Queen Mary
University of London

Main Examination period 2023 – January – Semester A

MTH6115 / MTH6115P: Cryptography

Duration: 2 hours

The exam is intended to be completed within **2 hours**. However, you will have a period of **4 hours** to complete the exam and submit your solutions.

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

All work should be **handwritten** and should **include your student number**. Only one attempt is allowed – **once you have submitted your work, it is final**.

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.

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;

Examiners: B. Noohi, S. Sasaki

© Queen Mary University of London (2023) **Continue to next page**

Question 1 [25 marks].

(a) In the following Caesar cipher the most frequent letter corresponds to e. Decrypt it. Show your working. **[4]**

```
XBLLU THYFB UPCLY ZPAF
```

(b) Find an affine cipher $\theta_{a,b}$ on the English alphabet such that application of the cipher $\theta_{a,b}$ followed by $\theta_{7,1}$ is equivalent to applying the affine cipher $\theta_{9,3}$. Show your working. **[6]**

(c) Consider the alphabet $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

(i) Determine the permutation on $\mathbb{Z}_5$ resulting from applying the affine cipher $\theta_{3,2}$. Show your working. **[3]**

(ii) Find a substitution table on this alphabet whose corresponding stream cipher is equivalent to the affine cipher $\theta_{3,2}$. **[3]**

(d) Let N be a positive integer and consider the alphabet $\mathbb{Z}_N$.

(i) Explain why the addition table corresponding to the binary operation $i \oplus j = i - j \pmod{N}$ is a Latin square. **[3]**

(ii) Find the adjugate of this Latin square. Show your working. **[3]**

(iii) Is this Latin square suitable for a one-time pad on the alphabet $\mathbb{Z}_N$? Justify your answer. **[3]**

© Queen Mary University of London (2023) **Continue to next page**

Question 2 [25 marks].

(a) Alice is using a one-time pad on the alphabet $\mathbb{Z}_2 = \{0, 1\}$ with addition modulo 2. The key for this one-time pad is generated by a primitive 5-bit shift register. Eve intercepts the following ciphertext:

$$000110001011011.$$

Her spies have informed her that the initial part of the plaintext is

$$1000111011 \cdots .$$

Decipher the full ciphertext. Show your working. **[8]**

(b) Determine (with proof) whether $x^5 + x^3 + 1$ is

(i) irreducible over $\mathbb{Z}_2$, **[3]**

(ii) primitive. **[3]**

(c) Write down a pseudo-noise sequence of length 31, explaining carefully why your sequence is pseudo-noise. Determine the number of length 2 runs of 0s in this sequence. **[7]**

(d) Explain what goes wrong if in a public-key cryptosystem the *go public* function $g : S \to K$ from the set of secret keys to the set of public keys is in the complexity class ExpTime. **[4]**

Question 3 [25 marks].

(a) Paul has written an algorithm that finds the greatest common divisor of two polynomials $f(x) = x^3 + ax^2 + bx + c$ and $g(x) = x^3 + a'x^2 + b'x + c'$ with positive integer coefficients in $aa' + bb' + cc'$ steps. Is this a polynomial time algorithm? Justify your answer **[5]**

(b) Assume that multiplying and adding two positive integers can be performed in polynomial time. Explain why the problem of computing the product of two arbitrary polynomials is in class P. **[5]**

(c) Calculate $2^{1212} \pmod{9211}$, reducing it to a positive number less than 9211. Show your calculations. [Hint. $9211 = (151)(61)$.] **[6]**

(d) Consider the map $T_{77} : \mathbb{Z}_{9211} \to \mathbb{Z}_{9211}$, $T_{77}(x) \equiv x^{77} \pmod{9211}$. Is this map surjective? Justify your answer. How many positive integers $e < 300$ are there such that $T_e : \mathbb{Z}_{9211} \to \mathbb{Z}_{9211}$ is injective? (Recall that $T_e(x) \equiv x^e \pmod{9211}$.) **[9]**

© Queen Mary University of London (2023) **Continue to next page**

Question 4 [25 marks].

(a) Explain what goes wrong if the modulus N used in RSA is divisible by 25. **[3]**

(b) Alice and Bob are using the prime $p = 89$ and a primitive root g mod p for the Diffie-Hellman key establishment. However, they suspect that Eve might be tampering with their communication. Alice's secret number is $a = 7$ and Bob's is $b = 4$. Alice receives 5 from Bob and Bob receives 11 from Alice. Prove that the communication has indeed been tampered with by Eve. **[6]**

(c) Bob has chosen $p = 89$, $g = -8$ and $a = 16$ for his El-Gamal key. Apart from the numbers being small, give another reason why this is a poor choice of key. **[6]**

(d) In the previous part, what is Bob's public key? Encrypt the message $x = 5$ for sending to Bob, with your random k being the sum of the last two digits of your student id. Simplify your answer as much as possible. [Hint. You may find $4^6 \equiv 16^3 \equiv 2 \pmod{89}$ useful in your calculations.] **[6]**

(e) Alice and Bob are using the knapsack cipher and Bob's public key is

$$(49, 23, 1, 110, 5, 425, 260, 811).$$

Alice sends the message 1126 to Bob. Decrypt it. Show your working. **[4]**

End of Paper.

© Queen Mary University of London (2023)