

αντικαταστάτες παραμένουν οι ίδιοι σε όλο το κείμενο (κάθε γράμμα του αρχικού κειμένου αντικαθίσταται πάντοτε από το ίδιο σύμβολο-αντικαταστάτη) τότε το σύστημα ονομάζεται *μονοαλφαβητικό*.

Αναπτύξτε ένα πρόγραμμα το οποίο υλοποιεί ένα μονοαλφαβητικό κρυπτοσύστημα αντικατάστασης. Πιο συγκεκριμένα, το πρόγραμμά σας θα πρέπει να:

- Διαβάζει από την πρώτη γραμμή της εισόδου μία μετάθεση των 26 (πεζών) γραμμάτων του λατινικού αλφαβήτου. Η μετάθεση εισάγεται ως μία συμβολοακολουθία 26 χαρακτήρων η οποία έχει την εξής έννοια: ο πρώτος χαρακτήρας αντικαθιστά το χαρακτήρα 'a', ο δεύτερος αντικαθιστά το χαρακτήρα 'b', κ.ο.κ.
- Ελέγχει αν η μετάθεση είναι έγκυρη. Κάθε πεζό λατινικό γράμμα πρέπει να εμφανίζεται ακριβώς μία φορά. Αν η μετάθεση δεν είναι έγκυρη, να εκτυπώνει το μήνυμα "error" και να σταματάει.
- Διαβάζει από τις επόμενες γραμμές της εισόδου το αρχικό κείμενο και να εκτυπώνει το κρυπτοκείμενο. Η κρυπτογράφηση να γίνεται χρησιμοποιώντας τη μετάθεση που έδωσε ο χρήστης. Αριθμοί, σημεία στίξης, κενά και αλλαγές γραμμής θα πρέπει να περνάνε στο κρυπτοκείμενο αμετάβλητα (αντικαθίστανται μόνο τα πεζά και κεφαλαία γράμματα a-z και A-Z). Τα κεφαλαία γράμματα του αρχικού κειμένου θα πρέπει να αντικαθίστανται σύμφωνα με την ίδια μετάθεση που ισχύει για τα πεζά, αλλά να παραμένουν κεφαλαία στο κρυπτοκείμενο.

Παράδειγμα εισόδου:

```
cbjalmvopqruytiezksnxdfghw
```

```
Once upon a time in China, some believe, around the year one double-ought three, head priest of the White Lotus Clan, Pai Mei was walking down the road, contemplating whatever it is that a man of Pai Mei's infinite power contemplates - which is another way of saying "who knows" - when a Shaolin monk appeared, traveling in the opposite direction. As the monk and the priest crossed paths, Pai Mei, in a practically unfathomable display of generosity, gave the monk the slightest of nods. The nod was not returned.
```

Παράδειγμα εξόδου:

```
Itjl xeit c npyl pt Joptc, siyl blupldl, ckixta nol hlck itl aixbul-ixvon nokll, Olca ekplsn im nol Fopnl Uinxs Juct, Ecp Ylp fcs fcurptv aift nol kica, jitnlyeucnptv focnldlk pn ps nocn c yct im Ecp Ylp's ptmptpnl eiflk jitnlyeucnls - fopjo ps ctinolk fch im schptv "foi rtifs" - folt c Sociupt yitr ceelckla, nkcdluptv pt nol ieeispnl apklnpfit. Cs nol yitr cta nol ekplsn jkissla ecnos, Ecp Ylp, pt c ekcjpnpjcuuh xtmcnoiycbul apseuch im vltlkispnh, vcdl nol yitr nol supvonlsn im tias. Nol tia fcs tin klnxktla.
```

Εξήγηση:

Βάσει της μετάθεσης που δίνεται στην πρώτη γραμμή της εισόδου, το γράμμα "c" αντικαθιστά το "a", το γράμμα "b" αντικαθιστά το "b", το γράμμα "j" αντικαθιστά το "c", κ.ο.κ.

► Να υποβληθεί στο αυτόματο σύστημα υποβολής και ελέγχου μέχρι την Παρασκευή 11/12/2020

Άσκηση 13.

Τροποποιήστε τη λύση της προηγούμενης άσκησης, ώστε το πρόγραμμά σας να μπορεί και να αποκρυπτογραφεί ένα κείμενο. Για το σκοπό αυτό, η δεύτερη γραμμή της εισόδου θα καθορίζει αν το πρόγραμμά σας πρέπει να κρυπτογραφήσει ή να αποκρυπτογραφήσει. Συγκεκριμένα:

- Αν η δεύτερη γραμμή της εισόδου αρχίζει με το γράμμα "d", τότε το πρόγραμμά σας πρέπει να αποκρυπτογραφεί το κείμενο που δίνεται.
- Διαφορετικά, θα πρέπει να το κρυπτογραφεί (όπως στην άσκηση 12).

Για την αποκρυπτογράφηση, η μετάθεση που δίνεται στην πρώτη γραμμή της εισόδου θα είναι εκείνη με την οποία κρυπτογραφήθηκε το αρχικό κείμενο. Στη συνέχεια, θα πρέπει να υπολογίζεται η αντίστροφη μετάθεση και βάσει αυτής να αποκρυπτογραφείται το κρυπτοκείμενο.

Στο παράδειγμα της προηγούμενης άσκησης, η αντίστροφη μετάθεση είναι:

dbavpwxycorefthijksnlgzumq

Παρατηρήστε ότι με αυτή τη μετάθεση γίνονται ακριβώς οι αντίστροφες αντικαταστάσεις, δηλαδή το γράμμα "a" αντικαθιστά το "c", το γράμμα "b" αντικαθιστά το "b", το γράμμα "c" αντικαθιστά το "j", κ.ο.κ. Κρυπτογραφώντας το κρυπτοκείμενο με την αντίστροφη μετάθεση, προκύπτει το αρχικό κείμενο (επαληθεύστε το).

Σημείωση: Από τη στιγμή που έχει υπολογιστεί η αντίστροφη μετάθεση, για την αποκρυπτογράφηση μπορεί να χρησιμοποιείται ακριβώς η ίδια διαδικασία που χρησιμοποιείται και για την κρυπτογράφηση!

Παραδείγματα εισόδου:

dzxhkbatvgmwrjoqeipsfnlcyu
encrypt

What are we waiting for, assembled in
the forum?
The barbarians are due here today.
Once the barbarians are here, they'll
do the legislating.

dzxhkbatvgmwrjoqeipsfnlcyu
decrypt

Ltds dik lk ldvsvja boi, dppkrzwhk vj
stk boifr?
Stk zdizdivdjp dik hfk tkik sohdy.
Ojxk stk zdizdivdjp dik tkik, stky'ww
ho stk wkavpwsdvja.

Παραδείγματα εξόδου:

Ltds dik lk ldvsvja boi, dppkrzwhk vj
stk boifr?
Stk zdizdivdjp dik hfk tkik sohdy.
Ojxk stk zdizdivdjp dik tkik, stky'ww
ho stk wkavpwsdvja.

What are we waiting for, assembled in
the forum?
The barbarians are due here today.
Once the barbarians are here, they'll
do the legislating.

► Να υποβληθεί στο αυτόματο σύστημα υποβολής και ελέγχου μέχρι την Παρασκευή 11/12/2020

Άσκηση N – Πρόβλημα Βασιλισσών. Λατινικά και Μαγικά Τετράγωνα. (Euler, Specker)

- i. Σε μια σκακιέρα 4×4 τοποθετήστε 4 βασίλισσες που να μην αλληλοαπειλούνται (μέθοδος οπισθοδρόμησης). Πόσες ουσιαστικά διαφορετικές λύσεις υπάρχουν;
- ii. Το ίδιο για σκακιέρα 5×5 με 5 βασίλισσες.
- iii. Η επιφάνεια που δημιουργείται, αν ταυτίσουμε αφενός την πάνω με την κάτω πλευρά αφετέρου την δεξιά με την αριστερή πλευρά της σκακιέρας λέγεται *τόρος*. Δεν υπάρχει τρόπος να τοποθετηθούν 4 βασίλισσες στην τορο-σκακιέρα 4×4 που να μην αλληλοαπειλούνται. Υπάρχει (ουσιαστικά μόνο ένας) τρόπος να τοποθετηθούν 5 βασίλισσες στην τορο-σκακιέρα 5×5 ώστε να μην αλληλοαπειλούνται.
- iv. Σε ένα πίνακα 5×5 τοποθετήστε τα γράμματα a,b,c,d,e (ένα σε κάθε τετραγωνάκι) έτσι ώστε σε κάθε γραμμή, στήλη και διαγώνιο (και τοροειδώς) να έχουμε διαφορετικά γράμματα.
- v. Τοποθετήστε τώρα στον πίνακα 5×5 συνδυασμούς των λατινικών γραμμάτων a,b,c,d,e και των ελληνικών γραμμάτων α,β,γ,δ,ε έτσι ώστε να ικανοποιούνται οι συνθήκες του (iv) για τα λατινικά και τα ελληνικά, και επιπλέον να μην έχουμε τον ίδιο συνδυασμό δύο φορές (Αυτό λέγεται λατινικό τετράγωνο).
- vi. Αν θέσουμε $a=\alpha=0$, $b=\beta=1$, $\gamma=c=2$, $d=\delta=3$, $e=\epsilon=4$ και διαβάσουμε το συνδυασμό ψηφίων στο πενταδικό σύστημα (π.χ. $b\delta=13_5=8$), τότε έχουμε ένα μαγικό τόρο (τοροειδές τετράγωνο). Δηλαδή, εμφανίζονται όλοι οι αριθμοί από 0 έως 24 έτσι ώστε τα αθροίσματα σε στήλες, γραμμές και (τοροειδείς) διαγωνίους να είναι ίσα. Ελέγξτε το.
- vii. Δοκιμάστε να βρείτε αλγοριθμικό κανόνα για την κατασκευή μαγικού τόρου 5×5 . Σημειώστε ότι δεν υπάρχει μαγικό τετράγωνο 2×2 , υπάρχει 3×3 , 4×4 , 6×6 , 8×8 , 9×9 αλλά δεν υπάρχει μαγικός τόρος. Υπάρχει όμως μαγικός τόρος 5×5 , 7×7 , 11×11 (και πολλοί 13×13). Τι σχέση υπάρχει μεταξύ των τριών προβλημάτων (όλα σε τόρο): Βασιλισσών-Λατινικών τετραγώνων-Μαγικών τετραγώνων;

► Να παραδοθεί στον υπεύθυνο του εργαστηρίου σας μέχρι την Παρασκευή 8/1/2021

Άσκηση Ο – Το παιχνίδι Specker Π_n

Το παιχνίδι Π_3 : Δίνονται 3 σωροί με ομοειδή κέρματα π.χ. με 2,3 και 4 κέρματα (γενικότερα: a,b,c κέρματα, a,b,c φυσικοί, $0 < a \leq b \leq c$). Δύο παίκτες, ο Α και ο Β παίζουν εναλλάξ με τους ίδιους κανόνες. Αρχίζει ο Α. Ο παίκτης διαλέγει δυο από τους 3 σωρούς. Βγάζει από τον μικρότερο σωρό όσα κέρματα θέλει και βάζει στον μεγαλύτερο σωρό όσα κέρματα θέλει (όχι αναγκαστικά τον ίδιο αριθμό και υποθέτουμε ότι υπάρχει απειρίοστη παρακαταθήκη κερμάτων). Αν οι δύο επιλεγμένοι σωροί είναι ίσοι, δεν έχει σημασία από ποιον θα αφαιρεθούν άρα και σε ποιόν σωρό θα προστεθούν κέρματα. Χάνει ο παίκτης που δεν έχει πια δυο σωρούς να επιλέξει.

- i. Από αρχική κατάσταση (2,3,4) ποιές είναι οι δυνατές καταστάσεις μετά από μια κίνηση του παίκτη Α; (αν απαγορεύεται σωρός με περισσότερα από 5 κέρματα).
 - ii. Ποια από τις ανωτέρω κινήσεις οδηγεί σε νίκη του Α ακόμα και αν ο Β παίζει με τον καλύτερο δυνατό τρόπο; (Άρα καλή στρατηγική για τον Α.)
 - iii. Πόσο διαρκεί το μακρύτερο παιχνίδι, όταν ο Α προσπαθεί να νικήσει το συντομότερο;
 - iv. Είναι δυνατόν να παίζουν έτσι ώστε το παιχνίδι να διαρκέσει περισσότερο από 1000000 κινήσεις (εάν παρεπιπτόντως δεν τους ενδιαφέρει η νίκη). Εξηγήστε.
 - v. Ποιος έχει στρατηγική για να νικήσει αν το παιχνίδι αρχίσει σε μια από τις επόμενες καταστάσεις; (5,5,5),(5,5,6),(5,6,6),(6,6,6)
 - vi. Μια κατάσταση (a,b,c) θα λέγεται επιτυχημένη αν ο παίκτης Α έχει στρατηγική να νικήσει. Μια κατάσταση θα λέγεται αποτυχημένη αν ο παίκτης Β έχει στρατηγική να νικήσει. Να χαρακτηρίσετε τις επιτυχημένες και τις αποτυχημένες καταστάσεις.
 - vii. Στο παιχνίδι Π_3 , είναι το σύνολο των επιτυχημένων καταστάσεων συμπληρωματικά του συνόλου των αποτυχημένων καταστάσεων; (Γενίκευση);
 - viii. Να εφεύρετε μια παραλλαγή του Π_3 επιτρέποντας επιπλέον κινήσεις έτσι ώστε η ένωση των επιτυχημένων και των αποτυχημένων καταστάσεων να μη δίνει το σύνολο όλων των καταστάσεων.
 - ix. Π_4 : Γενικεύστε το παιχνίδι Π_3 έτσι ώστε η αρχική κατάσταση να έχει 4 σωρούς από κέρματα.
 - x. Βρείτε τις επιτυχημένες και τις αποτυχημένες καταστάσεις για το Π_4 (με απόδειξη).
 - xi. (*) Αναλόγως ορίστε Π_5 (Π_6) και βρείτε τις επιτυχημένες και αποτυχημένες καταστάσεις.
 - xii. (*) Δείξτε: Στο Π_5 είναι δυνατόν σε μια επιτυχημένη κατάσταση (για τον Α) να καταφέρει ο Β να καθυστερήσει την ήττα του όσο θέλει.
 - xiii. (*) Το παιχνίδι Π_n (γενίκευση):
 - Καταστάσεις: $(a_1, \dots, a_n) \in \mathbb{N}^n$, δηλ. $a_i \leq a_{i+1}$, a_i φυσικοί,
 - Κινήσεις: a_i, a_j ($i < j$ άρα και $a_i \leq a_j$) να αντικατασταθεί με a_i', a_j' έτσι ώστε $a_i' < a_i$, $a_j' > a_j$ και να ταξινομηθεί η νέα n-άδα.
 - Ήττα: Δεν υπάρχει κίνηση, δηλ. $(0, 0, \dots, a_n)$
- Αποδείξτε το ακόλουθο:
Θεώρημα: Το παιχνίδι Π_n είναι πεπερασμένο, δηλαδή τελειώνει πάντα μετά από πεπερασμένο αριθμό κινήσεων. (Με επαγωγή για το n).

► Να παραδοθεί στον υπεύθυνο του εργαστηρίου σας μέχρι την Παρασκευή 8/1/2021