2	3	1	4
3	4	2	1
4	1	3	2
1	2	4	3

[6]

(c) State and prove Shannon's Theorem about one-time pads. (You do not need to define what a one-time pad is.) **[8]**

Question 3. [18 marks]

(a) State two of the three *Golomb's postulates* **G1**, **G2** and **G3** for a finite sequence of 0's and 1's. (Any two you like.) You do not need to define the terms *run* and *correlation*. **[6]**

(b) Define a *trapdoor one-way* function and explain its relevance to public-key cryptography. **[4]**

(c) Let p be a prime number such that $2^p - 1$ is also prime. Prove that every irreducible polynomial of degree p over $\mathbb{Z}_2$ is primitive. [Hint. How many irreducible/primitive polynomials are there?] **[8]**

Question 4. [16 marks]

(a) Let a and n be positive integers that are relatively prime. Define the *order* of a modulo n. **[3]**

(b) Compute $97^{121} \pmod{14300}$. Simplify your answer as much as possible. [Hint. The Carmichael function $\lambda(n)$ may be helpful.] **[7]**

(c) We know that 2077 is the product of two prime numbers, and that $\lambda(2077) = 330$. Use this information to factorise 2077. (The marks are for the method, not just the factorisation.) **[6]**

Question 5. [12 marks]

(a) Apply the Miller-Rabin primality test with $x = 46$ to test whether 133 is a prime number or not. (The marks are for the method, not the final yes/no answer.) [Hint. $46^{33} \equiv 113 \pmod{133}$.] **[7]**

(b) Suppose Bob's Knapsack key is $(52, 26, 108, 445, 3, 896, 1792, 3584)$. Why is this a bad choice for a key? Suppose Alice sends the ciphertext $b = 1059$ to Bob. Decrypt it. **[5]**

Question 6. [20 marks]

(a) Explain the *Discrete Logarithm Problem*. Is it NP-complete? **[4]**

(b) Explain the *Diffie-Hellman key establishment* protocol. Suppose Eve knows a fast way of solving the Discrete Logarithm Problem. Explain how she can recover the key that has been established between Alice and Bob through the Diffie-Hellman key establishment protocol. **[8]**

(c) Anna and Ben are using El-Gamal for encryption. They are using the prime $p = 59$, and primitive root $g = 6$ modulo 59. Ben's secret number is $b = 37$. Calculate the rest of Ben's public key, and encrypt the plaintext $x = 11$ for sending to him. [Hint. You may use the fast method from the lectures to compute powers of 6 modulo 59.] **[8]**

End of Paper.