Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

2η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 22/12/2021

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

Άσκηση 2. Να βρείτε όλες τις υποομάδες της ομάδας $\mathbb{Z}_{29}^*$. Εξηγήστε αναλυτικά με ποιον τρόπο σκεφτήκατε και τι δοκιμές κάνατε.

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.

(α) Να δείξετε ότι κάθε υποομάδα μιας κυκλικής ομάδας είναι επίσης κυκλική.

(β) Πόσες υποομάδες έχει η ομάδα $U(\mathbb{Z}_{4872961})$;

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.

Στο ηλιακό σύστημα του πλανήτη Ραττατάκ υπάρχουν κάτι πολύ περίεργες λευκές τρύπες, τις οποίες οι Ραττατακιανοί χρησιμοποιούν για τις μετακινήσεις τους. Οι αξιολάτρευτες κατά τα άλλα αυτές λευκές τρύπες έχουν η καθεμιά ένα διαφορετικό αριθμό-αναγνωριστικό αναλόγως με το πόσο αδύναμες ή δυνατές είναι ως προς την ικανότητά τους να επιφέρουν τηλεμεταφορά στον χώρο αλλά και στον χρόνο. Επίσης, ο χρόνος μέσα σε αυτές κυλάει (μα και φυσικά!) με διαφορετικό τρόπο από ό,τι στον "έξω" κόσμο, και συγκεκριμένα, για μια λευκή τρύπα με αναγνωριστικό έστω M και απόσταση έστω Z που ο Ραττατακιανός επιθυμεί να τηλεμεταφερθεί, η λευκή τρύπα τον καθυστερεί για μια (πολύ μικρή!) χρονική διάρκεια:

$$Z^{1998000^{100^{10}}} \mod 10^M \quad \text{"πλεξοδευτερόλεπτα"}$$

Καλείστε να βοηθήσετε έναν μικρό Ραττατακιανό, γράφοντας ένα κομψό και αποδοτικό πρόγραμμα, κατά

προτίμηση σε γλώσσα C ή Python που με είσοδο τους αριθμούς , θα υπολογίζει πόσο χρόνο θα χρειαστεί (σε πλεξοδευτερόλεπτα) για το ταξίδι του στον χωροχρόνο.

Αιτιολογήστε τη σκέψη σας πίσω από το πρόγραμμα και ως παράδειγμα, υπολογίστε τα πλεξοδευτερόλεπτα που θα χρειαστεί ο μικρούλης για την λευκή τρύπα $M = 3$ σε απόσταση $Z = 548$.

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, προτιμώμενα σε γλώσσα C ή Python, το οποίο να υπολογίζει τα τελευταία 17 ψηφία του αριθμού $1707 \uparrow\uparrow 1783$.

Σημείωση: ο ζητούμενος υπολογισμός μπορεί να γίνει σε χρόνο λιγότερο από 3 sec σε υπολογιστή 'κανονικών' προδιαγραφών χρησιμοποιώντας μεταβλητές τύπου long (ακέραιους 64-bit).

Άσκηση 8. 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 9.

1. 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 $gcd(k, m) = 1$. Ισχύει η ιδιότητα για οποιαδήποτε (πεπερασμένη) αβελιανή ομάδα;
2. Να δείξετε ότι σε μια (πεπερασμένη) αβελιανή ομάδα η τάξη κάθε στοιχείου διαιρεί την μέγιστη τάξη (μεταξύ όλων των στοιχείων της ομάδας).
   Υπόδειξη: μπορεί να σας φανεί χρήσιμη η διαδικασία απόδειξης του ερωτήματος (6.1).
3. Έστω μια (πεπερασμένη) αβελιανή ομάδα που έχει την εξής ιδιότητα: έχει το πολύ μία υποομάδα για κάθε πιθανή τάξη (παρατήρηση: σε γενικές ομάδες, είναι δυνατόν αυτό να μην συμβαίνει, δηλαδή να υπάρχουν δύο υποομάδες διαφορετικές μεταξύ τους με την ίδια όμως τάξη). Να δείξετε ότι είναι κυκλική.
4. Χρησιμοποιώντας το θεώρημα Lagrange της θεωρίας αριθμών που μπορείτε να λάβετε ως δεδομένο, ότι δηλαδή αν g είναι ένα μη-σταθερό πολυώνυμο βαθμού d με συντελεστές στο $\mathbb{Z}_p^*$ τότε το πολυώνυμο αυτό έχει το πολύ d ρίζες στο $\mathbb{Z}_p^*$, να δείξετε ότι η ομάδα $\mathbb{Z}_p^*$ είναι κυκλική για κάθε πρώτο p.

Άσκηση 10. Εξετάστε τη γεννήτρια ψευδοτυχαιότητας RC4. Αποδείξτε ότι το δεύτερο byte (κλειδί) εξόδου είναι ίσο με 0 με πιθανότητα περίπου ίση με 2^{-7}. Ξεκινήστε δείχνοντας ότι αν μετά τη φάση δημιουργίας κλειδιών (KSA) ισχύει για την μετάθεση P ότι $P[2] = 0$ και $P[1] \neq 2$ τότε το δεύτερο byte εξόδου είναι ίσο με 0 με πιθανότητα 1.

Άσκηση 11. Έστω $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ ψευδοτυχαία συνάρτηση. Εξετάστε τις παρακάτω συναρτήσεις ως προς την ψευδοτυχαιότητα τους:

1. $F_1(k, x) = F(k, x) \oplus x$
2. $F_2(k, x) = F(F(k, 0^n), x)$
3. $F_3(k, x) = F(F(k, 0^n), x)||F(k, x)$

Άσκηση 12. Θεωρήστε την παραλλαγή του DES-X, με 2 κλειδιά k_1, k_2, όπου η κρυπτογράφηση ενός απλού κειμένου M γίνεται ως εξής :

$$Enc_{k_1,k_2}(M) = E_{k_1}(M \oplus k_2),$$

όπου E η συνάρτηση κρυπτογράφησης του DES.

Έχουμε περισσότερη ασφάλεια από τον κλασσικό DES στο παραπάνω σύστημα; Θεωρήστε ότι ο αντίπαλος έχει δυνατότητα KPA (διαθέτει αρκετά ζεύγη απλού κειμένου - κρυπτοκειμένου).

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*.

Προσοχή: αν θέλετε, μπορείτε να επιλέξετε μία από τις ασκήσεις 6, 7 και μία από τις 8, 9.