8 Security I (MGK)

(a) Block ciphers usually process 64 or 128-bit blocks at a time. To illustrate how their modes of operation work, we can use instead a pseudo-random permutation that operates on the 26 letters of the English alphabet:

| 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 |
| A B C D E F G H I J K L M N O P Q R S T U V W X Y Z |

As the XOR operation is not defined on the set \{A, \ldots, Z\}, we replace it here during encryption with modulo-26 addition (e.g., \( C \oplus D = F \) and \( Y \oplus C = A \)).

(i) Decrypt the following ciphertexts, which were encrypted using

(A) Electronic codebook mode: UOMHDJT  [2 marks]

(B) Cipher feedback mode: RVPHTUH  [4 marks]

(C) Output feedback mode: LNMSUUY  [4 marks]

(ii) Determine the CBC-MAC for the message TRIPOS.  [4 marks]

(b) Consider another small pseudo-random permutation, this time defined over the set of decimal digits \{0, 1, 2, \ldots, 9\}, using modulo-10 addition instead of XOR (e.g., \( 7 \oplus 3 = 0 \)).

(i) You have intercepted the message 100 with appended CBC-MAC block 4. The message represents an amount of money to be paid to you and can be of variable length. Use this information to generate a message that represents a much larger number, and provide a valid CBC-MAC digit, without knowing the pseudo-random permutation or key that the recipient will use to verify it.  [4 marks]

(ii) What mistake did the designer of the communication system attacked in part (b)(i) make (leaving aside the tiny block size), and how can this be fixed?  [2 marks]