# Vigener cipher

# CPSPC 2010 Prague, Day 1.

| Submit: | vigener.c / vigener.cpp / vigener.pas | Time limit:   | $5 \mathrm{s}$   |
|---------|---------------------------------------|---------------|------------------|
| Input:  | stdin                                 | Memory limit: | $64 \mathrm{MB}$ |
| Output: | stdout                                | Points:       | 100              |

Probably everyone have heard about so called Vigener cipher. This cipher adds cyclically repeated key to the original text. The key is added as follows – let us assume that  $A = 0, B = 1, C = 2 \dots Z = 25$ . Then we just sum the letter of the original text and the letter of the key modulo 26. For example for the text CPSPCISANABBREVIATION and the key CPSPC we obtain encypted message EEKEEKHSCCDQJTXKPLXQP (see figure).

| С | Ρ | S | Ρ | С | С | Ρ | S | Ρ | С | С | Ρ | S | Ρ | С | С | Ρ | S | Ρ | С | С |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| С | Ρ | S | Ρ | С | I | S | A | Ν | A | В | В | R | Е | V | I | A | Т |   | 0 | Ν |
| Ε | Е | Κ | Е | Е | K | Η | S | С | С | D | Q | J | Т | Х | K | Ρ | L | Х | Q | Ρ |

Your task will be to try to decode the encrypted text, assuming that you know the table of the frequences of all pairs of letters in the language of the encrypted text and the length of the key. Such analyze gives surprisingly good results.

## Task:

You will get the encrypted text without spaces, which was encrypted by the Vigener cipher with the key of the length K. In addition you will get the table of the frequences of all pairs of letters of the language of the original text. Find such key (which does not have to be unique), for which the decoded text reaches the maximal sum of the frequences of the pairs of letters.

#### Input:

On the first line of the input there are two natural numbers K ( $K \leq 5000$ ) and N, where K denotes the length of the key and N denotes the number of the pairs of letters whose frequence is known. Then there follows N lines every containing two upper case of the english alphabet followed by one space and one integer F ( $F \leq 10^8$ ), which is the value of the frequence of this pair of letters. If the pair is omitted, its frequency is considered to be a zero. This frequence is always positive integer. It holds that the higher the frequence is, the higher the probability of the occurrence of that pair is. On the last line of the input, there is the encrypted text. This text consists only of the upper case from english alphabet. You can assume that the length of the text is smaller than 10000. The maximal sum of probabilities for the whole text is  $10^8$ .

#### **Output:**

On the only line of the output you should write the most probable key, by which the original text was encrypted. If there are more such keys, write the arbitrary one.

## **Example:**

| input                 | output |
|-----------------------|--------|
| 5 6                   | CPSPC  |
| TE 2                  |        |
| YP 1                  |        |
| XT 1                  |        |
| RY 1                  |        |
| PT 1                  |        |
| OI 1                  |        |
| JTDAQKPETPEGQEVGSLTZV |        |
|                       |        |

The input in the example corresponds to the original text HELLOIAMENCRYPTEDTEXT, which was encrypted by the key CPSPC. The overall probability of the key is 9.