COMPUTER SCIENCE TRIPOS Part II – 2019 – Paper 8

5 Cryptography (mgk25)

(*a*) The *Tripos Encryption Standard (TES)* is a block cipher optimized for use on UGPs ("undergraduate processors"). It operates on 4-bit blocks, written as hexadecimal digits (e.g., `a` $\oplus$ `9` = `3`). For one particular key K, it implements the following permutation:

m	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$E_K(m)$	1	b	5	c	7	e	2	a	4	9	f	d	0	3	6	8

Using this key K, decrypt the following three ciphertexts according to the indicated modes of operation. [*Note:* the XOR table at the bottom of this page may be of use.]

(*i*) ECB: `188b06` [2 marks]

(*ii*) CBC: `301b2` [3 marks]

(*iii*) CFB: `10f6d` [3 marks]

(*b*) State four advantages that counter mode has over either CBC or CFB mode. [4 marks]

(*c*) Using the same K as in Part (*a*):

(*i*) Show that the CBC-MAC tag for message `1234` is `d`. [3 marks]

(*ii*) Demonstrate that CBC-MAC with a given K is not collision resistant, by showing how to find another message, of the form `1`x`04`, that results in the same CBC-MAC message tag (without iterating over different candidates for 4-bit block x). [5 marks]

UGP XOR accelerator:

$\oplus$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	1	0	3	2	5	4	7	6	9	8	b	a	d	c	f	e
2	2	3	0	1	6	7	4	5	a	b	8	9	e	f	c	d
3	3	2	1	0	7	6	5	4	b	a	9	8	f	e	d	c
4	4	5	6	7	0	1	2	3	c	d	e	f	8	9	a	b
5	5	4	7	6	1	0	3	2	d	c	f	e	9	8	b	a
6	6	7	4	5	2	3	0	1	e	f	c	d	a	b	8	9
7	7	6	5	4	3	2	1	0	f	e	d	c	b	a	9	8
8	8	9	a	b	c	d	e	f	0	1	2	3	4	5	6	7
9	9	8	b	a	d	c	f	e	1	0	3	2	5	4	7	6
a	a	b	8	9	e	f	c	d	2	3	0	1	6	7	4	5
b	b	a	9	8	f	e	d	c	3	2	1	0	7	6	5	4
c	c	d	e	f	8	9	a	b	4	5	6	7	0	1	2	3
d	d	c	f	e	9	8	b	a	5	4	7	6	1	0	3	2
e	e	f	c	d	a	b	8	9	6	7	4	5	2	3	0	1
f	f	e	d	c	b	a	9	8	7	6	5	4	3	2	1	0