NANYANG TECHNOLOGICAL UNIVERSITY

SEMESTER I EXAMINATION 2022-2023

MH4311 – Cryptography

November 2022 TIME ALLOWED: 2 HOURS

INSTRUCTIONS TO CANDIDATES

1. This examination paper contains **SIX (6)** questions and comprises **THREE (3)** printed pages.
2. Answer all questions. The marks for each question are indicated at the beginning of each question.
3. Answer each question beginning on a **FRESH** page of the answer book.
4. This is an **OPEN BOOK** exam.
5. Candidates may use calculators. However, they should write down systematically the steps in the workings.

Question 1. Polynomial Quotient Ring (10 marks)
A finite field $\mathbf{GF}(2^5)$ is defined with the reduction polynomial $x^5 + x^2 + 1$. This finite field is used in the polynomial quotient ring $\mathbf{GF}(2^5)[x]/(x^4 + 1)$. Compute the product of two elements of this polynomial quotient ring: $\{08\}x^3$ and $\{12\}x^2$, where $\{08\}$ and $\{12\}$ are in hexadecimal format.

Question 2. Block Cipher Mode (10 marks)
Message M consists of three message blocks, $M = m_0 \parallel m_1 \parallel m_2$, where each m_i is a 128-bit block. We use a 256-bit key K in AES-256 to encrypt M using CFB mode, the 128-bit nonce is IV, and the ciphertext is $C = c_0 \parallel c_1 \parallel c_2$. We now use the same key K in AES-256 to encrypt another message M' using CBC mode, the 128-bit nonce is IV', and the ciphertext is $C' = c'_0 \parallel c'_1 \parallel c'_2$. Suppose that $c'_0 = c_2 \oplus m_2$, $c'_1 = c_0 \oplus m_0$, $c'_2 = c_1 \oplus m_1$. Suppose that IV, IV' are known, m_i, c_i and c'_i are known for $0 \leq i \leq 2$, and the last message block of M' is a full block. What is the message M' in terms of IV, IV', m_i, c_i and c'_i $(0 \leq i \leq 2)$?

Question 3. Message Authentication Code (20 marks)

(a) We use SHA-256 in HMAC to authenticate a 1000-bit message. Suppose that it takes 300 clock cycles to compute the compression function of SHA-256 on a computer. How many clock cycles are needed to generate the authentication tag of this message?

(b) Message M consists of three message blocks, $M = m_0 \parallel m_1 \parallel m_2$, where each m_i is a 128-bit block. A 128-bit secret key K is used in AES-128 to encrypt M in CBC mode, the 128-bit nonce is $IV = 0$, and the ciphertext is $C = c_0 \parallel c_1 \parallel c_2$. The same secret key K is used in AES-128 in CMAC to protect the plaintext M, and the authentication tag is t. IV, C and t are sent to the receiver. You are required to modify C (and modify IV if IV needs to be modified) so that the modified C, IV and the authentication tag can pass verification.

Question 4. Elliptic Curve Cryptography (20 marks)

(a) The elliptic curve $y^2 = x^3 + 5x + 7$ is over $\mathbf{GF}(17)$. $P = (3, 7)$ is a point on this curve. What is the value of $2P$?

(b) Prime number p is 256-bit. A non-singular elliptic curve E is over $\mathbf{GF}(p)$. P and Q are two points on the curve E, x is a 60-bit unknown integer, and $Q = xP$. Given the values of P and Q (P and Q are not the identity element), what is the lowest computational complexity to find the value of x? Please justify your answer in details.

Question 5. RSA and ElGamal (30 marks)

(a) In a toy RSA encryption scheme, the public key is (n, e), and the private key is d. $n = 629 = 17 \times 37$. Generate a key pair (e, d).

(b) Use Miller-Rabin primality test to show that 153 is a composite number.

(c) We use blinding technique to protect the private key in RSA decryption. In ElGamal decryption, do we need to use blinding technique to protect the private key? Please justify your answer. If your answer is yes, please specify the details of the blinding technique for ElGamal decryption.

Question 6. Malicious WiFi Router (10 marks)
Is it secure to use your computer to access your NTU email account through a malicious WiFi router? Please justify your answer.

END OF PAPER

MH4311 CRYPTOGRAPHY

Please read the following instructions carefully:

1. **Please do not turn over the question paper until you are told to do so. Disciplinary action may be taken against you if you do so.**

2. You are not allowed to leave the examination hall unless accompanied by an invigilator. You may raise your hand if you need to communicate with the invigilator.

3. Please write your Matriculation Number on the front of the answer book.

4. Please indicate clearly in the answer book (at the appropriate place) if you are continuing the answer to a question elsewhere in the book.