Queen Mary
University of London

Main Examination period 2022 – January – Semester A

MTH6115 / MTH6115P: Cryptography

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

In completing this assessment:

- **You may use books and notes.**
- **You may use calculators and computers, but you must show your working for any calculations you do.**
- **You may use the Internet as a resource, but not to ask for the solution to an exam question or to copy any solution you find.**
- **You must not seek or obtain help from anyone else.**

All work should be **handwritten** and should **include your student number**.

The exam is available for a period of **24 hours**. Upon accessing the exam, you will have **3 hours** in which to complete and submit this assessment.

When you have finished:

- scan your work, convert it to a **single PDF file**, and submit this file using the tool below the link to the exam;
- e-mail a copy to **maths@qmul.ac.uk** with your student number and the module code in the subject line;
- with your e-mail, include a photograph of the first page of your work together with either yourself or your student ID card.

Please try to upload your work well before the end of the submission window, in case you experience computer problems. **Only one attempt is allowed – once you have submitted your work, it is final**.

Examiners: B. Noohi, S. Sasaki

 Continue to next page

Notation: Given a modulus n, $\theta_{a,b}$ denotes the affine map $x \mapsto ax + b \pmod{n}$.

Question 1 [25 marks].

(a) Give two Vigenère keys which combine to the key `SXNUMLUSVBXF` such that one of the keys has length 4 (the other key can have any length you like). [**4**]

(b) We say that two affine ciphers on the English alphabet *commute* if it does not matter in which order we apply them; otherwise we say that they do not commute. Find an affine cipher that commutes with $\theta_{7,1}$ and another affine cipher that does not commute with $\theta_{7,1}$. [**5**]

(c) The following text has been encrypted using an affine cipher on the English alphabet:

`PJADQ RDMBW`

We know that the first and the last letters of the plaintext are `w` and `n`, respectively. Decrypt the text. Show your working. [**7**]

(d) A ciphertext is obtained by applying a Vigenère cipher followed by an affine cipher. Does the first step in Kasiski's method give the correct key length? Justify your answer. [**5**]

(e) Can we use the following table for a stream cipher on the alphabet $\{a, b, c, d\}$? If the answer is yes, explain why. If the answer is no, justify your answer by giving an example of what can go wrong.

	a	b	c	d
a	a	b	b	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

[**4**]

 Continue to next page

Question 2 [25 marks].

(a) Which of the following encryption methods is more secure?

(i) A Vigenère cipher on the English alphabet with a key that is of the same length as the plaintext.

(ii) A Vigenère cipher on the binary alphabet $\{0, 1\}$ with a key that is of the same length as the plaintext.

Justify your answer. [**4**]

(b) The following is the output sequence of a 5-bit shift register.

$$10010110011111000$$

Determine the shift register. Show your working. [**7**]

(c) Prove that $x^5 + x^2 + 1$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$. [**7**]

(d) How many primitive 8-bit shift registers are there? Show your calculations. [**7**]

Question 3 [25 marks].

(a) Albert has written an algorithm for finding the inverse of a 2-by-2 matrix.

(i) Give an estimate, in terms of N, of the size of the input of this algorithm when the entries of the matrix are taken from natural numbers smaller than $N \in \mathbb{N}$. [**3**]

(ii) For matrix entries as in (i), Albert's algorithm computes the inverse in $N^2 + N$ steps. Is this a polynomial time algorithm? Justify your answer. [**4**]

(iii) Does the problem of finding the inverse of a 2-by-2 matrix belong to the class P? Justify your answer (but you do not need to give a rigorous proof). [**5**]

(b) For any integer a coprime to a prime number p, prove that $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. [**5**]

(c) In lectures, you have seen a method to compute $x^a \bmod n$ with at most $2 \log_2 a$ multiplications and reductions modulo n (I called it "the fast method"). Illustrate this method by calculating $5^{100} \pmod{37}$. Show your working. [**8**]

 Continue to next page

Question 4 [25 marks]. In parts (a) and (b) below your calculations in Q3(c) can be useful.

(a) Bob's El-Gamal public key is $(p, g, h) = (37, 5, 12)$ and his secret key is $a = 20$. Bob receives the message $(5, 17)$ from Alice. Decipher it, simplifying your answer as much as possible. [**7**]

(b) Alice and Bob are using the Diffie-Hellman key exchange protocol and they have agreed on the prime 37. Alice uses $(e_A, d_A) = (17, 17)$ and Bob uses $(e_B, d_B) = (5, 29)$.

(i) What relations should e_A, d_A, e_B and d_B satisfy? Verify that this is the case for the given numbers. [**4**]

(ii) Alice wants to share $x = 5$ with Bob. Calculate the three values that are exchanged through the process. [**4**]

(iii) Assuming that Eve sees the three exchanged numbers, what equation does she have to solve in order to recover x? What hard problem is this an instance of? [**4**]

(c) Let $a_1 < a_2 < \ldots < a_n$ be a super-increasing sequence. Prove that if the knapsack problem has a solution for an integer b, then the solution is unique.

[Hint. Suppose there are two solutions and compare the biggest terms in the two solutions.] [**6**]

End of Paper.