TECHNOLOGICAL UNIVERSITY DUBLIN
Grangegorman

_____

TU857- BSc. (Honours) Degree in Computer Science (Infrastructure)
TU856- BSc. (Honours) Degree in Computer Science
TU858- BSc. (Honours) Degree in Computer Science (International)
TU821- BSc. (Honours) Degree in Electrical & Electronic/ Computer & Communications Engineering

Year 3 & 4
_____

SEMESTER 1 EXAMINATIONS 2022/23
_____

CMPU 4007 **Advanced Security 1**

Internal Examiner(s): Dr. Aneel Rahim,
Dr. Paul Doyle

External Examiner(s): Sanita Tifentale – TU856, TU858
Dr. Charles Markham – TU857

Instructions To Candidates: ANSWER **THREE** QUESTIONS OUT OF **FOUR**.
ALL QUESTIONS CARRY EQUAL MARKS.
ONE (1) COMPLIMENTARY MARK WILL BE GIVEN.

Exam Duration: 2 hours

Special Instructions /Handouts/ Materials Required:

1. (a) Explain the following

    (i) Categories of passive and active security attacks   (6 marks)

    (ii) Categories of security services   (5 marks)

(b) What are the five essential ingredients of a symmetric cipher?   (10 marks)

(c) In relation to classical encryption techniques, explain the following

    (i) Steganography   (4 marks)

    (ii) Hill Cipher   (4 marks)

    (iii) Playfair Cipher   (4 marks)

2. (a) Bob wants to send a message to Alice, as shown in the image. In relation to Public key cryptography, does the communication shown below provide confidentiality and authentication? If not, then describe the changes required to achieve this. Explain your reasoning.   (10 marks)
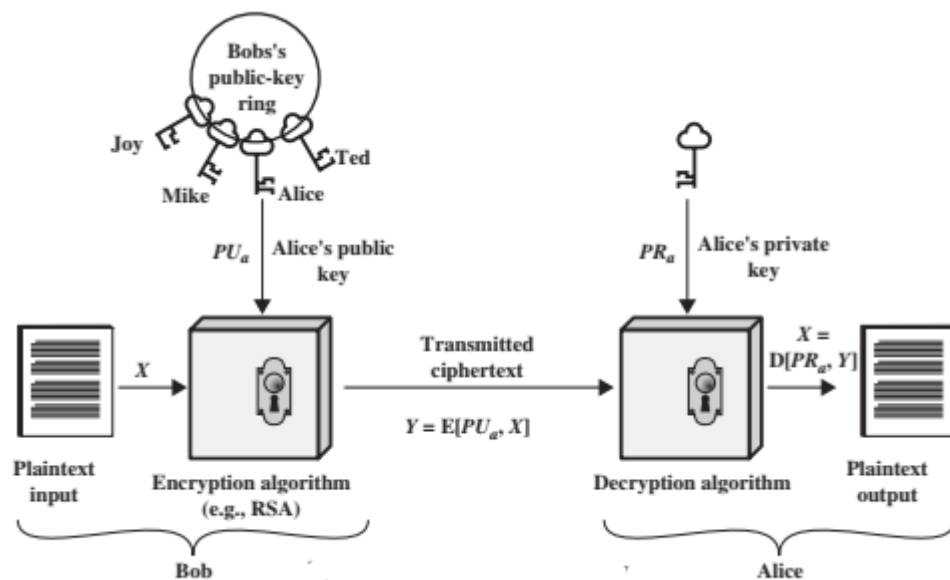

Figure 1: Public-Key Cryptosystem: Authentication and Confidentiality

    (b) Write a brief summary of what you have learned in relation to Feistel Cipher with no more than 400 words.

        (12marks)

(c) In relation to public key cryptography, explain the following:

    (i) Public-Key Requirements   (6 marks)

    (ii) Attacks on RSA algorithms   (5 marks)

3. (a) In relation to number theory, explain the following:

    (i) Fermat's Theorem   (5marks)

    (ii) Euclidean algorithm   (5 marks)

    (iii) Euler's Theorem   (5 marks)

(b) Explain the Vigenère Cipher. Include an example to support your answer. (10 marks)

(c) Explain the Double DES and Triple-DES.   (8 marks)

4. (a) Explain the True Random Number Generator (TRNG) and Pseudorandom Number Generator (PRNG).   (10 marks)

(b) Explain the block Cipher Operation of output feedback mode (OFB). Use a diagram to illustrate your answer   (11 marks)

(c) (i) Perform AES SubByte Transformation on the matrix using S box (See next page)

                                                                     (6 marks)

DB	A1	F8	77
18	6D	8B	BA
A8	30	08	4E
FF	D5	D7	AA

→

    (ii) Perform AES Shift Row Transformation on the matrix.

                                                                      (6 marks)

99	1E	73	F1
AF	18	15	30
84	DD	97	3B
08	08	0C	A7

→

Table 5.2 AES S-Boxes

									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

(a) S-box