Lab 3 (29/12/2025)

QUESTION 1 – Polyalphabetic Cipher (Vigenère Cipher)

Problem Statement

Implement the **Vigenère Cipher encryption** (a polyalphabetic substitution cipher) with the following constraints:

1. Key should be **case-insensitive**
2. Ignore **spaces and special characters** in plaintext
3. Key should be **repeated cyclically** to match plaintext length
4. Plaintext and key should be treated as **uppercase**
5. Mapping rule:

   $$C = (P + K) \bmod 26$$

Sample Input

```
Plaintext : ATTACK AT DAWN!
Key       : LEMON
```

Processing (Hidden from Students)

```
Plaintext : ATTACKATDAWN
Key       : LEMONLEMONLE
```

Sample Output

```
Ciphertext : LXFOPVEFRNHR
```

QUESTION 2 – Columnar Transposition Cipher (Encryption)

Problem Statement

Write a program to implement **Columnar Transposition Cipher encryption** using a keyword.

The program should:

1. Remove spaces from plaintext
2. Arrange plaintext in rows based on key length
3. Pad empty cells with **X**
4. Rearrange columns based on **alphabetical order of key**
5. Read columns top-to-bottom to generate ciphertext

Sample Input

```
Plaintext : MEET ME TOMORROW
Key       : ZEBRA
```

Matrix Formation

```
Z E B R A
5 3 2 4 1   ← Column order

M E E T M
E T O M O
R R O W X
```

Sample Output

```
Ciphertext : MEOERXETRMTOW
```

QUESTION 3 – Combined Cipher (Vigenère + Rail Fence Transposition)

Problem Statement

Encrypt a message using:

1. **Vigenère Cipher** first
2. Then apply **Rail Fence Transposition Cipher (2 rails)**

Sample Input

```
Plaintext : SECURITY
Key       : KEY
Number of Rails : 2
```

Step 1: Vigenère Encryption

```
Plaintext : SECURITY
Key       : KEYKEYKE
Cipher    : CIEYVVMC
```

Step 2: Rail Fence (2 Rails)

```
Rail 1 : C E V M
Rail 2 : I Y V C
```

Sample Output

```
Final Ciphertext : CEVMIYVC
```
