TEAM OUROBOROS

CLOCK – V SCHEME

Prepared By:

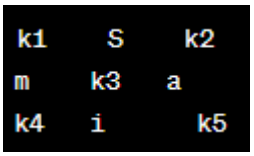
Hamza Ahmed Khan	CT-20035
Saim Ahmed	CT-20019
Muhammad Abdul Rafay	CT-20050
Muhammad Arqam Khursheed	CT-20018

Overview:

The code defines a function encrypt_decrypt that takes a plaintext and keys (k1 to k5) as input and performs encryption or decryption based on user choice. The encryption process involves dividing the plaintext into chunks of 4 characters, mapping characters to their corresponding integer values, and applying the specified operations for each character in the chunk. The main program takes user input for encryption or decryption, keys, and plaintext or ciphertext.

1. Scheme Requirements:

1.1 Matrix Layout:



1.2 Encryption Process:

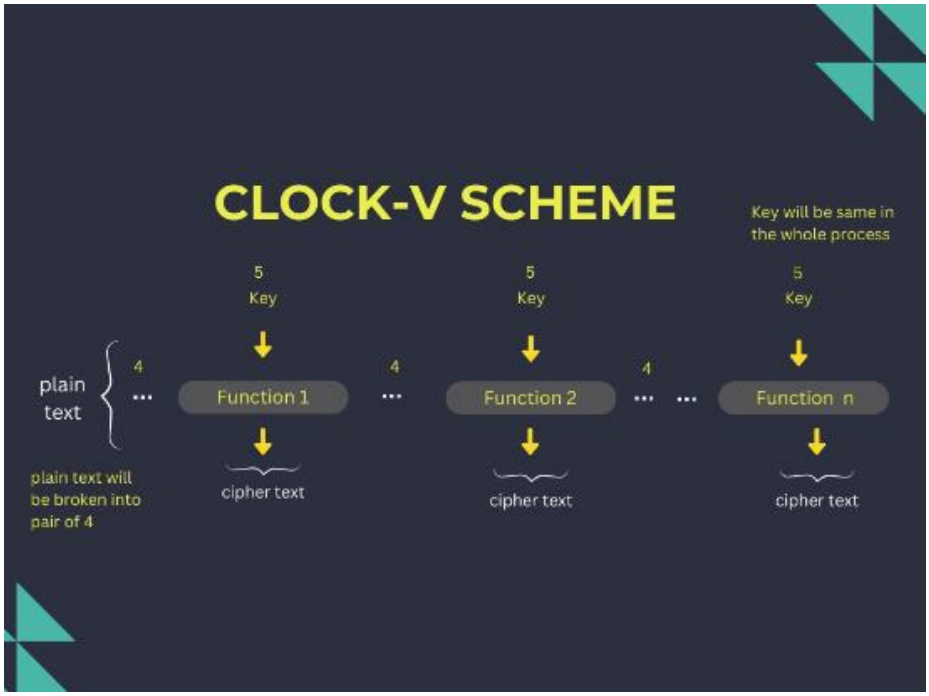
For each character in a 4-character chunk:
Multiply k3 with k1 for the first character, k3 with k2 for the second character, k3 with k5 for the third character, and k3 with k4 for the fourth character.
Subtract the character value (mapped from 'a' to 0) from the result.
If the result is negative, adjust it to a positive value.
Apply modulo 26 to keep the result within the alphabet range.
Map the result back to characters ('a' to 'z').

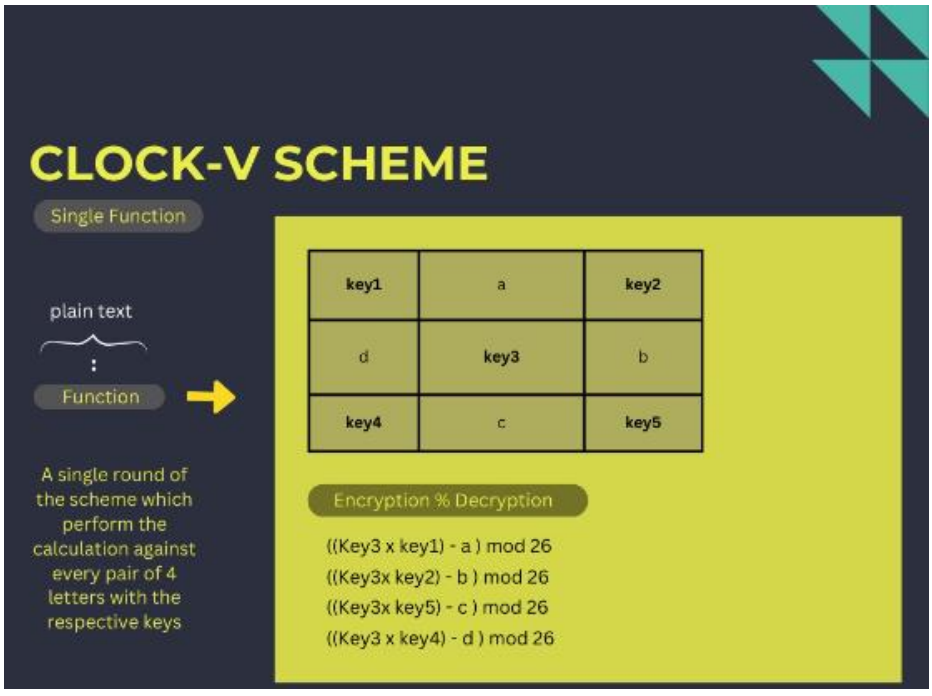
1.3 Sample Key:

plaintext: saim ahmed

Encrypted text: eybdwrxlthsy

FLOWCHART


CLOCK-V SCHEME
Key will be same in the whole process
5
Key
5
Key
5
Key
plain text
4
4
4
Function 1
Function 2
Function n
plain text will be broken into pair of 4
cipher text
cipher text
cipher text


CLOCK-V SCHEME
Single Function
plain text
Function
key1
a
key2
d
key3
b
key4
c
key5
A single round of the scheme which perform the calculation against every pair of 4 letters with the respective keys
Encryption % Decryption
((Key3 x key1) - a) mod 26
((Key3x key2) - b) mod 26
((Key3x key5) - c) mod 26
((Key3 x key4) - d) mod 26