Q7. Cipher Algorithm (40 marks)

A **cipher algorithm** is a mathematical formula designed specifically to obscure the value and content of the data so that unintended recipients cannot understand it. In this question, you are required to write a program which is able to use a given keyword to encrypt an original string to an encrypted string, or, decrypt an encrypted string back to the original string by using the same keyword.

The encryption principle is explained as follows.

(1) First of all, each alphabet is corresponding to a number by referring to the following table.

Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Number	0	1	2	3	4	5	6	7	8	9	10	11	12
Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number	13	14	15	16	17	18	19	20	21	22	23	24	25

(2) The system will then be given an original string and a keyword with different lengths.

(3) To encrypt the original string, the keyword will be repeated indefinitely until the keyword string has the same length as that of the original string, so that there is a one-to-one correspondence between the original string and the keyword string

(4) Then, at each position in the strings, the number of the original character is added to the number of the corresponding keyword character.

(5) The sum from (4) will then be divided by 26 in order to get the modulo (i.e., remainder). With this modulo number, the encrypted character can then be obtained.

For example, if the string is "HOWAREYOUTODAY", the keyword is "IMFINE". The encrypted string will be "PABIEIGAZBBBHIK" based on the following table.

Original String	H	O	W	A	R	E	Y	O	U	T	O	D	A	Y
Keyword String	I	M	F	I	N	E	I	M	F	I	N	E	I	M
Encrypted String	P	A	B	I	E	I	G	A	Z	B	B	H	I	K

Please note that in the second row of the above table, the keyword is repeated until the keyword string has the same length as that of the original string.

Then each encrypted character is obtained by adding the number of the original character and the number of the corresponding keyword character. If the sum exceeds 26, then the sum will be substracted by 26 in order to get the encrypted character.

For example, the 1st alphabet from the original string is "H", which corresponds to number 7, and the 1st alphabet from the keyword string is "I", which corresponds to number 8. The sum of 7 and 8 is 15, which results in the encrypted alphabet "P".

For another example, with reference to the 10th column of the above table, alphabet “T” from the original string corresponds to number 19, and alphabet “I” from the keyword string corresponds to number 8. When 19 and 8 are added, the sum is 27. Since there is no number 27 in the table, it should be subtracted by 26, resulting in number 1, which is corresponding to the alphabet “B”.

Write a program to

Input three lines as described below.

The first line is the string to be encrypted or decrypted.

The second line is the keyword to be used for encryption and decryption.

The third line is a single alphabet, either “E” or “D”. If it is an “E”, the programme needs to encrypt the string given in the first line by using the keyword in the second line. However, if it is a “D”, the programme needs to decrypt the string in the first line by using the keyword in the second line.

Note: The inputs in the first and second lines are limited to the alphabets in uppercase, each line contains maximum up to 20 alphabets.

Output the encrypted/decrypted string for the string given in the first line, by using the keyword as instructed. If any of the input strings is more than 20 alphabets, or contains undefined character(s)/symbol(s), or the single alphabet in the third line is neither “E” nor “D”, then output “Invalid Input”.

试题 7. 密码算法（40 分）：

密码算法是一种专门设计来隐蔽数据价值和内容的数学公式，以阻止非预期的接收者读取数据里面的信息。 在这个试题中，你需要编写一个程式，以使用给定的关键词对一组原始字符串进行加密，或，使用相同的关键词将已加密的字符串进行解密。

以下是加密原理的解释。

(1) 首先，参照下表，每个字母对应了一个数字。

字母	A	B	C	D	E	F	G	H	I	J	K	L	M
数字	0	1	2	3	4	5	6	7	8	9	10	11	12
字母	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
数字	13	14	15	16	17	18	19	20	21	22	23	24	25

(2) 之后，系统会接收到一个原始字符串和一个不同长度的关键词。

(3) 为了对原始字符串进行加密，关键词可无限重复以延申成另一个字符串。其中条件是，关键词字符串的长度必须与原始字符串的长度相同，以使得两字符串可以一对一的对应。

(4) 然后在相同位置上，计算原始字符和关键词字符对应的数字之和。

(5) 将步骤(4)所得的和除以 26， 可得其模数（即余数）。此模数对应到的字符即为加密字符。

例如，如果原始字符串是“HOWAREYOUTODAY”，同时关键词是“IMFINE”。 根据下表，加密字符串将是“PABIIEIGAZBBBHIK”。

原始字符串	H	O	W	A	R	E	Y	O	U	T	O	D	A	Y
关键词字符串	I	M	F	I	N	E	I	M	F	I	N	E	I	M
加密字符串	P	A	B	I	E	I	G	A	Z	B	B	H	I	K

请注意，在上表的第二行中，关键词是重复的，直到关键词字符串的长度与原始字符串的长度相同。

然后通过将原始字符对应的数字和同位置上关键词字符对应的数字相加，则可得到该位置上加密字符对应的数字。 如果上述的和超过 26，则将其减去 26 以获得加密字符对应的数字。

例如，原始字符串的第一个字母是“H”，对应数字为 7；关键词字符串的第一个字母是“I”，对应数字为 8。把 7 和 8 相加，其和为 15，而 15 即可求得对应的加密字母“P”。

又如，参考上表第 10 列，原始字符串中的字母“T”对应数字为 19，关键词字符串中的字母“I”对应数字为 8。把 19 和 8 相加，其和为 27。由于表中没有数字 27，所以要减去 26，得到数字 1，则对应到的加密字母为“B”。

试写一程式以

依序输入，如下所述的三行：

第一行是要被加密或被解密的字符串。

第二行是用于加密和解密的关键词。

第三行是一个字母，“E”或“D”。 如果是“E”，则程式需要使用第二行的关键词对第一行的字符串进行加密。 但如果是“D”，则程式需要使用第二行中的关键词来解密第一行的字符串。

注意：第一行和第二行的输入仅限于大写字母，且每一行字符串最多只有 20 个字母。

输出，经过加密/解密处理后的字符串。必须注意的是，如果输入的字符串超过 20 个字母，或包含未定义的字符/符号，或第三行的单个字母不是“E”或“D”，则输出“Invalid Input”。

Test Cases:

Input (输入)	**Output (输出)**
HELLOWORLD GOOD E	NSZOUKCURR
RSVYCAQEYMSVBEQ YES D	TODAYISAGOODDAY
LETSSTARTTOCODE OKA* E	Invalid Input
IMHAPPYTODAY WHY E	ETFWWNUAMZHW
HSVVPHCIMSNX LOVE D	WEARETHEBEST
ABCDEFGHIJKLMNOPQRSTUVWXYZ HAPPY D	Invalid Input
GOODBYESEEYOU SURE K	Invalid Input
F E D	B