Encrypt and decrypt with the Viginere cipher

Ο κρυπτογράφος (cipher) του Viginere μετασχηματίζει ένα μήνυμα σε μια μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους εκτός σε όσους έχουν το κλειδί (key).

Για κρυπτογράφηση του μηνύματος, προσθέτει το κλειδί πάνω στο μήνυμα που θέλουμε να κρυπτογραφήσουμε. Πιο συγκεκριμένα:

Encrypted = Message [+] Key

Πρόσεξε ότι η πρόσθεση γίνεται σε αντιστοιχία των χαρακτήρων (γι αυτό έβαλα το σύμβολο + μέσα σε brackets στη πιο πάνω γραμμή). Για παράδειγμα:

```
      Message = “AVECAESAR”
          Key = “ROME”
Repeated_Key = “ROMEROMER”
   Encrypted = “RJQGRSEEI”
```

όπου

```
A + R => R
V + 0 => J
E + M => Q
C + E => G
A + R => R
E + O => S
S + M => E
A + E => E
R + R => I
```

Πως γίνεται όμως A+R να μας κάνει R; Το A είναι το πρώτο γράμμα του αλφαβήτου (αυτό που βρίσκεται στη θέση μηδέν) και το R είναι το γράμμα του αλφαβήτου που βρίσκεται στη θέση δεκαεπτά: 0+17=17. Και ποιο είναι το γράμμα του αλφαβήτου που βρίσκεται στη θέση 17 (λαμβάνοντας υπόψη ότι ξεκινήσαμε να μετρούμε από το μηδέν). Η απάντηση είναι το R.

Πως γίνεται τώρα E + M να μας κάνει Q; Με παρόμοιο τρόπο 4+12=16. Και ποιο γράμμα βρίσκεται στη θέση 16 (λαμβάνοντας υπόψη ότι ξεκινήσαμε να μετρούμε από το μηδέν). Η απάντηση είναι το Q.

Τέλος, πως γίνεται S+M να μας κάνει E; Με παρόμοιο τρόπο, 18+12=30. Επειδή όμως έχουμε μόνο 26 γράμματα στο αλφάβητο που χρησιμοποιούμε γι αυτό το σκοπό ['A':'Z'], χρησιμοποιώντας modulo αριθμητική (δηλαδή κρατώντας μόνο το υπόλοιπο της διαίρεσης με το 26), το αποτέλεσμα γίνεται 4. Δηλαδή, το γράμμα στη θέση 4 (λαμβάνοντας υπόψη ότι ξεκινήσαμε να μετρούμε από το μηδέν) που είναι το E.

Συνεπώς το ένα που πρέπει να προσέξεις είναι το μέγεθος του αλφαβήτου που χρησιμοποιείται κάθε φορά. (δες length_of_alphabet στον κώδικα) και πως γίνεται η πράξη modulo. Η πράξη mod(x,y) επιστρέφει το υπόλοιπο της διαίρεσης του x με το y. Για παράδειγμα, mod(30,26) μας κάνει 4.

Τι άλλο πρέπει να προσέξεις; Πρόσεξε ότι η πράξη modulo επιστρέφει ένα αριθμό από το μηδέν μέχρι το y-1 ενώ εμείς θέλουμε ένα αριθμό από το 1 μέχρι το y. Πιο συγκεκριμένα, αν θέλουμε να

δούμε πιο είναι το i-οστό γράμμα στο αλφάβητο και ξεκινήσαμε να μετρούμε από το μηδέν, τότε πρέπει να προσθέσουμε ένα στο i, δηλαδή θα κοιτάξουμε το γράμμα alphabet(i+1).

Για αποκρυπτογράφηση, είναι παρόμοιος ο τρόπος με τη διαφορά ότι κάνει την αντίθετη πράξη. Αφαιρεί, δηλαδή, το κλειδί από το κρυπτογραφημένο μήνυμα ώστε να προκύψει το αρχικό μήνυμα.

Για να κάνει όμως την αντίθετη πράξη χρειάζεται το κόλπο με το πρόσημο (sign) που χρησιμοποιώ στον κώδικα. Χρειάζεται επίσης να μετατρέψουμε ένα διάνυσμα από αρνητικούς σε θετικούς αριθμούς. Για παράδειγμα, το -'ROME' είναι το διάνυσμα [-82,-79,-77,-69] και πρέπει να το μετατρέψουμε πίσω στο [82, 79, 77, 69].

Όταν έχει γίνει αυτό, χρησιμοποιούμε τη συνάρτηση char για να μετατρέψουμε ξάνα το νέο (θετικό) διάνυσμα σε συμβολοσειρά (στην προκειμένη περίπτωση τη 'ROME'). Αυτή είναι η δουλειά που κάνει το key=char(-key) όταν το πρώτο στοιχείο του κλειδιού είναι αρνητικός αριθμός.

ΠΡΟΣΟΧΗ!!! Ο κώδικας καλύπτει όλες τις περιπτώσεις με το καλύτερο δυνατό τρόπο. Σημειώνεται όμως ότι χρειάζεται ιδιαίτερη μαεστρία για να συνοψίσεις τον κώδικα σε τόσες λίγες γραμμές. Εννοείται ότι θα μπορούσα να τον γράψω σε περισσότερες γραμμές με σκοπό να φατσάρει λιγότερο "καλός". Μερικές αλλαγές που θα μπορούσαν να γίνουν (**για να γίνει χειρότερος**) είναι οι ακόλουθες:

- Αντί να χρησιμοποιούμε modulo αριθμητική (στη γραμμή 26) για να υπολογίζουμε τη θέση του χαρακτήρα του κλειδιού που μας ενδιαφέρει (πρόσεξε ότι αυτό είναι δεν είναι το ίδιο με τη θέση του υπόψη χαρακτήρα στο αλφάβητο). Αντί λοιπόν να υπολογίζουμε τη θέση του χαρακτήρα κατ' αυτόν τον τρόπο, μπορούμε να ξεκινήσουμε να επαναλαμβάνουμε τους χαρακτήρες του κλειδιού (δες Repeated_Key στην αρχή του κειμένου) ώστε να συμπληρώσουμε τα κενά που ενδεχομένως έχει η παράμετρος key σε σχέση με την παράμετρο message.
- Θα μπορούσαμε να γράφαμε δύο διαφορετικές συναρτήσεις, μια για την κρυπτογράφηση και μια για την αποκρυπτογράφηση (τις οποίες θα καλούσαμε από τη Vigenere αναλόγως της περίπτωσης). Η μόνη τους διαφορά θα ήταν στις πράξεις, δηλαδή πρόσθεση για τη συνάρτηση κρυπτογράφησης και αφαίρεσης για την αποκρυπτογράφηση. Όλα αυτά επιτυγχάνονται τώρα χάρην στο κόλπο με τη μεταβλητή sign. Πρόσεξε ότι αυτό περιμένει κι ο καθηγητής σας από κάποιους από εσάς, η άσκηση λέει **"Upload the file Vigenere.m and, if necessary, other files that contain functions which you call inside Vigenere "**.
- Χωρίς τη χρήση της συνάρτησης index στις γραμμές 28-33 (επιστρέφει τη θέση μιας φράσης μέσα σε μια συμβολοσειρά) θα μπορούσες να πιάσεις τις μονάδες όταν το αλφάβητο είναι το ['A':'Z'] και να χάσεις τις μονάδες που χρησιμοποιούν οποιοδήποτε άλλο αλφάβητο.

ΜΗΝ ΑΛΛΑΞΕΙΣ ΤΙΠΟΤΑ ΧΩΡΙΣ ΝΑ ΜΕ ΣΥΜΒΟΥΛΕΥΘΕΙΣ.