# Olimpíadas Nacionais de Informática 2002

## www.api.pt

## 3 de Maio de 2002


## Departamento de Informática
## Faculdade de Ciências e Tecnologia
## Universidade Nova de Lisboa


# Problema 1 – Secreto

## 1 Problema

Queremos um programa para cifrar mensagens secretas e também para decifrá-las. Cada mensagem em claro (isto é, na sua forma original, antes de ser cifrada) é uma cadeia de caracteres formada exclusivamente pelas 26 letras do alfabeto, na sua forma maiúscula, sem espaços ou pontuação, por exemplo ATACAMOSAOAMANHECER.

A cifra faz-se usando uma chave, que é uma cadeia de caracteres (mantida secreta, é claro), por exemplo FCTUNL, e um número *N* (também secreto), por exemplo 4. A mensagem cifrada é obtida a partir na mensagem em claro de acordo com as seguintes regras:

1. As letras são cifradas sucessivamente, uma a uma, da esquerda para a direita.
2. Um letra que não pertença à chave é cifrada pela letra *N* posições à frente no alfabeto. (Recorde que *N* é o tal número secreto.) Para efeito desta regra, consideramos que o alfabeto é circular. Por exemplo, a letra 4 posições a seguir ao X é o B.
3. Uma letra que pertença à chave é cifrada por uma sequência de três letras: a *m*-ésima letra da chave, seguida da letra *N* posições à frente no alfabeto (tal como na regra anterior para as letras que não pertencem à chave), seguida da (*m*+1)-ésima letra da chave. A variável *m* aqui usada vale inicialmente 1 e é incrementada de uma unidade de cada vez que esta regra é utilizada. Para efeitos desta regra, consideramos que a chave é circular. Por exemplo, a décima letra da chave indicada é U.

Por exemplo, o primeiro A da mensagem usada com exemplo é cifrado em E; o T é cifrado em FXC; o segundo A é novamente cifrado em E; o C é cifrado em CGT; etc. Assim, o início da mensagem cifrada será EFXCECGT. Repare que ao cifrar o C a variável *m* já vale 2.

A chave secreta e o número secreto *N* são sempre escolhidos de modo a que seja possível decifrar as mensagens de uma única maneira. Isto quer dizer que não existem na chave letras afastadas entre si de *N* posições no alfabeto.

## 2 Tarefa

A sua tarefa é escrever um programa para cifrar e para decifrar mensagens de acordo com o esquema descrito.

## 3 Dados

Cada mensagem a cifrar ou a decifrar vem num ficheiro de texto de nome “SECRETO.IN”, juntamente com a chave secreta e com o número secreto. Este ficheiro tem quatro linhas. Na primeira linha aparece a letra C ou D. C significa que é para cifrar, D significa que é para de-

cifrar. Na segunda linha vem a chave secreta. Na terceira linha vem o número secreto. Na quarta linha vem a mensagem a cifrar ou decifrar. Por exemplo:

```
C
FCTUNL
4
ATACAMOSAOAMANHECER
```

# 4 Resultado

O resultado do programa, a cadeia cifrada ou decifrada, deve vir num ficheiro de texto de nome "SECRETO.OUT". Este ficheiro tem uma única linha (terminada por um fim de linha). O resultado correspondente ao exemplo anterior é:

```
EFXCECGTEQSWESEQETRULIUGNIV
```

# 5 Limites

A cadeia a cifrar tem no máximo 80 caracteres. A cadeia a decifrar tem no máximo 240 caracteres. O valor de *N* está entre 1 e 25 (inclusive). A cadeia a decifrar foi obtida cifrando uma outra, o que garante que é a decifração é possível.

# 6 Note bem

Respeite rigorosamente os nomes do ficheiros e o formato do ficheiro de resultado. O júri copiará o seu programa para uma pasta de teste no computador de avaliação e tentará correr o programa com ficheiros de dados com o nome indicado, na pasta de teste. O júri espera encontrar depois o ficheiro de resultado também na pasta de teste. O ficheiro de resultado gerado pelo seu programa será comparado automaticamente (isto é, por meio de um programa) com o ficheiro de resultado "oficial". O seu programa será considerado certo se os dois ficheiros forem iguais e errado se não.

Os ficheiros de teste usados pelo júri são válidos, garantidamente, pelo que o seu programa escusa de ser preocupar em validar os dados.