28

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
(ONLINE)
SEMESTER I
SESSION 2020/2021

COURSE NAME	:	CRYPTOGRAPHY
COURSE CODE	:	BIS 20404
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JANUARY /FEBRUARY 2021
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS. 2. PLEASE MAKE SURE TO CLICK "SAVE ANSWER" BUTTON FOR SUBJECTIVE QUESTIONS.

THIS QUESTION PAPER CONSISTS OF **FOUR (4)** PAGES

Q1 Explain the importance of the following principles or concepts or idea in the design of a secure block cipher.

(a) Kerckhoffs's Principle

(3 marks)

(b) Confusion and diffusion

(3 marks)

(c) Brute Force Attack

(3 marks)

(d) Avalanche Effect

(3 marks)

(e) Free from side channel attack

(3 marks)

Q2 (a) Compute the value of correlation coefficient (r) between message and ciphertext in the Table **Q2 (a).** These values are message and ciphertext pair generated from a newly developed encryption algorithm.

$$r = \frac{n(\Sigma xy) - (\Sigma x)(\Sigma y)}{\sqrt{[n\Sigma x^2 - (\Sigma x)^2][n\Sigma y^2 - (\Sigma y)^2]}}$$

TABLE Q2 (a)

Item	Message (Decimal)	Ciphertext (Decimal)
1	43	99
2	21	65
3	25	79
4	42	75
5	57	87
6	59	81

(6 marks)

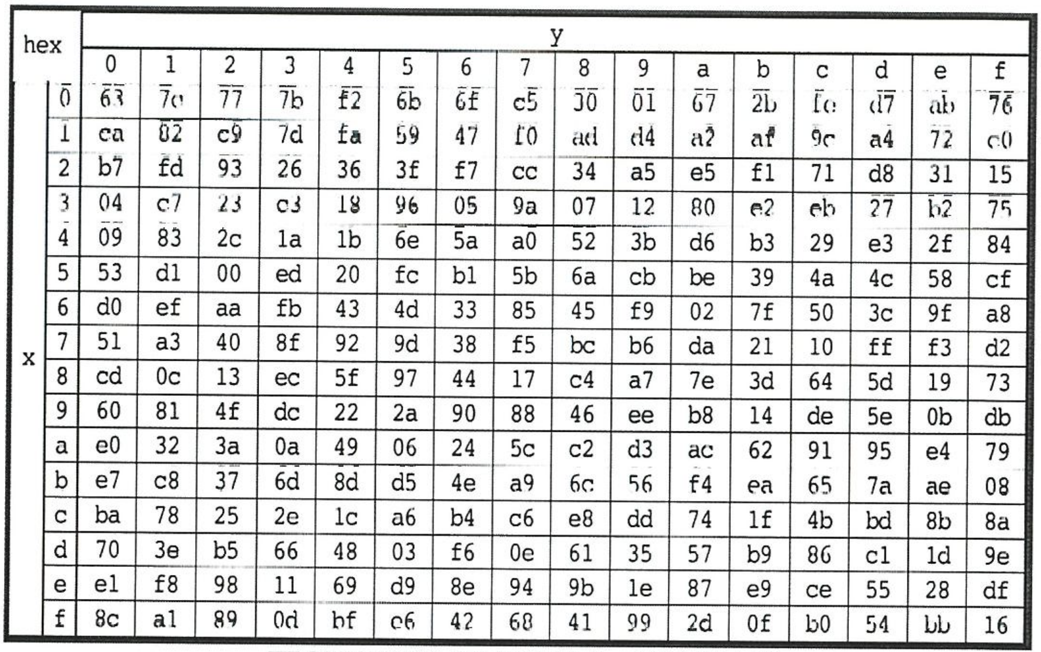
(b) Discuss the importance of this correlation coefficient value in **Q2 (a)** for evaluating the security of a new encryption algorithm.

(4 marks)

Q3 (a) Convert the following message WELCOMETOUTHMJHR into 128-bit HEXADECIMAL block format suitable for input to Rijndael Algorithm (Show your work).

(5 marks)

(b) Based on Figure **Q3 (b)**,



hex		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

FIGURE Q3 (b) SBOX for RIJNDAEL

Compute the value of the following message after SUBBYTE operation (Show your work).

$$\text{Message} = \begin{pmatrix} ff & ed & 12 & be \\ 3d & f4 & c6 & f8 \\ e3 & e2 & 8d & 48 \\ be & 3d & 2a & 80 \end{pmatrix}$$

(5 marks)

(c) Compute the output message from **Q3 (a)** after a SHIFTROWS operation. (Show your work).

(5 marks)

(d) Compute the intermediate result (first entry ONLY row 1 column 1) from **Q1 (c)** using MIXCOLUMN based on the following MDS matrix (Show your work).

$$MDS = \begin{pmatrix} 2 & 1 & 1 & 3 \\ 3 & 2 & 1 & 1 \\ 1 & 3 & 2 & 1 \\ 1 & 1 & 2 & 3 \end{pmatrix}$$

(5 marks)

Q4 Alice wants to use Rivest-Shamir-Adleman (RSA) algorithm to send encrypted messages to Bob. Thus, Bob needs to distribute his public key to Alice before she can encrypt the messages. Bob selects two prime number 19 and 23 as p and q respectively. Then, he selects an exponent $e = 11$ which is coprime to $\emptyset(n)$.

(a) Calculate the value of $\emptyset(n)$.

(1 mark)

(b) Calculate the value of the private key, d.

(5 marks)

(c) Show the pairs of Bob's public and private key.

(3 marks)

(d) Compute its corresponding ciphertext if Alice wants to send a plaintext, $p = 88$ to Bob.

(4 marks)

(e) Show how Bob computes the corresponding plaintext after he receives the ciphertext.

(2 marks)

- END OF QUESTIONS -