**COMSAT UNIVERSITY ISLAMABAD ATTOCK CAMPUS**

****

**INFORMATION SECURITY**

**NAME:** MENAHIL NOOR

**REGISTRATION NO:** SP24-BSE-035

**LAB TASK**

**SUBMITTED TO:** Ms. AMBAREEN GUL

**DEPARTMENT:** SOFTWARE ENGINEERING

**DATE:** 14th October 2025

**Lab work (as on page 58 of lab manual)**

**Task 1**

Perform following tasks for following Transposition Cipher code.

(Alphabet Number \* key) mod (total number of alphabets

def split\_len(seq, length):

return [seq[i:i + length] for i in range(0, len(seq), length)]

def encode(key, plaintext):

order = {

int(val): num for num, val in enumerate(key)

}

ciphertext = ''

for index in sorted(order.keys()):

for part in split\_len(plaintext, len(key)):

try:

ciphertext += part[order[index]]

except IndexError:

pass

return ciphertext

print(encode('3214', 'HELLO'))

**1) Handle Different Key Sizes**

Modify the encode function to handle cases where the length of the key is not equal to the length of the plaintext. Task: Add padding to the plaintext when it is shorter than the key.

**2) Decode Function**

Create a decode function that reverses the encode process. Task: Write a function decode(key, ciphertext) that deciphers the encrypted message and returns the original plaintext.

**3) Support for Uppercase and Lowercase Letters**

Modify the code to preserve the original case (uppercase and lowercase letters) in the **plaintext.**

**Task 2**: Adjust the encode function to handle both uppercase and lowercase letters, so it doesn’t always convert to lowercase.

**4) Encrypt Full Sentences with Spaces**

Modify the encode function to handle spaces and punctuation without removing them.

Task: Ensure that spaces and punctuation are preserved and not encrypted when encoding full sentences.

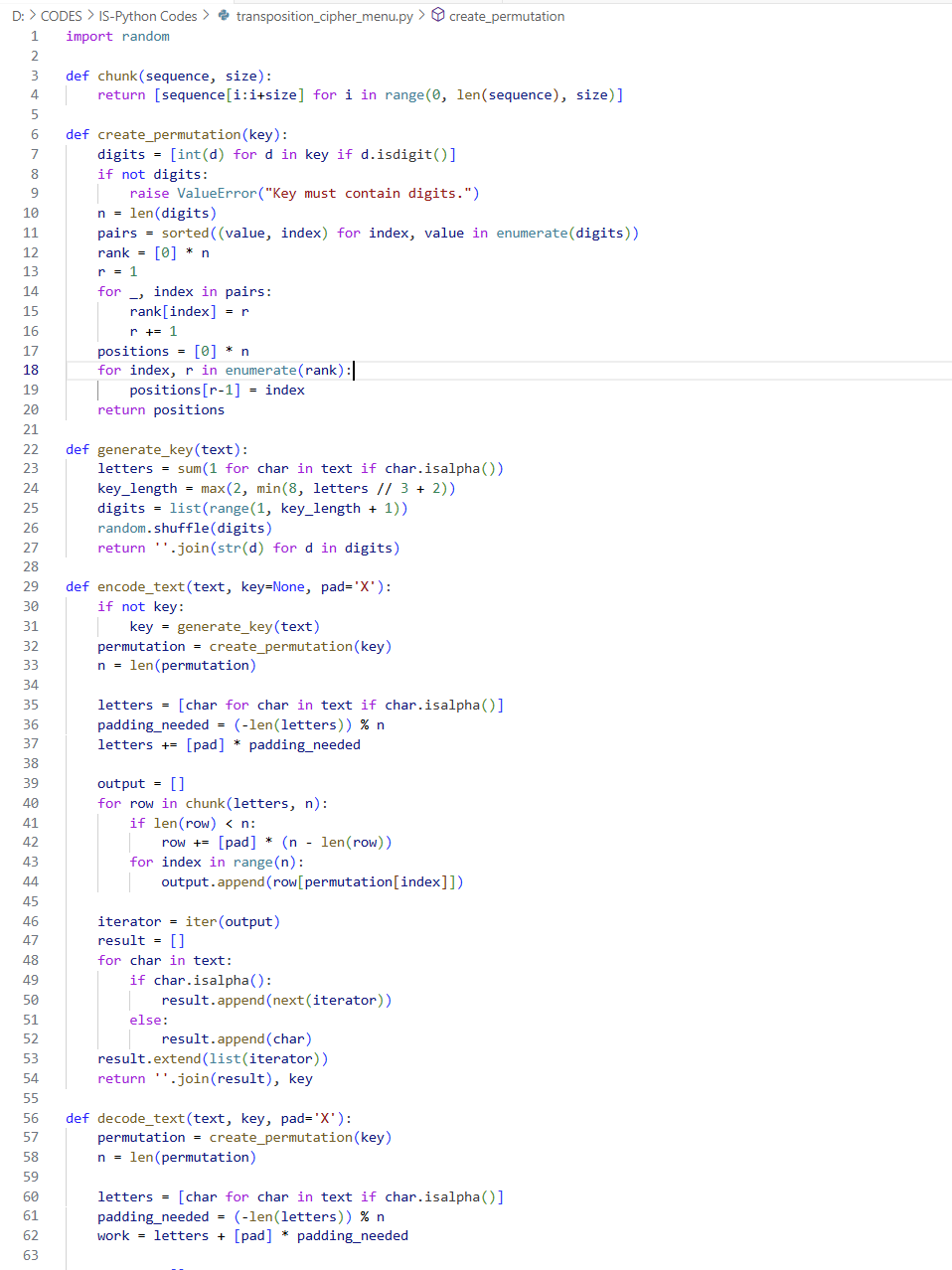
**5) Dynamic Key Generation**

Automatically generate a random key if the user does not provide one. Task: Write a function that generates a random key based on the length of the plaintext.

**6) Add a Menu Interface**

Create a simple command-line interface where the user can choose to encode or decode a message. Task: Write a menu system where the user can input a choice to either encode, decode, or exit.

**Solution Code:**



A screenshot of a computer program

AI-generated content may be incorrect.

**Output Code:**

**A screenshot of a computer code

AI-generated content may be incorrect.**

**Explanation: Columnar Transposition**

* **Transposition** ciphers hide messages by **reordering** characters (no letter substitutions).
* **Columnar method:** a numeric key defines a **permutation** (column read order).
* **Encrypt:** take letters, place in rows with columns = key length, **pad** with X to fill last row, read columns by key order. If preserving text format, only shuffle **letters**; keep **spaces/punctuation** and **case** unchanged.
* **Decode:** use the same permutation to place letters back into their columns/rows, merge into the original text layout, then **strip padding**.
* **Keys:** classic keys are a permutation of **1..n** (no repeats). To accept **any digits**, convert digits to **ranks** (ties left-to-right) → valid permutation.
* **Dynamic key:** if none provided, **generate** a random key length (e.g., 2–8) and shuffle.
* **Security:** simple and educational, but **not secure** by modern standards.