# НАЦИОНАЛЕН ЕСЕНЕН ТУРНИР ПО ИНФОРМАТИКА
# Шумен, 23 - 25 ноември 2018 г.
# Група D, 6 клас

## Задача D2: Шифроване на съобщение

Петър е доста любознателен и прочита в една стара книга криптографска техника, която изглежда проста, но е относително трудна за прилагане. Ето в какво се състои тази техника:

1. Избира се ключова дума от най-малко шест латински букви, но не повече от 30. Да изберем, например думата SQUANDER. След това се създава таблица с 5 реда и 5 колони, във всяка клетка, на която се записва последователно по една буква от думата, започвайки от горния ляв ъгъл на таблицата и движейки се по редовете от ляво надясно и отгоре надолу, както е показано на Фиг.1.

| | | | | |
|---|---|---|---|---|
| S | Q | U | A | N |
| D | E | R | | |
| | | | | |
| | | | | |
| | | | | |

Фиг. 1

2. Останалите празни клетки на таблицата се запълват с поредните букви от латинската азбука, които не се срещат в избраната ключова дума.
3. Тъй като таблицата има 25 клетки, а латинската азбука – 26 букви, използва се стар римски обичай според, който буквите I и J се смятат за една буква и се записват в една клетка на таблицата, както е показано на Фиг. 2.

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

Фиг. 2

4. Взема се съобщението, което ще се кодира. Разбива се на двойки букви, започвайки от най-лявата буква и движейки се на дясно в текста. Ако в съобщението се срещат две съседни еднакви букви, те се разделят с буквата Q. Нека избраното съобщение е: *'All is known, fly at once'*. Разбито на двойки, то изглежда така:
   `AL QL IS KN OW NF LY AT ON CE`

Според описаното правило между двете букви LL е вмъкната буквата Q

5. Ако последната двойка не е пълна, тя се допълва от дясно с буквата Q.
6. Взема се първата двойка букви `AL` и се намират позициите на буквите A и L в таблицата. Вижда се, че са диагонални върхове на правоъгълника `LPAS`. В кодираното съобщение заменяме `A` и `L` със `S` и `P`, които са другите диагонални върхове. По същото правило заменяме `QL` със `SM` и `IS` с `FA`.
7. Когато двойката букви са на една линия, то ги заменяме с буквите от следващия ред, когато са на вертикална линия или с буквите от дясно на тях, когато са на хоризонтална линия. По този начин `KN` от примера се заменят с `TC`.

Продължавайки по описаните правила, заменяме `OW` с `MX`, `NF` с `SK`, `LY` с `PV`, `AT` с `NP`, `ON` с `TU`.

8. Когато двойката букви са на една линия, но някоя от тях е последна в реда или

колоната, то се взема съответно първата буква в реда или колоната от тази линия. По това правило `CE` се заменя с `DR`.

След извършване на всички замени, получаваме:

```
SP SM FA TC MX SK PV NP TU DR
```

9. Ако в зададеното за кодиране съобщение имаме нечетен брой букви и последните две букви са еднакви, тези букви се разделят с буквата `Q`. Така, ако искаме да кодираме думата `ALL`, тя ще се промени на `ALQL` преди кодирането.
10. Ако се срещнат две букви `Q` една до друга, те се разделят с буквата `Z`. Например, ако искаме да кодираме думата `FAQQAD`, тя ще се промени на `FAQZQADQ` преди кодирането.
11. Ако броят на буквите в зададеното за кодиране съобщение е нечетно число и последната буква е `Q`, то добавяме най-накрая буквата `Z`. Така, ако искаме да кодираме думата `HUQ`, тя ще се промени на `HUQZ` преди кодирането.

Помогнете на Петър да прилага тази техника за зададен от него ключ и съобщение за кодиране като напишете програма **`coding`**, реализираща описаната криптографска техника.

**Вход**

От първия ред на стандартния вход се въвежда ключовата дума. От следващия ред се въвежда съобщението, което трябва да бъде кодирано.

**Изход**

На единствения ред на стандартния изход се извежда кодираното съобщение, както се е получило след кодирането по двойки букви, разделени с по един интервал.

**Ограничения**

Всички букви са главни латински.

Ключовата дума съдържа само букви. Ако в нея има повтарящи се букви, отчита се само първото срещане на буквата. Останалите се игнорират. Максималната дължина на ключовата дума е 30 символа.

Съобщението, което ще се кодира, може да съдържа препинателни знаци и интервали.

В кодираното съобщение IJ се заменя с I.

**Примери**

**Вход**

```
SQUANDER
ALL IS KNOWN FLY AT ONCE
```

**Изход**

```
SP SM FA TC MX SK PV NP TU DR
```

**Вход**

```
JUXTAPOSITION
THE ROOSTER CROWED AT MIDNIGHT
```

**Изход**

```
IM CW BK SN XF IH VP XL GU NY UC PT CQ AM
```