NANYANG TECHNOLOGICAL UNIVERSITY

SEMESTER I EXAMINATION 2023-2024

MH4311 – Cryptography

December 2023 TIME ALLOWED: 2 HOURS

INSTRUCTIONS TO CANDIDATES

1. This examination paper contains **SIX (6)** questions and comprises **FOUR (4)** 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 $\mathbf{GF}(2^6)$ is defined with the irreducible binary polynomial $x^6 + x + 1$. This finite field is used to construct the polynomial quotient ring $\mathbf{GF}(2^6)[x]/(x^5+1)$. Compute the product of two elements of this polynomial quotient ring: $\{21\}x^3 + 1$ and $\{02\}x^3 + 1$, where $\{21\}$ and $\{02\}$ are in hexadecimal format.

QUESTION 2. Block Cipher Mode (20 marks)
A message was encrypted using AES-128. The message length is 1024 **bytes**. The IV and the ciphertext were sent to the receiver.

(a) Suppose that AES-128 in OFB mode was used for encryption. If there is transmission error in the 17th byte of the ciphertext, how many plaintext blocks would be decrypted wrongly?

(b) Suppose that AES-128 in OFB mode was used for encryption. If there is transmission error in the 6th byte of IV, how many plaintext blocks would be decrypted wrongly?

(c) Suppose that AES-128 in OFB mode was used for encryption. If the second ciphertext block was lost during transmission (the receiver does not notice that one block of the ciphertext was lost), how many plaintext blocks would be decrypted wrongly? (If a plaintext block can be recovered correctly, but the position of the plaintext block is modified, we consider that this plaintext block is decrypted correctly in this question.)

(d) Suppose that AES-128 in CFB mode was used for encryption. If there is transmission error in the 6th byte of IV, how many plaintext blocks would be decrypted wrongly?

(e) Suppose that AES-128 in CFB mode was used for encryption. If the second ciphertext block was lost during transmission (the receiver does not notice that one block of the ciphertext was lost), how many plaintext blocks would be decrypted wrongly? (If a plaintext block can be recovered correctly, but the position of the plaintext block is modified, we consider that this plaintext block is decrypted correctly in this question.)

QUESTION 3. Message Authentication Code (20 marks)

(a) AES-128 is used in CBC-MAC to authenticate messages. Suppose that all the message lengths are 64 bytes. Both the sender and the receiver are aware of the length information. Is this authentication scheme secure? Please justify your answer.

(b) Alice used a key K in AES-128 in ECB mode to encrypt a long message M. Every message block of M is non-zero. The ciphertext is C. Eve knows both M and C. Now Alice and Bob use the same key K in AES-128 in CMAC to authenticate the messages being transmitted between Alice and Bob (the communication between Alice and Bob is not encrypted). Eve observed that the message M and its authentication tag t was sent to Bob. Can Eve forge a message successfully? Please justify your answer.

QUESTION 4. Elliptic Curve Cryptography (20 marks)

(a) The elliptic curve $y^2 = x^3 + 7x + 2$ is over $\mathbf{GF}(23)$. $P = (19, 5)$ and $Q = (13, 6)$ are two points on this curve. Compute $P + Q$.

(b) A non-singular elliptic curve E is over $\mathbf{GF}(p)$, where p is a 1024-bit prime number. The order of the group of this elliptic curve is a 1023-bit integer n, and n is 2^{32}-smooth. Is it secure to use this elliptic curve in the Elliptic Curve Diffie-Hellman Key Exchange? Please justify your answer in details.

QUESTION 5. RSA (20 marks)

(a) In a toy RSA encryption scheme, the public key is (n, e), and the private key is d. $n = 4171 = 43 \times 97$. Please generate a key pair (e, d).

(b) Let $n = 242321$ and $m = \lfloor \sqrt{n} \rfloor = 492$. We obtained the following relations:

$$(m+2)^2 - n = 5 \times 7^3$$
$$(m-3)^2 - n = (-1) \times 2^7 \times 5^2$$
$$(m-6)^2 - n = (-1) \times 5^3 \times 7^2$$
$$(m-21)^2 - n = (-1) \times 2^{12} \times 5$$
$$(m+22)^2 - n = 5^5 \times 7$$

Use the above information to factorize n.

QUESTION 6. Insecure Communication (10 marks)

Alice is using a remote server. The communication between Alice and the server is protected using AES encryption. Whenever Alice types a character on the keyboard, the character is encrypted using AES, then the ciphertext is sent to the server. Each character is encrypted independently using AES ECB mode, and the character is padded with zero-valued bits to obtain a full message block for encryption. Suppose that Alice typed a report. Please develop an attack to recover Alice's report from the intercepted ciphertexts.

END OF PAPER