Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

2η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 31/10/2019

Άσκηση 1. Δίνεται ένα κρυπτοσύστημα που διαθέτει τέλεια μυστικότητα για την ομοιόμορφη κατανομή πιθανότητας πάνω στα αρχικά κείμενα. Εξετάστε αν ισχύει στο κρυπτοσύστημα αυτό η ιδιότητα της τέλειας μυστικότητας για την εξής κατανομή πιθανότητας: ένα από τα αρχικά κείμενα εμφανίζεται με πιθανότητα 1/2, ενώ τα υπόλοιπα με πιθανότητα $1/2(|\mathcal{M}| - 1)$.

Άσκηση 2. Αποδείξτε ότι $(p-1)! \equiv -1 \pmod{p}$, όπου p πρώτος αριθμός.

Άσκηση 3. Υπολογίστε το $25^{-1} \bmod 77$ χωρίς αριθμομηχανή, χρησιμοποιώντας μόνο εμπειρικές παρατηρήσεις και το Κινέζικο Θεώρημα Υπολοίπων (CRT). Μπορείτε να βρείτε και 2ο τρόπο, χωρίς χρήση του CRT;

Άσκηση 4. Έστω $a \in U(\mathbb{Z}_n)$ τάξης k και $b \in U(\mathbb{Z}_n)$ τάξης m. Αποδείξτε ότι ο αριθμός $ab \in U(\mathbb{Z}_n)$ έχει τάξη km αν και μόνο αν $gcd(k, m) = 1$.

Άσκηση 5. Υλοποιήστε τον έλεγχο πρώτων αριθμών Fermat σε πρόγραμμα (απαιτείται να υποστηρίζονται πράξεις μεγάλων αριθμών, χιλιάδων ψηφίων). Εφαρμόστε τον για να ελέγξετε τους παρακάτω αριθμούς:
$67280421310721, 170141183460469231731687303715884105721, 2^{2281} - 1, 2^{9941} - 1, 2^{19939} - 1$

Άσκηση 6. Έστω $\mathbb{Z}_p^*$ με p πρώτο και g ένας γεννήτορας, p, g γνωστά.

1. Αν d ένας ακέραιος που διαιρεί το $p-1$, βρείτε με αποδοτικό τρόπο ένα στοιχείο b του $\mathbb{Z}_p^*$ τάξης d (δηλαδή d ο μικρότερος ακέραιος με $b^d \equiv 1 \pmod{p}$)
2. Πόσα στοιχεία τάξης d υπάρχουν μέσα στο $\mathbb{Z}_p^*$;
3. Πόσους γεννήτορες έχει η κυκλική υποομάδα που παράγει ένα στοιχείο b τάξης d;
4. Πόσες κυκλικές υποομάδες τάξης d υπάρχουν στο $\mathbb{Z}_p^*$;
5. Αν μας δώσουν ένα στοιχείο h, την τάξη του d και ένα τυχαίο στοιχείο a, πώς μπορούμε να δούμε αν το a ανήκει στην υποομάδα που παράγει το h σε πολυωνυμικό χρόνο;

Άσκηση 7. (*)

Ο τελεστής $\uparrow\uparrow$ ορίζεται ως εξής:

$\alpha \uparrow\uparrow (n+1) = \alpha^{\alpha\uparrow\uparrow n}$ με $\alpha \uparrow\uparrow 1 = \alpha$.

Για παράδειγμα $3 \uparrow\uparrow 4 = 3^{3^{3^3}} = 3^{3^{27}} = 3^{7625597484987}$

Να φτιάξετε ένα κομψό και αποδοτικό πρόγραμμα το οποίο να υπολογίζει τα τελευταία 16 ψηφία του αριθμού $1707 \uparrow\uparrow 1783$.

Σημείωση: ο ζητούμενος υπολογισμός μπορεί να γίνει σε χρόνο λιγότερο από 5sec σε υπολογιστή 'κανονικών' προδιαγραφών χρησιμοποιώντας μεταβλητές τύπου long (ακέραιους 64-bit).

(*): άσκηση bonus.

Σύντομες οδηγίες: (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητές σας, (γ) αναζητήστε ιδέες στο διαδίκτυο, με αυτή τη σειρά και αφού αφιερώσετε αρκετό χρόνο σε κάθε στάδιο! Σε κάθε περίπτωση οι απαντήσεις πρέπει να είναι *αυστηρά ατομικές*.