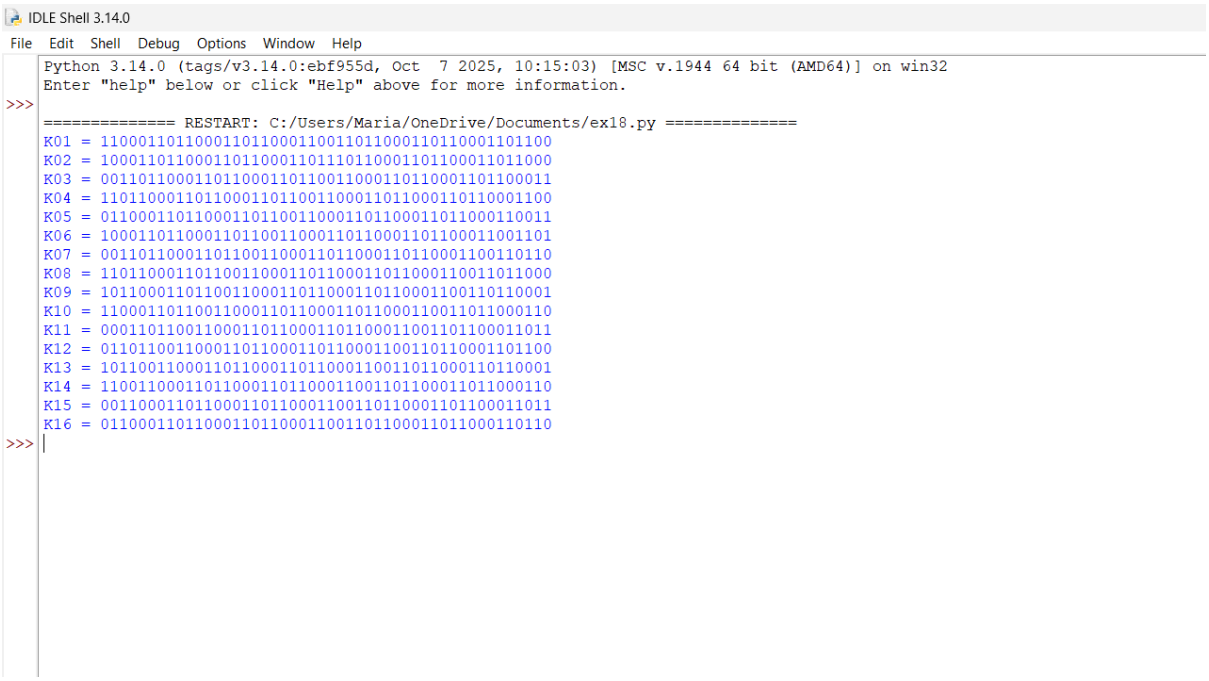
18. Write a python program for DES the first 24 bits of each subkey come from the same subset of 28 bits of the initial key and that the second 24 bits of each subkey come from a disjoint subset of 28 bits of the initial key.

Code:

```
# DES Key Scheduling Demo

# Each subkey = 24 bits from C + 24 bits from D (disjoint halves)

shifts = [1,1,2,2,2,2,2,2, 1,2,2,2,2,2,2,1]

def left_shift(b, n):

   return b[n:] + b[:n]

def generate_subkeys(key56):

   C = key56[:28]     # first 28 bits

   D = key56[28:]     # last 28 bits

   subkeys = []

for s in shifts:

       C = left_shift(C, s)

       D = left_shift(D, s)

  # FIRST 24 bits from C (subset of its 28 bits)

       # SECOND 24 bits from D (subset of its 28 bits)

       K = C[:24] + D[:24}]

 subkeys.append(K)

   return subkeys

   # Example 56-bit key

key = "01100011011000110110001101100011011000110110001101100011"

keys = generate_subkeys(key)

for i, k in enumerate(keys, 1):

   print(f"K{i:02d} = {k}")
```


IDLE Shell 3.14.0
File Edit Shell Debug Options Window Help
Python 3.14.0 (tags/v3.14.0:ebf955d, Oct 7 2025, 10:15:03) [MSC v.1944 64 bit (AMD64)] on win32
Enter "help" below or click "Help" above for more information.
>>>
========== RESTART: C:/Users/Maria/OneDrive/Documents/ex18.py ==========
K01 = 110001101100011011000110011011000110110001101100
K02 = 100011011000110110001101110110001101100011011000
K03 = 001101100011011000110110011000110110001101100011
K04 = 110110001101100011011001100011011000110110001100
K05 = 011000110110001101100110001101100011011000110011
K06 = 100011011000110110011000110110001101100011001101
K07 = 001101100011011001100011011000110110001100110110
K08 = 110110001101100110001101100011011000110011011000
K09 = 101100011011001100011011000110110001100110110001
K10 = 110001101100110001101100011011000110011011000110
K11 = 000110110011000110110001101100011001101100011011
K12 = 011011001100011011000110110001100110110001101100
K13 = 101100110001101100011011000110011011000110110001
K14 = 110011000110110001101100011001101100011011000110
K15 = 001100011011000110110001100110110001101100011011
K16 = 011000110110001101100011001101100011011000110110
>>>