Question 2

A digital solutions team is tasked with implementing a Vigenère Cipher for secure message encryption.

a) Develop an algorithm in pseudocode, to encrypt a plaintext message with a given keyword using the Vigenère Cipher. [12 marks]

b) Desk test your algorithm using:
    a. Plaintext – digital
    b. Key – dog [8 marks]

Question 2 Marking Guide

#	Category	Response	Mark
A	Logical Correctness	Accepts user input for plaintext and key	1
		Converts both to uppercase	1
		Correctly extends the keyword to match plaintext length.	1
		Encrypts plaintext using `(plainValue + keyValue) MOD 26`	1
		Outputs the ciphertext	1
	Pseudocode has example of	Assignment	1
		Condition	1
		Selection	1
		Iteration	1
		Modularisation	1
	Pseudocode syntax (choose one)	*No pseudocode errors*	*2*
		Pseudocode with one error	*1*
		Pseudocode with more than one error	*0*
B	Correct algorithm	Produce the correct encrypted text (JWMLHGO)	2
	Desk Check Process *(Choose one)*	*Complete desk check showing each step of the encryption;*	*6*
		Complete desk check with one error	*5*
		Complete desk check with two errors	*4*
		Complete desk check with three errors	*3*
		Complete desk check with four errors	*2*
		Complete desk check with five errors	*1*
		Complete desk check with more than five errors	*0*

Sample answer

```
FUNCTION GenerateExtendedKeyword(plaintextMessage, keyword)
    extendedKeyword = ""
    keywordIndex = 0
    FOR messageIndex = 0 TO LENGTH(plaintextMessage) - 1
        extendedKeyword = extendedKeyword & keyword[keywordIndex]
        keywordIndex = keywordIndex + 1
        IF keywordIndex = LENGTH(keyword) THEN
            keywordIndex = 0
        END IF
    END FOR
    RETURN extendedKeyword
END FUNCTION


FUNCTION EncryptVigenere(plaintextMessage, keyword)
    plaintextMessage = UPPER(plaintextMessage)
    keyword = UPPER(keyword)
    extendedKeyword = GenerateExtendedKeyword(plaintextMessage, keyword)

    encryptedMessage = ""
    FOR messageIndex = 0 TO LENGTH(plaintextMessage) - 1
        plainValue = POSITION(plaintextMessage[messageIndex])   # A=0 … Z=25
        keyValue = POSITION(extendedKeyword[messageIndex])
        cipherValue = (plainValue + keyValue) MOD 26
        encryptedMessage = encryptedMessage & LETTER(cipherValue)
    END FOR

    RETURN encryptedMessage
END FUNCTION


# Main program
INPUT "Enter the plaintext message:" -> plaintextMessage
INPUT "Enter the keyword:" -> keyword
ciphertext = EncryptVigenere(plaintextMessage, keyword)
OUTPUT "Ciphertext: ", ciphertext
```

Line	plaintextMessage	keyword	extendedKeyword	keywordIndex	messageIndex	plainValue	keyValue	cipherValue	encryptedMessage	Output
1	digital									"digital"
2	digital	dog								"dog"
3	DIGITAL	dog								
4	DIGITAL	DOG								
5	DIGITAL	DOG								
6	DIGITAL	DOG		0						
8	DIGITAL	DOG	D	1	0					
8	DIGITAL	DOG	DO	2	1					
9	DIGITAL	DOG	DOG	0	2					
8	DIGITAL	DOG	DOGD	1	3					
8	DIGITAL	DOG	DOGDO	2	4					
9	DIGITAL	DOG	DOGDOG	0	5					
8	DIGITAL	DOG	DOGDOGD	1	6					
14	DIGITAL	DOG	DOGDOGD							
16	DIGITAL	DOG	DOGDOGD		0	3 (D)	3 (D)	6	J	
16	DIGITAL	DOG	DOGDOGD		1	8 (I)	14 (O)	22	JW	
16	DIGITAL	DOG	DOGDOGD		2	6 (G)	6 (G)	12	JWM	
16	DIGITAL	DOG	DOGDOGD		3	8 (I)	3 (D)	11	JWML	
16	DIGITAL	DOG	DOGDOGD		4	19 (T)	14 (O)	7	JWMLH	
16	DIGITAL	DOG	DOGDOGD		5	0 (A)	6 (G)	6	JWMLHG	
16	DIGITAL	DOG	DOGDOGD		6	11 (L)	3 (D)	14	JWMLHGO	
21	DIGITAL	DOG	DOGDOGD						JWMLHGO	JWMLHGO