

# 12 Sometimes, older is better

4 points

## Introduction

At HP, a group of engineers in Sant Cugat is collaborating with a group of engineers in San Diego to design and develop a new printing product, completely revolutionary for the world-wide industry. The company CEO, who is located in Silicon Valley, is very interested in this new product and has committed a large part of the company's budget to complete it within the upcoming year.

However, the CEO is concerned about the secrecy of the project, since all the e-mails between Sant Cugat and San Diego are transmitted over the Internet in plain text and, thus, could be intercepted by a third party and used against HP. Since he does not know much about cryptography, he has asked you to implement a simple mechanism to cypher all the communications between Engineers in both places. After some research, and given the lack of time due to the tight schedule of the project, you have decided to implement one of the first and simplest cypher mechanisms: the Caesar algorithm. This cypher algorithm is named after Roman emperor Julius Caesar, who used it for communicating his military secrets to his generals deployed in the field and, perhaps, also for sending his love letters to Cleopatra. Your task is to implement a program that is able to decrypt messages that have been cyphered using the Caesar algorithm. The idea behind the Caesar algorithm is simple. Each letter of the original text is substituted by another, following these rules:

- find the letter (which should be encrypted) in the English alphabet
- move K positions further down (the alphabet)
- take the new letter from here
- if "shifting" goes beyond the end of the table, continue from A

For example, if  $K = 3$  (shift value used by Caesar himself), then A becomes D, B becomes E, W becomes Z and Z becomes C and so on, according to the following table:

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

So if the source message was VENI VIDI VICI then after encoding it becomes YHQL YLGL YLFL.

To decrypt a message each letter has to be "shifted back" to decode it - or shifted by  $26-K$ . So if we have encoded message HYHQ BRX EUXWXV, we can apply shift of  $26 - K = 26 - 3 = 23$  and find the original text to be EVEN YOU BRUTUS.

## Input

The first line of the input data will contain two integers separated by a space; the number of lines of encrypted text to be processed and the value of K, that is, the positions that the alphabet has to be shifted to encrypt/decrypt the message.

The following lines will contain encrypted text, consisting of capital Latin letters A ... Z. Each line will be terminated with a dot which should not be decoded.

```
1 3
YHQL YLGL YLFL.
```

## Output

Your answer should contain the decrypted message (in a single line, no line splitting needed) and the final dot in the encrypted message.

```
VENI VIDI VICI.
```

