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

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]**

Solution

(a) [SEEN SIMILAR] The most frequent letter in the ciphertext is `L`, which by assumption is mapped to `e`. Therefore, to decrypt we need to shift to the left by 7. **[2]** The answer is `Queen Mary University`. **[2]**

(b) [SEEN SIMILAR] We need to solve $\theta_{7,1} \circ \theta_{a,b} = \theta_{9,3}$. **[2]** The formula for composition is easy to work out (and is seen in class). The resulting system of equations is

$$\begin{aligned} 7a &\equiv 9 \pmod{26}, \\ 7b + 1 &\equiv 3 \pmod{26}. \end{aligned}$$

[2] Solving the first equation we find $a \equiv 5 \pmod{26}$. Solving the second equation we find $b \equiv 4 \pmod{26}$. The answer is $\theta_{5,4}$. **[2]**

(c) [SEEN SIMILAR]

(i) We need to work out $\theta_{3,2}(x) = 3x + 2$ for all $x \in \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. **[1]** The result is

$$0 \mapsto 2, \;\; 1 \mapsto 0, \;\; 2 \mapsto 3, \;\; 3 \mapsto 1, \;\; 4 \mapsto 4. \;\; [\mathbf{2}]$$

(ii) The answer is the following substitution table with constant rows: [**3**]

	0	1	2	3	4
0	2	2	2	2	2
1	0	0	0	0	0
2	3	3	3	3	3
3	1	1	1	1	1
4	4	4	4	4	4

(d) [UNSEEN]

(i) For each fixed i, the operation $i \oplus * = i - * \pmod{N}$ is a permutation on $\mathbb{Z}_N$, and similarly for $* \oplus j = * - j \pmod{N}$ for any fixed j. [**3**]

(ii) The adjugate corresponds to the operation $a \ominus b$, where $c = a \ominus b$ is defined by $c \oplus b = a$. In this case, this relation gives $a \ominus b = a + b \pmod{N}$. [**3**]

(iii) Yes, any Latin square is suitable for a one-time pad. [**3**]

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]**

Solution

(a) [SEEN SIMILAR] Subtracting the first 10 digits of the plaintext from the ciphertext we obtain the first 10 bits of the key: 1001011001. **[1]** We then solve the following system of equations:

$$\begin{array}{rcccccccccc} 1 & = & a_0 & + & & & & + & a_3, & & \\ 1 & = & & & & & a_2 & & & + & a_4, \\ 0 & = & & & a_1 & + & & + & a_3 & + & a_4, \\ 0 & = & a_0 & + & & + & a_2 & + & a_3, & & \\ 1 & = & & & a_1 & + & a_2. & & & & \end{array}$$

[2] Solving the system, we find $a_0 = 1$, $a_1 = 0$, $a_2 = 1$, $a_3 = 0$ and $a_4 = 0$. **[2]** We can now generate the rest of the key:

$$1001011001\mathbf{11110}.$$

[2] and subtract it from the cipher text to obtain the answer:

$$1000111011\mathbf{00101}.$$

[1]

(b) [SEEN SIMILAR] We will show that this polynomial is primitive. This would then imply, by a theorem seen in lectures, that the polynomial is irreducible. **[3]** For instance, we can take the initial state 11001 and generate the output sequence of the shift register associated to the polynomial:

$$[1100110100100001010111011000111]110011010\cdots.$$

This is periodic of period $31 = 2^5 - 1$, so the shift register, hence the polynomial, is primitive. **[3]**

(c) [SEEN SIMILAR] Take the sequence from the previous part. Since the shift register is primitive, by a theorem seen in lectures, it is pseudo-noise. **[4]** By the proof of the above theorem (or by inspection), the number of length 2 runs of 0s in this sequence is $2^{5-2-2} = 2$. **[3]**

[The only way they can answer the question is to start with a primitive 5-bit shift register. It is almost impossible to find the answer by guesswork.]

(d) [BOOKWORK] Bob will then not be able to create a public key in order for Alice to encrypt the message before sending it to him. **[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]**

Solution

(a) [UNSEEN] The size of the problem is $\log_2(a) + \log_2(b) + \log_2(c) + \log_2(a') + \log_2(b') + \log_2(c')$. **[3]** The expression $aa' + bb' + cc'$ is not a polynomial in the size (it is essentially exponential), so the algorithm is not polynomial time. **[2]**

(b) [UNSEEN] If the polynomials have n and m coefficients, respectively, then by mn multiplications and less than mn additions one can compute the coefficients of the product polynomial. **[3]** Since each of these operations can be done using at most $P(k)$ operations, where k is the size of the problem, at most $2mnP(k)$ operations are needed to compute the product polynomial. **[2]**

(c) [SEEN SIMILAR] We have $N = 151 \cdot 61 = 9211$, and $\lambda(9211) = \mathrm{lcm}(150, 60) = 300$. **[2]** So, by Lemma A,

$$2^{1212} \pmod{9211} \equiv 2^{12} \pmod{9211},$$

and the latter is equal to 4096 modulo 9211. **[2+2]**

(d) [SEEN SIMILAR] We first note that T_e is injective if and only if it is surjective if and only if it is bijective **[2]** and for $T_e : \mathbb{Z}_N \to \mathbb{Z}_N$ to have this property is equivalent to $\gcd(e, \lambda(N)) = 1$. **[2]** In our example this is the case as $\gcd(77, 300) = 1$. Therefore, the map is surjective. **[2]** The number of $1 < e < 300$ satisfying $\gcd(e, 300) = 1$ is equal to $\varphi(300) = 2^{2-1}(2-1) \cdot (3-1) \cdot 5^{2-1}(5-1) = 80$. **[3]**

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]**

Solution

(a) [BOOKWORK] The modulus N of RSA should be a product of two distinct primes because otherwise, as seen in lectures, the encryption map $T_e : \mathbb{Z}_N \to \mathbb{Z}_N$ will not be injective even if $\gcd(e, \lambda(N)) = 1$. [**3**]

(b) [UNSEEN, but easy] By definition, $5 = g^b$ and $11 = g^a$ modulo 89. [**2**] The shared key should then be $g^{ab} \equiv 5^7 \equiv (?)11^4 \pmod{89}$, but the last congruence is wrong as $5^7 \equiv 72$ and $11^4 \equiv 45 \pmod{89}$. [**3**] This means at least one of the numbers 5 or 11 is wrong, hence the communication has been tampered with. [**1**]

(c) [SEEN SIMILAR] Because $-8 \equiv 81 \equiv 3^4 \pmod{89}$, so $81^{22} \equiv 1 \pmod{89}$ by Fermat. [**3**] Thus, 81 is not a primitive root (in fact, it has a relatively small order) and thus the Discrete Log Problem can be easily solved for powers of 81. [**3**]

(d) [SEEN SIMILAR] Bob's public key is (p, g, h), where $h = g^a \equiv (-8)^{16} = 16 \pmod{89}$. [**1**] (The latter is easily computed by noting that $(-8)^4 \equiv 2 \pmod{89}$.) [**2**] The encrypted message is $(g^k, xh^k) = ((-8)^k, 5(16)^k) \pmod{89}$. This should be easy to work out even by hand using the fact that $4^6 \equiv 16^3 \equiv 2 \pmod{89}$. [**3**]

(e) [UNSEEN] We can use the Greedy algorithm because up to re-ordering the sequence is super-increasing. [**1**] The answer is $1126 = 811 + 260 + 49 + 5 + 1$. (The numbers on the right hand side are found in the decreasing order.) [**3**]

End of Paper.