Queen Mary
University of London

MTH6115 / MTH6115P: Cryptography

Duration: 2 hours

Date and time: 09 June 2016, 10:00–12:00

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 awarded 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 workings 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.

Examiner(s): B. Noohi

Question 1.

(a) Suppose you want to encrypt a plaintext by composing an affine cipher with a Vigenère. Which order of the composition ensures higher security? Does the resulting ciphertext depend on the order in which you apply the ciphers? Justify your answers. **[6]**

(b) Decrypt the following Caesar cipher:

```
YHUB HDVB FDHV DUFL SKHU
```

[6]

(c) Suppose you want to apply a transposition to the ciphertext in Part (b). How many different such transposition ciphers are there? **[3]**

Question 2.

(a) Determine how many positive integers there are that are less than and coprime to 10000. Find $\lambda(10000)$. **[5]**

(b) Find the last four digits of 3^{1005}. [Hint. You may use Part (a).] **[6]**

(c) We know that 1457 is the product of two prime numbers and that $\lambda(1457) = 690$. Use this information to factorise 1457. (The marks are for the method, not the factorisation.) **[6]**

Question 3.

(a) The sequence 0011110110 is generated by a 5-bit shift register. Determine the shift register. Is this shift register primitive? Justify your answer. **[8]**

(b) Explain the *Diffie-Hellman key exchange* protocol. **[6]**

(c) Suppose Eve knows a fast way of solving the Discrete Log Problem. Explain how she can crack the message being communicated via Diffie-Hellman key exchange. **[6]**

Question 4.

(a) Let p be a prime number and let a be an integer not divisible by p. Prove that the order of a modulo p divides $p - 1$. **[5]**

(b) Define what a *Sophie Germain* pair is. **[3]**

(c) Is 3 a primitive root modulo 59? Prove your claim. **[6]**

Question 5.

(a) Define the complexity classes P and NP. **[4]**

(b) Explain the operation of the El-Gamal cipher for encrypting messages. Which hard problem is it based on? Is it NP-complete? **[5]**

(c) Bob's Knapsack public key is $(812, 2, 20, 200, 55, 8, 3, 436)$. Why is this a bad choice for a Knapsack public key? What can Bob do with this sequence to make it more secure for use in Knapsack cipher? **[6]**

(d) Suppose Bob is using the Knapsack public key in Part (b). You have intercepted the ciphertext 519 sent from Alice to Bob. What is the plaintext? **[6]**

Question 6. The following is an orthogonal array on the alphabet $\{0, 1, 2, 3\}$:

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

(a) What are the degree k and the strength t of this orthogonal array? **[3]**

(b) What are the missing entries? **[4]**

(c) Your password is 23 and you want to use the above orthogonal array to share it between two friends so that 1) none of them alone can get any information about the password, and 2) both of them together can recover the password. How would you do it? Explain why your solution satisfies (1) and (2). **[6]**

End of Paper.