Algorithms and Pseudocode Extended

Question 1

A team of software developers is tasked with creating a secure messaging system for a private organisation. They decide to implement the Vigenère cipher, which was historically considered unbreakable for centuries, as a foundational encryption layer for internal communications.

a) Develop a comprehensive pseudocode algorithm for an encrypt_vigenere function that takes plaintext (string) and a keyword (string) as inputs. (9 marks)

b) Explain **two key characteristics** of the Vigenère cipher that contributed to its historical strength compared to simpler ciphers like the Caesar cipher. Despite these strengths, critically evaluate **one primary weakness** of the Vigenère cipher that makes it easily breakable by modern standards, explaining the technique used to exploit this weakness. (6 marks)

Question 1 Marking Guide

Part	Marks	Criteria	Evidence of achievement
A	1	Input handling and setup	Defines function with plaintext and keyword inputs. Converts both inputs to uppercase.
	1	Keyword repetition logic	Correctly repeats keyword to match plaintext length using index or modulo arithmetic.
	1	Shift value calculation	Calculates alphabet position of keyword character (A=0 … Z=25).
	1	Modular arithmetic	Applies (plaintext_position + shift) MOD 26 to find new position.
	1	Encryption step	Maps new position back to correct character (wraparound handled).
	1	Output construction	Sequentially adds encrypted characters to ciphertext string.
	1	Return statement	Returns completed ciphertext.
	1	Case handling	Preserves consistent case (all uppercase as specified).
	1	Non-letter handling	Leaves non-letter characters unchanged in ciphertext.
B	1	First characteristic of strength	Explains polyalphabetic substitution or variable shifts resisting simple frequency analysis.
	1	Second characteristic of strength	Explains another strength such as longer keyword increasing complexity.
	1	Contrast with Caesar	Explicitly contrasts strengths of Vigenère with Caesar cipher.
	1	Identification of weakness	Identifies repetition of keyword as a weakness.
	1	Attack technique	Names the Kasiski examination or Friedman test as method of breaking cipher.
	1	Explanation of breakability	Explains how repeating patterns allow frequency analysis once key length is known.

Sample Response

Part A

```
FUNCTION EncryptVigenere(plaintext AS STRING, keyword AS STRING) RETURNS STRING

    DECLARE ciphertext AS STRING = ""
    DECLARE keyIndex AS INTEGER = 0
    DECLARE keyLength AS INTEGER = LENGTH(keyword)

    FOR i FROM 0 TO LENGTH(plaintext) - 1
        DECLARE char AS CHARACTER = plaintext[i]

        IF IsLetter(char) THEN
            DECLARE keyChar AS CHARACTER = keyword[keyIndex MOD keyLength]
            DECLARE shift AS INTEGER = (ORD(Uppercase(keyChar)) - ORD('A'))

            IF IsUppercase(char) THEN
                DECLARE base AS INTEGER = ORD('A')
            ELSE
                DECLARE base AS INTEGER = ORD('a')
            END IF

            DECLARE encryptedChar AS CHARACTER =
                CHR( ( (ORD(char) - base + shift) MOD 26 ) + base )

            ciphertext = ciphertext + encryptedChar

            keyIndex = keyIndex + 1
        ELSE
            ciphertext = ciphertext + char
        END IF
    END FOR

    RETURN ciphertext
END FUNCTION
```

Part B

Two key characteristics that made the Vigenère cipher historically strong are:

- **Polyalphabetic substitution**: Instead of using a single shift like the Caesar cipher, the Vigenère cipher applies different shifts depending on the keyword. This disguises the frequency of letters, making simple frequency analysis much harder.
- **Keyword length**: A longer keyword increases the variation in shifts across the plaintext. This reduces obvious repeating patterns and makes brute-force guessing of the key far more complex than a Caesar cipher.

Despite these strengths, the cipher has a major weakness: **the keyword repeats**. This repetition introduces periodic patterns into the ciphertext. Modern cryptanalysts exploit this using methods like the **Kasiski examination** or the **Friedman test**. These techniques identify repeated sequences in the ciphertext, estimate the key length, and then apply frequency analysis to each segment. This process allows the keyword to be reconstructed and the entire message to be decrypted.