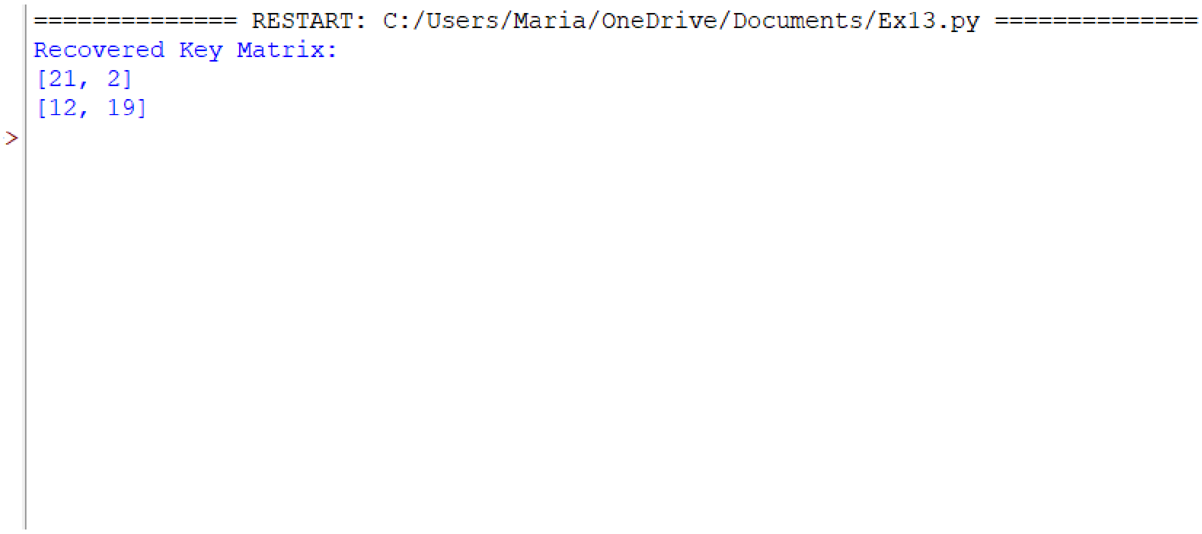
13. Write a C program for Hill cipher succumbs to a known plaintext attack if sufficient plaintext ciphertext pairs are provided. It is even easier to solve the Hill cipher if a chosen plaintext attack can be mounted. 13. Write a C program for Hill cipher succumbs to a known plaintext attack if sufficient plaintext ciphertext pairs are provided. It is even easier to solve the Hill cipher if a chosen plaintext attack can be mounted.

Code:

```
# Convert letters A-Z to numbers 0-25

def n(c):

  return ord(c) - 65

def mod_inv(a):

    for i in range(26):

        if (a * i) % 26 == 1:

            return i

    return None

# Known plaintext and ciphertext (4 letters = 2 blocks of size 2)

P = "HELP"

C = "ZEBB"

# Build matrices

p = [[n(P[0]), n(P[2])],

     [n(P[1]), n(P[3])]]

c = [[n(C[0]), n(C[2])],

     [n(C[1]), n(C[3])]]

# Invert plaintext matrix

det = (p[0][0]*p[1][1] - p[0][1]*p[1][0]) % 26

inv_det = mod_inv(det)

pi = [

    [( p[1][1] * inv_det) % 26, (-p[0][1] * inv_det) % 26],

    [(-p[1][0] * inv_det) % 26, ( p[0][0] * inv_det) % 26]

]
```

```
# Compute key = C * P^-1  (mod 26)
K = [
    [(c[0][0]*pi[0][0] + c[0][1]*pi[1][0]) % 26,
     (c[0][0]*pi[0][1] + c[0][1]*pi[1][1]) % 26],
  [(c[1][0]*pi[0][0] + c[1][1]*pi[1][0]) % 26,
     (c[1][0]*pi[0][1] + c[1][1]*pi[1][1]) % 26]
]
print("Recovered Key Matrix:")
for row in K:
    print(row)
```



```
============== RESTART: C:/Users/Maria/OneDrive/Documents/Ex13.py ==============
Recovered Key Matrix:
[21, 2]
[12, 19]
>
```