NANYANG TECHNOLOGICAL UNIVERSITY

SEMESTER I EXAMINATION 2024-2025

MH4311 – Cryptography

December 2024 TIME ALLOWED: 2 HOURS

INSTRUCTIONS TO CANDIDATES

1. This examination paper contains **SEVEN (7)** questions and comprises **FIVE (5)** 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. Block Cipher Mode (20 marks)

Alice wants to send the following text to Bob:

```
Transmit two thousand dollars to DBS 345678901
```

In the Hex editor, the text appears as:

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   54 72 61 6E 73 6D 69 74 20 74 77 6F 20 74 68 6F  Transmit two tho
00000010   75 73 61 6E 64 20 64 6F 6C 6C 61 72 73 20 74 6F  usand dollars to
00000020   20 44 42 53 20 33 34 35 36 37 38 39 30 31         DBS 345678901
```

Alice encrypts the message using AES-128 in CBC mode. PKCS#7 padding is used for the encryption. The IV and ciphertext are given below.

```
IV:         73 21 96 53 CD 9E 9B 13 48 95 EF 3F C7 43 F8 E8
Ciphertext: DB 64 B5 5D E4 9A 0D 37 C4 FB BB B1 E3 8F F7 C0
            F0 D4 3E E2 24 7A 7A A3 89 AB F0 32 F0 14 E7 3B
            33 5D 30 25 90 D2 C1 20 A6 81 07 F8 D0 39 8B 76
```

Message authentication is not used. The IV and ciphertext are sent to Bob.

The ASCII table of printable characters is given in Table 1 on Page 3.

(a) Is it possible for an attacker to modify the transmission from Alice to Bob so that, after decryption, Bob obtains the following text?

```
Transmit ten thousand dollars to DBS 345678901
```

Please justify your answer. If your answer is yes, explain how the attacker modifies the transmission.

(b) Is it possible for an attacker to modify the transmission from Alice to Bob so that, after decryption, Bob obtains the following text?

```
Transmit two thousand dollars to DBS 345678916
```

Please justify your answer. If your answer is yes, explain how the attacker modifies the transmission.

Question 1 is continued on the next page.

Table 1: ASCII Table of Printable Characters

Character	Hex	Decimal		Character	Hex	Decimal		Character	Hex	Decimal
	20	32		@	40	64		`	60	96
!	21	33		A	41	65		a	61	97
"	22	34		B	42	66		b	62	98
#	23	35		C	43	67		c	63	99
$	24	36		D	44	68		d	64	100
%	25	37		E	45	69		e	65	101
&	26	38		F	46	70		f	66	102
'	27	39		G	47	71		g	67	103
(	28	40		H	48	72		h	68	104
)	29	41		I	49	73		i	69	105
*	2a	42		J	4a	74		j	6a	106
+	2b	43		K	4b	75		k	6b	107
,	2c	44		L	4c	76		l	6c	108
-	2d	45		M	4d	77		m	6d	109
.	2e	46		N	4e	78		n	6e	110
/	2f	47		O	4f	79		o	6f	111
0	30	48		P	50	80		p	70	112
1	31	49		Q	51	81		q	71	113
2	32	50		R	52	82		r	72	114
3	33	51		S	53	83		s	73	115
4	34	52		T	54	84		t	74	116
5	35	53		U	55	85		u	75	117
6	36	54		V	56	86		v	76	118
7	37	55		W	57	87		w	77	119
8	38	56		X	58	88		x	78	120
9	39	57		Y	59	89		y	79	121
:	3a	58		Z	5a	90		z	7a	122
;	3b	59		[	5b	91		{	7b	123
<	3c	60		\	5c	92		|	7c	124
=	3d	61		]	5d	93		}	7d	125
>	3e	62		^	5e	94		~	7e	126
?	3f	63		_	5f	95		Delete	7f	127

QUESTION 2. Finite Field (12 marks)

A finite field $\mathbf{GF}(2^6)$ is defined with the irreducible binary polynomial $x^6 + x + 1$.

(a) What is the additive inverse of 6 in this finite field?

(b) What is the multiplicative inverse of 6 in this finite field?

(c) For a different finite field $\mathbf{GF}(5^6)$, what is the additive inverse of $x^3 + 2$?

QUESTION 3. Hash Function (8 marks)

On a cloud storage server hosting a vast number of files, SHA-256 is used to hash each file, with the message digest serving as the file's identifier. When two or more files have the same identifier (hash), only one copy of the file is stored to conserve space.

Given that there are 2^{60} files stored on the server, what is the probability that two different files will produce the same message digest? Is it practically possible for two distinct files to produce the same SHA-256 identifier, leading to one file being wrongly deleted from the server?

QUESTION 4. Authenticated Encryption (15 marks)

Alice uses AES-128-GCM to protect the transmitted messages. We have learned that if the IV is reused with the same key, AES-128-GCM becomes insecure. Alice wants to improve the security of AES-128-GCM.

(a) To protect a message, Alice sets the IV to zero, then applies AES-128-GCM to the message to obtain an authentication tag t'. The ciphertext is discarded. Alice then sets the IV to t', applies AES-128-GCM to the message again, and sends the IV, associated data, ciphertext, and authentication tag to the receiver. Is AES-128-GCM secure when used this way? Please justify your answer.

(b) To protect a message M, Alice sets the IV to SHA-256(M), then applies AES-128-GCM to the message, and sends the IV, associated data, ciphertext, and authentication tag to the receiver. Is AES-128-GCM secure when used this way? Please justify your answer. (Hint: Consider the security of short messages.)

QUESTION 5. Elliptic Curve Cryptography (15 marks)

(a) The elliptic curve $y^2 = x^3 + 4x + 7$ is over $\mathbf{GF}(19)$. $Q = (7, 6)$ is a point on this curve. Compute $3Q$.

(b) A non-singular elliptic curve E is defined over $\mathbf{GF}(p)$, where p is a 512-bit prime number. The order of this elliptic curve group is a 510-bit prime number q. Let G be a generator of this elliptic curve group. Both E and G are known. In the equation $xG = T$, T is a known element in this elliptic curve group, and x is a 100-bit unknown integer. What is the lowest computational complexity to find x?

QUESTION 6. RSA (15 marks)

(a) In a toy RSA encryption scheme, the public key is (n, e), and the private key is d. $n = 1739 = 37 \times 47$. Please generate a key pair (e, d).

(b) Alice and Bob generated their RSA keys independently. The public keys of Alice and Bob are (n_a, e_a) and (n_b, e_b), respectively. The moduli n_a and n_b are 2048-bit integers. An attacker noticed that n_a and n_b are not coprime. Can the attacker recover the private keys of Alice and Bob? Please justify your answer. What might be the possible reason that n_a and n_b are not coprime?

QUESTION 7. OAEP (15 marks)

A random number r is used in the OAEP padding of RSA. To encrypt a message m, all the users generate r as $r = \text{SHA-256}(m)$. All the users use 2048-bit moduli in their RSA keys.

(a) Is it secure for all users to use the same $e = 17$? Please justify your answer.

(b) Is it secure to encrypt a 40-bit message? Please justify your answer.

END OF PAPER

MH4311 CRYPTOGRAPHY

CONFIDENTIAL

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.