encryption

For this question, we consider a cipher working on an alphabet consisting of 26 English characters (A-Z), plus underscore (_), comma (,) and full stop (.), which corresponds to integers 0 to 28. The encryption is done by:

$$c = E_2(E_1(p))$$

Here E_1 is the encryption function used in Hill cipher. The plaintext is processed successively in blocks of size m. The encryption algorithm takes a block with m plaintext digits $(p_1, p_2, \ldots, p_m)$ and transforms into a cipher block of size m $(c_1, c_2, \ldots, c_m)$ using a key matrix of size *m* × *m* by the linear transformation, which is given by:

$$\begin{gathered} c_1 = (k_{1,1}p_1 + k_{1,2}p_2 + \cdots + k_{1,m}p_m) \bmod 29 \\ c_2 = (k_{2,1}p_1 + k_{2,2}p_2 + \cdots + k_{2,m}p_m) \bmod 29 \\ \cdots \\ c_m = (k_{m,1}p_1 + k_{m,2}p_2 + \cdots + k_{m,m}p_m) \bmod 29 \end{gathered}$$

E_2 is the encryption function used in Vernam cipher. It processes a block of plaintext at a time, and produces a same length ciphertext. In this task, our Vernam cipher uses the same block size *m* as used in Hill cipher. The encryption is performed by:

$$\begin{gathered} c_1 = p_1 + K_1 \bmod 29 \\ c_2 = p_2 + K_2 \bmod 29 \\ \cdots \\ c_m = p_m + K_m \bmod 29 \end{gathered}$$

Note: For this question, correspondence between plaintext and number modulo

29 are as follows *"A"* ↔ 0, *"B"* ↔ 1, *"C"* ↔ 2, . . . , *"Z"* ↔ 25, *" "* ↔ 26, *", "* ↔ 27 and *"."* ↔ 28. All following tasks use block size *m* = 5.

leak

For the encryption above $c = E_2(E_1(p))$, we got one plaintext and its ciphertext:

p = ZQIUOMCEFZGVRGTBAAAAAJRTKENSNQ
c = WUJQYGCAHAAAAAGDPQXUXHIDTDLIRG

challenge

C = OKCZKNCSQ_ULYOKPKW,PL.UXIWX,YCLXZFGBM_SUJLSCOXZT.AIGFZRDCIX,

Please recover the secret from C, and the flag format is flag{secret}.

attention

The arrangement of the plaintext matrix is row first.