8 Security I (MGK)

(*a*) *NybbleCrypt* is a block cipher optimized for use in exam questions. It has a block size of 4 bits and a key length of 64 bits. Each block can be written as a single hexadecimal digit, for example `5` $\oplus$ `9` = `c`.

(*i*) The *NybbleCrypt* encryption function for a particular key K is given in the following table:

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

Decrypt the following messages, which were encrypted using E_K under the following modes of operation, respectively:

(A) ECB mode: `c994f88` [2 marks]

(B) CBC mode: `b144f` [3 marks]

(C) OFB mode: `eae26` [3 marks]

(*ii*) Calculate the CBC-MAC of the following message, using the same key K as in part (*a*)(*i*) above: `face` [2 marks]

(*iii*) *NybblePay* point-of-sale card terminals send 4-digit customer PINs to the bank's transaction-processing centre for verification. The bank's reply to the terminal consists of a 7-digit message in the following format:

(A) 4-digit PIN $m_1m_2m_3m_4$

(B) 2-digit result code m_5m_6: `10` if the PIN was correct, `e1` if not

(C) check digit $m_7 = m_1 \oplus \cdots \oplus m_6$ (the bit-wise XOR of previous digits)

This reply is sent OFB-encrypted using the *NybbleCrypt* blockcipher. You have intercepted such a ciphertext message: `a59defc2`. You are confident that it contains the result code m_5m_6 = `e1` for an incorrect PIN. Without knowing the encryption key K, modify the ciphertext message such that after decryption it shows the result code for a correct PIN, and a matching check digit, while preserving the included PIN. [5 marks]

(*b*) *NybbleShuffle* is a transposition cipher that operates on blocks of 32768 bytes. It splits each such block into 4-bit subblocks, and then rearranges these subblocks in pseudo-random order, under the control of a secret key K, in order to form the 32768-bytes long ciphertext block that it outputs. What is the smallest number of test blocks that you have to feed into an instance of the *NybbleShuffle* cipher in order to unambiguously reconstruct the permutation of subblocks that it applies, and how do you construct these test blocks? [5 marks]