Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχ. και Μηχ. Υπολογιστών
Προγραμματισμός Ηλεκτρονικών Υπολογιστών, 1ο εξάμηνο
http://courses.softlab.ntua.gr/progintro/
Ε. Ζάχος, Ν. Παπασπύρου, Α. Παγουρτζής

5η Σειρά Ασκήσεων

Άσκηση 9 – Μαγικά τετράγωνα

Αναπτύξτε ένα πρόγραμμα σε γλώσσα Pascal το οποίο θα εμφανίζει στην οθόνη μαγικά τετράγωνα, με μήκος πλευράς περιττό αριθμό (από το 3 έως το 13 για να χωράει στην οθόνη) που θα επιλέγεται από το χρήστη. Το πρόγραμμά σας θα πρέπει να εμφανίζει κατάλληλο ενημερωτικό μήνυμα σε περίπτωση που ο χρήστης δεν δώσει αποδεκτό μήκος πλευράς, και σε κάθε περίπτωση να τον ρωτάει αν θέλει να επαναλάβει τη διαδικασία.

Άσκηση 10 – Μονοαλφαβητικό κρυπτοσύστημα αντικατάστασης

Ένα *κρυπτοσύστημα*, γενικά, αποτελείται από δύο αλγορίθμους: έναν αλγόριθμο *κρυπτογράφησης* ή κωδικοποίησης (encryption or enciphering algorithm) και έναν αλγόριθμο *αποκρυπτογράφησης* ή αποκωδικοποίησης. Το *αρχικό κείμενο* (plaintext – απλό κείμενο) είναι το κείμενο προς κρυπτογράφηση. Χρησιμοποιώντας το αρχικό κείμενο για είσοδο του αλγορίθμου κρυπτογράφησης, παίρνουμε στην έξοδο το *κρυπτοκείμενο* (cryptotext ή ciphertext). Ο αλγόριθμος αποκρυπτογράφησης (η αντίστροφη διαδικασία δηλαδή) χρησιμοποιεί για είσοδο το κρυπτοκείμενο και εξάγει το αντίστοιχο αρχικό κείμενο.

Στα συστήματα *αντικατάστασης* (substitution ciphers), τα γράμματα του αρχικού κειμένου αντικαθίστανται από άλλα τα οποία διατηρούνται στην ίδια διάταξη όπως και τα πρωτότυπά τους στο αρχικό κείμενο. Αν οι 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 σε γλώσσα Pascal, το οποίο υλοποιεί ένα μονοαλφαβητικό κρυπτοσύστημα αντικατάστασης. Πιο συγκεκριμένα, το πρόγραμμά σας θα πρέπει να:

- Ζητάει από το χρήστη 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.ό.κ.
- Ελέγχει αν η μετάθεση που έδωσε ο χρήστης είναι έγκυρη. Κάθε πεζό λατινικό γράμμα πρέπει να εμφανίζεται ακριβώς μία φορά. Αν η μετάθεση δεν είναι έγκυρη, να ζητάει μία νέα μέχρι ο χρήστης να δώσει μία έγκυρη μετάθεση.
- Διαβάζει το αρχικό κείμενο από ένα αρχείο κειμένου και να γράφει το κρυπτοκείμενο σε ένα άλλο αρχείο κειμένου. 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.
- Προαιρετικά, να δίνει στο χρήστη την επιλογή να **αποκρυπτογραφήσει** ένα κείμενο. Για το σκοπό αυτό, να ζητάει απο το χρήστη τη μετάθεση με την οποία κρυπτογραφήθηκε το αρχικό κείμενο. Στη συνέχεια, να υπολογίζει την αντίστροφη μετάθεση και με βάση αυτή να αποκρυπτογραφεί το κρυπτοκείμενο. *Σημείωση:* από

τη στιγμή που έχει υπολογιστεί η αντίστροφη μετάθεση, για την αποκρυπτογράφηση χρησιμοποιείται ακριβώς η ίδια διαδικασία που χρησιμοποιείται και για την κρυπτογράφηση!

Παράδειγμα κρυπτογράφησης και αποκρυπτογράφησης

Ας υποθέσουμε ότι χρησιμοποιούμε την ακόλουθη μετάθεση:

```
cbjalmvopqruytiezksnxdfghw
```

Δηλαδή το γράμμα 'c' αντικαθιστά το 'a', το γράμμα 'b' αντικαθιστά το 'b', το γράμμα 'j' αντικαθιστά το 'c', κ.ό.κ. Ας υποθέσουμε ακόμη ότι το αρχικό κείμενο είναι το ακόλουθο:

```
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.
```

Τότε το κρυπτοκείμενο που θα προκύψει είναι το παρακάτω:

```
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
apkljnpit. Cs nol yitr cta nol ekplsn jkissla ecnos, Ecp Ylp, pt c ekcjnpjcuuh
xtmcnoiycbul apseuch im vltlkispnh, vcdl nol yitr nol supvonlsn im tias. Nol tia fcs
tin klnxktla.
```

Για την αποκρυπτογράφηση, η αντίστροφη μετάθεση είναι:

```
dbavpwxyocrefthijksnlgzumq
```

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.ό.κ. Κρυπτογραφώντας το κρυπτοκείμενο με την αντίστροφη μετάθεση, προκύπτει το αρχικό κείμενο (επαληθεύστε το).

Να επιδειχθούν στον υπεύθυνο του εργαστηρίου σας την εβδομάδα 8/1/07 – 12/1/07

Άσκηση Λ – Πρόβλημα Βασιλισσών. Λατινικά και Μαγικά Τετράγωνα.

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=α=0, b=β=1, γ=c=2, d=δ=3, e=ε=4 και διαβάσουμε το συνδυασμό ψηφίων στο πενταδικό σύστημα (π.χ. bδ=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. Σημειωτέον 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;

Άσκηση Μ – 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 παίχτες, ο Α και ο Β παίζουν εναλλάξ με τους ίδιους κανόνες. Αρχίζει ο Α.
Ο παίχτης 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 απεριόριστη παρακαταθήκη κερμάτων). Αν οι δύο επιλεγμένοι σωροί είναι ίσοι τότε δεν έχει σημασία από ποιον θα αφαιρεθούν άρα και σε ποιόν σωρό θα προστεθούν κέρματα.
Χάνει ο παίχτης που δεν έχει πια δυο σωρούς να επιλέξει.

1) Από αρχική κατάσταση (2,3,4) ποιές είναι οι δυνατές καταστάσεις μετά από μια κίνηση του παίχτη Α; (αν απαγορεύεται σωρός με περισσότερα από 5 κέρματα).
2) Ποια από τις ανωτέρω κινήσεις οδηγεί σε νίκη του Α ακόμα και αν ο Β παίξει με τον καλύτερο δυνατό τρόπο; (Άρα καλή **στρατηγική** για τον Α)
3) Πόσο διαρκεί το μακρύτερο παιχνίδι, όταν ο Α προσπαθεί να νικήσει το συντομότερο;
4) Είναι δυνατόν να παίζουν έτσι ώστε το παιχνίδι να διαρκέσει περισσότερο από 1000000 κινήσεις (εάν παρεπιπτόντως δεν τους ενδιαφέρει η νίκη). Εξηγείστε.
5) 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)

6) Μια κατάσταση (a,b,c) θα λέγεται **επιτυχημένη** αν ο παίχτης Α έχει στρατηγική να νικήσει. Μια κατάσταση θα λέγεται **αποτυχημένη** αν ο παίχτης Β έχει στρατηγική να νικήσει. Να χαρακτηρίσετε τις επιτυχημένες και τις αποτυχημένες καταστάσεις.
7) Στο παιχνίδι Π_3, είναι το σύνολο των επιτυχημένων καταστάσεων συμπληρωματικά του συνόλου των αποτυχημένων καταστάσεων; (Γενίκευση;)
8) 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.
9) Π_4: Γενικεύστε το παιχνίδι Π_3 έτσι ώστε η αρχική κατάσταση να έχει 4 σωρούς από κέρματα.
10) Βρείτε τις επιτυχημένες και τις αποτυχημένες καταστάσεις για το Π_4 (με απόδειξη).
11) (*) Αναλόγως ορίστε Π_5 (Π_6) και βρείτε τις επιτυχημένες και αποτυχημένες καταστάσεις.
12) (*) Δείξτε: Στο Π_5 είναι δυνατόν σε μια επιτυχημένη κατάσταση (για τον Α) να καταφέρει ο Β να καθυστερήσει την ήττα του όσο θέλει.
13) (*) Το παιχνίδι Π_n (Γενίκευση):
    a. Καταστάσεις: $(a_1,\ldots,a_n)^{\leq}$, δηλ. $a_i \leq a_i+1$, a_i φυσικοί,
    b. 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.
    c. Ήττα: Δεν υπάρχει κίνηση, δηλ. $(0,0,....,a_n)$

    Αποδείξτε το:

    Θεώρημα: Το παιχνίδι Π_n είναι πεπερασμένο (δηλαδή τελειώνει πάντα μετά από πεπερασμένο αριθμό κινήσεων) (με επαγωγή για το n).

<u>Να παραδοθούν στον υπέυθυνο του εργαστηρίου σας την εβδομάδα 22/1/07 – 26/1/07</u>