ΥΠΟΛΟΓΙΣΤΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΠΑΝ/ΜΙΟΥ ΠΕΙΡΑΙΩΣ
Μάιος 2020

Απαλλακτική προγραμματιστική εργασία
Παράδοση μέχρι και την 22η ΣΕΠΤΕΜΒΡΙΟΥ 2020

Εκφώνηση: Να υλοποιηθεί αλγόριθμος για την παραγωγή ενός τυχαίου πρώτου αριθμού με k bits, $k > 1$, με χρήση του κριτηρίου Miller-Rabin. Συγκεκριμένα, ο αλγόριθμος δέχεται ως είσοδο τον ακέραιο $k > 1$, επιλέγει τυχαία έναν ακέραιο n, με $2^{k-1} < n < 2^k$ και στη συνέχεια εφαρμόζει τον έλεγχο Miller-Rabin για τον n. Αν ο n περάσει τον έλεγχο, τον επιστρέφει ως τον ζητούμενο πρώτο, αλλιώς επιλέγει άλλο n, μέχρι να βρεθεί πρώτος n.

Η υλοποίηση μπορεί να γίνει σε όποιο προγραμματιστικό περιβάλλον προτιμάτε.

Περισσότερες πληροφορίες για τον αλγόριθμο μπορείτε να βρείτε στο σύγγραμα του μαθήματος (σελ. 293): V. Shoup, Μια υπολογιστική εισαγωγή στη θεωρία αριθμών και την άλγεβρα, Κλειδάριθμος, 2005.

Παραδοτέα:

1. Ένα κείμενο σε μορφή pdf που θα περιέχει: ένα εξώφυλλο με τα στοιχεία σας (ονοματεπώνυμο, αριθμό μητρώου), μια περιγραφή της υλοποίησης, τον ψευδοκώδικα του αλγορίθμου, screenshots της εκτέλεσης του αλγορίθμου, οδηγίες εγκατάστασης και χρήσης της εφαρμογής.

2. Ο πηγαίος κώδικας και το εκτελέσιμο (αν υπάρχει) της εφαρμογής.

Η εργασία θα παραδοθεί ηλεκτρονικά, στο `kmanes@unipi.gr`, ως ένα συμπιεσμένο αρχείο.