**Mock Exam – As part of the seen exam pilot - for weeks 7 – 12**

**5.** a) Explain the difference between Symmetric cipher and a-Symmetric cipher. [4]

b) Use symmetric ciphers to encrypt message “security” and decrypt message “DVLMNWZ”

[15]

The representation of characters in modulo 26 is described as follows:

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext → | 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 |
| Ciphertext → | 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 |
| Value → | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

The mathematical equations for encryption and decryption can be described as follows:

$$\text{Encryption } E_{(k)} : i \; ! \quad i + k \bmod 26$$

$$\text{Decryption } D_{(k)} : i \; ! \quad i - k \bmod 26$$

*i* represents the messages (plaintext or cipher), k represents a symmetric key. In this case k=12.

c) The message is placed row-wise in a 2D array (in this case 3x5 matrix) starting at top left. The encrypted message is read out column-wise starting at the bottom right. Write down plaintext and encrypted messages. [6]

| | | | | |
|---|---|---|---|---|
| D | E | F | A | C |
| | T | | O | S |
| T | A | N | | D |