MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Monoalphabetic Substitution with Camouflage – Part 6

Author: Viktor Veselovsky

June 2012

In previous parts of this challenge, there were always two alphabets, but it is possible to use any number of alphabets.

In this part, 9 alphabets have been used. Each alphabet consists of 26 letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ.
In total, there are 26*9=234 letters represented by numbers 0,1,2,...,232,233.

To distinguish between the alphabets, letters will be represented by numbers in the following way:

1) Transformation of a number N into a letter:

```
    if mod(N,26)=0 then N represents "A"
    if mod(N,26)=1 then N represents "B"
    ...
    if mod(N,26)=25 then N represents "Z"
```

2) Determination of the alphabet that contains N:

```
    if quotient(N,26)=0 then N belongs to alphabet 1
    if quotient(N,26)=1 then N belongs to alphabet 2
    ...
    if quotient(N,26)=8 then N belongs to alphabet 9
```

For example, N=113 represents letter "J" of alphabet 5 because mod(113,26)=9 and quotient(N,26)=4.

The encryption works in the same way as in the previous parts. The plaintext is separated into 9 pieces. Each piece is written in its corresponding alphabet.

All pieces are mixed together randomly, but in such a way that the order of characters in each piece is preserved. Afterwards, a monoalphabetic substitution is performed with a key that is a random permutation of all 234 numbers. The resulting numbers are written into a binary file in which each byte represents one number, i.e. one letter.

The decryption process is the reversion of all previous steps.

Challenge

Decrypt the file ciphertext.bin. The plaintext is written in English.

Find the sentence that does not fit to the rest of the plaintext. Write it in capital letters with spaces between the words and submit it as a solution to this challenge. There are no punctuation marks in this sentence.

Additional Information

The zip file mtc3-veselovsky-14-material.zip contains an example that can be used to test your algorithm. It consists of three files:

- exampledecryptionkey.bin contains the key for the decryption in binary format.
  (The first two bytes have the values 77 and 214 which means that bytes of value 0 in the ciphertext are replaced by 77 and bytes of value 1 are replaced by 214.)
- exampleciphertext.bin contains the ciphertext in binary format.
- exampleplaintext.txt contains the plaintext in text format.