Queen Mary
University of London

**Main Examination period 2020 – January – Semester A**

# **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 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 B. Noohi**

---

 

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 [28 marks].** Let $n$ be a positive integer. For integers $a$ and $b$ (which may be taken modulo $n$), the affine map $\theta_{a,b} : \mathbb{Z}_n \to \mathbb{Z}_n$ is defined by $\theta_{a,b} : x \mapsto ax + b$.

(a) State a necessary and sufficient condition (in terms of $a$, $b$ and $n$) for the map $\theta_{a,b}$ to be invertible, that is a permutation of $\mathbb{Z}_n$. Prove your answer. **[6]**

(b) State (without proof) a formula for the number of distinct invertible affine maps there are on $\mathbb{Z}_n$. **[2]**

(c) Determine the number of (invertible) affine ciphers on the English alphabet fixing the word `AN`. **[6]**

(d) The following ciphertext has been encrypted using an affine cipher on the English alphabet.

`EHUBE TKGHJ EFZEH ZFUEX XJ`

You are also given the information that `E` decrypts to `z` and `X` **does not** decrypt to `e`.

(i) Determine the **decrypt** map $\theta_{c,d}$ for this cipher. [Hint: the last word is `EXXJ`.] **[4]**

(ii) Determine the full table Bob would use for decryption. **[4]**

(iii) Decrypt the message, clearly indicating word spacing. **[3]**

(e) Alice decides to encrypt a piece of text using the affine map $\theta_{6,5}$ applied to the English alphabet. State what is wrong with this plan. **[3]**

**Question 2 [16 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) When attempting to decrypt a Vigenère cipher, I notice that the most common trigram occurs four times, at positions 4, 56, 121 and 238 in the cipher text. Give a likely key length for the cipher based on this information. Also, say what calculation you performed to obtain this information. **[3]**

(c) After obtaining the key length, the next step in decrypting a Vigenère cipher is to sort the text into 'bins' or letter strings and take letter frequencies. Explain how each 'bin' (or letter string) is constructed when the key length is 11. **[4]**

(d) The letter frequencies for the first four 'bins' (or letter strings) are given in the appendix (Table 1). Write down, without justification, the (likely) first four letters of the keyword. **[4]**

**Question 3 [24 marks].** In this question, $p$ denotes plaintext and $z$ denotes ciphertext.

(a) Let $\mathscr{A}$ be an alphabet of size $q$. Define what it means for a $q \times q$ array of symbols from $\mathscr{A}$ to be a **Latin square**. **[4]**

(b) For each integer $q \geqslant 1$, write down a construction of a self-adjugate self-transpose Latin square of order $q$. [Half marks if you simply write down a Latin square of order $q$.] **[4]**

(c) State Shannon's Theorem. [You do not have to define the notion of a one-time-pad.] **[4]**

(d) A message in the 4-letter alphabet $\{0,1,2,3\}$ has been encrypted using a random keystring, with the keys uniformly distributed, and (weak) substitution table:

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 2 | 1 | 3 |
| 1 | 3 | 3 | 0 | 0 |
| 2 | 1 | 1 | 3 | 1 |
| 3 | 2 | 0 | 2 | 2 |

The message has length 3. Before intercepting the ciphertext your estimates of the probabilities of the plaintext strings are

$$\mathbb{P}(p = 012) = \tfrac{1}{3}, \quad \mathbb{P}(p = 300) = \tfrac{2}{3},$$

with the other probabilities being 0. Calculate the probability $\mathbb{P}(z = 231)$ given the above. You intercept the ciphertext $z = 231$. Given this information, calculate the conditional probability $\mathbb{P}(p = 012 \mid z = 231)$. Explain briefly why your answer does not contradict Shannon's Theorem. **[12]**

**Question 4 [32 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 60000. **[3]**

(c) Define what it means for an integer $n > 1$ to be a **Carmichael number**, and show that 1729 is such a number. [Note that $1729 = 12^3 + 1^3 = 10^3 + 9^3$.] **[6]**

(d) Explain briefly the operation of the El-Gamal cryptosystem. If Eve intercepts an El-Gamal communication, which "hard" problems does she have to solve in order to break the cipher? **[10]**

(e) In lectures you have seen a method to compute $x^a \pmod n$ with at most $2\log_2 a$ multiplications and reductions modulo $n$. Illustrate this method by calculating $3^{81} \bmod 31$. (Show your working.) **[7]**

---

**End of Paper – An appendix of 1 page follows.**

 

| letter | freq Bin 1 | freq Bin 2 | freq Bin 3 | freq Bin 4 |
|---|---|---|---|---|
| A | 1 | 3 | 0 | 2 |
| B | 0 | 15 | 0 | 0 |
| C | 0 | 2 | 5 | 4 |
| D | 0 | 1 | 8 | 9 |
| E | 9 | 3 | 3 | 4 |
| F | 2 | 7 | 0 | 4 |
| G | 2 | 0 | 5 | 0 |
| H | 8 | 1 | 7 | 5 |
| I | 15 | 0 | 5 | 0 |
| J | 2 | 1 | 3 | 3 |
| K | 2 | 11 | 0 | 0 |
| L | 5 | 8 | 4 | 5 |
| M | 10 | 3 | 0 | 4 |
| N | 0 | 0 | 2 | 3 |
| O | 1 | 9 | 0 | 2 |
| P | 3 | 5 | 4 | 11 |
| Q | 0 | 12 | 1 | 1 |
| R | 5 | 1 | 4 | 3 |
| S | 5 | 1 | 4 | 5 |
| T | 2 | 1 | 10 | 11 |
| U | 0 | 0 | 2 | 0 |
| V | 2 | 1 | 5 | 1 |
| W | 7 | 0 | 10 | 4 |
| X | 8 | 4 | 9 | 2 |
| Y | 2 | 1 | 0 | 4 |
| Z | 2 | 3 | 1 | 6 |

Table 1: Some letter frequencies (for Question 2(d))

---

**End of Appendix.**