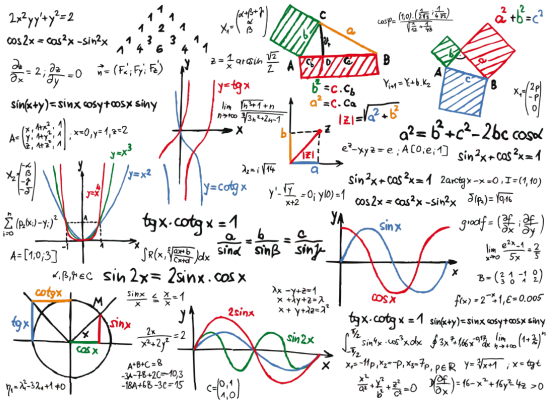

B1- Mathematics

B-MAT-100

103cipher

Mathematical Message Masking Multiplying Matrices

Matrix computation

Mathematical Message Masking Multiplying Matrices

binary name:	103cipher
repository name:	103cipher_$ACADEMICYEAR
repository rights:	ramassage-tek
language:	C, C++, perl 5, python 3 (≥ 3.5), ruby 2 (≥ 2.2), php 5.6, bash 4
group size:	1 to 2
compilation:	via Makefile, including re, clean and fclean rules

- Your repository must contain the totality of your source files, but no useless files (binary, temp files, obj files,...).
- All the bonus files (including a potential specific Makefile) should be in a directory named *bonus*.
- Error messages have to be written on the error output, and the program should then exit with the 84 error code (0 if there is no error).

Subject

Cryptography is a very old science, whose goal is to secure communication, so that only its recipient could read it.

There are a lot of methods to encrypt a message, from the simplest (like the 2000-year-old Cesar's code) to the most complex (like the World War 2 Enigma code) ; they all need both encryption and decryption keys (sometimes identical).
In some cases (such as the Hill cipher), the key is represented by a matrix.

You have to carry out such a matrix-based ciphering software, using the following process to encrypt :

1. transcript the key into numbers using the ASCII table,
2. convert the numbered key into a square matrix, the smallest possible size, and filling the lines first,
3. transcript the clear message into numbers using the ASCII table,
4. convert the numbered message into a matrix ; its number of columns should fit the key matrix size, and its number of lines should be as small as possible,
5. multiply the 2 matrices, and write the answer linearly to get the encrypted message.

During the conversion into matrices, zeros can be added at the end of the message or the key to fit the proper matrix size

The decryption process logically follows from the previous encryption method, using the same key (be careful ! you need to inverse the key matrix, which is not always possible).

2-dimension and 3-dimension matrices invertions are rather easy, but inverting bigger matrices is a difficult problem ; it would be considered as a bonus point if you can do that !

Usage

```
Terminal
~/B-MAT-100> ./103cipher message key flag
```

messsage	a message, made of ASCII characters
key	the encryption key, made of ASCII characters
flag	0 for the message to be encrypted, 1 to be decrypted

The use of library including matrix calculus (such as numpy) is prohibited !

Bonus

- cryptanalysis of the code, to find the original message without the key,
- refining the encryption process,

Examples

```
Terminal
~/B-MAT-100> ./103cipher "Just because I don't care doesn't mean I don't understand."
"Homer S" 0
Key matrix :
72          111         109
101         114         32
83          0           0

Encrypted message :
26690 21552 11810 19718 16524 13668 25322 22497 14177 28422 26097 16433 12333 11874
5824 27541 23754 14452 17180 17553 7963 26387 22047 13895 18804 14859 12033 27738
23835 15331 21487 16656 13238 21696 15978 6976 20750 23307 14093 16788 11751 8981
22339 24861 15619 21295 16524 13668 26403 23610 15190 29451 25764 16106 26394 23307
14093 3312 5106 5014
```

Indeed, "Homer", transcripted into numbers using the ASCII table, gives the following 3-3-matrix : $\begin{pmatrix} 72 & 111 & 109 \\ 101 & 114 & 32 \\ 83 & 0 & 0 \end{pmatrix}$

Using the ASCII table, the clear message becomes :
74 117 115 116 32 98 101 99 97 117 115 101 32 73 32 100 111 110 39 116 32 99 97 114 101 32 100 111 101 115 110 39 116 32 109 101 97 110 32 73 32 100 111 110 39 116 32 117 110 100 101 114 115 116 97 110 100 46

Written as a 3-column-matrix : $\begin{pmatrix} 74 & 117 & 115 \\ 116 & 32 & 98 \\ 101 & 99 & 97 \\ \dots & \dots & \dots \\ 46 & 0 & 0 \end{pmatrix}$

The product of these matrices is $\begin{pmatrix} 26690 & 21552 & 11810 \\ 19718 & 16524 & 13668 \\ 25322 & 22497 & 14177 \\ \dots & \dots & \dots \\ 3312 & 5106 & 5014 \end{pmatrix}$, which gives the encrypted message.

```
Terminal
~/B-MAT-100> ./103cipher "26690 21552 11810 19718 16524 13668 25322 22497 14177 28422 26097
16433 12333 11874 5824 27541 23754 14452 17180 17553 7963 26387 22047 13895 18804 14859
12033 27738 23835 15331 21487 16656 13238 21696 15978 6976 20750 23307 14093 16788 11751
8981 22339 24861 15619 21295 16524 13668 26403 23610 15190 29451 25764 16106 26394 23307
14093 3312 5106 5014" "Homer S" 1
Key matrix :
0.0         0.0         0.012
-0.004      0.012       -0.012
0.013       -0.013      0.004

Decrypted message :
Just because I don't care doesn't mean I don't understand.
```

Elements of the key matrix are separated by tabulations in the final output

For decryption, key matrix is given as an indication, but will not be tested ; do not bother having the exact same outuput !