Εργασία 2

Κωσταντίνος Σαΐτας - Ζαρκιάς - 2406
Οδυσσεύς Κρυσταλάκος - 2362

1 Μαΐου 2016

Θέμα 1

(vii)

Με p και q γνωστά μπορούμε να υπολογίσουμε το N και $f(n)$.

$$N = p \cdot q = 463 \cdot 547 = 253261$$

$$\phi(n) = (p-1) \cdot (q-1) = 462 \cdot 546 = 252252$$

επομένως το d υπολογίζεται:

$$ed \equiv 1(\mathrm{mod}\phi(n)) \Leftrightarrow d = 27473$$

Τελικά για την αποκρυπτογράφηση του ς αρκεί να υπολογισθεί

$$c^d(\mathrm{mod}\phi(n)) = 13500$$

(x)

Ισχύει

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = pq - (p+q) + 1$$

και επειδή $N = pq$

$$\phi(n) = N - (p+q) + 1$$

Θέμα 2

(i)

Υλοποιώντας και χρησιμοποιώντας τον εκτεταμένο αλγόριθμο του Ευκλείδη για την εύρεση του GCD, βρέθηκε:

$$GCD(126048, 5050) = 202$$

$$-1 \cdot 126048 + 25 \cdot 5050 = 202$$

(ii)

Για τον υπολογισμό του αντίστροφου, υπολογίσθηκαν όλα τα γινόμενα $809 * i$ όπου i παίρνει τιμές από 1 έως 1000. Βρέθηκε πως ο αντίστροφος είναι το 464.

(iii)

Καθώς το 2^{100} είναι δύσκολο να αποθηκευτεί και να χρησιμοποιηθεί σε πράξεις με ακρίβεια, χρησιμοποιήθηκε μία διαφορετική τεχνική. Υπολογίσθηκε το 2 modulo 101 και το αποτέλεσμα πολλαπλασιάστηκε(modulo 101) με το 2. Αυτό έγινε επαναληπτικά 100 φορές και το αποτέλεσμα είναι 464.

(iv)

Ο αλγόριθμος υλοποιήθηκε στο αρχείο fast.py. Τα αποτελέσματα είναι:

$$2^{1234567} \mathrm{mod} 12345 = 8648$$

$$130^{7654321} \mathrm{mod} 567 = 319$$

Θέμα 3

Θέμα 4

Θέμα 5

Θέμα 6

(i)

$$\frac{123454}{546542} = 0 + \cfrac{1}{4 + \cfrac{52726}{123454}}$$

$$= 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{18002}{52726}}} = 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{16722}{18002}}}} = 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1280}{16722}}}}}$$

$$= 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{13+\cfrac{82}{1280}}}}}} = 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{13+\cfrac{1}{15+\cfrac{50}{82}}}}}}} = 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{13+\cfrac{1}{15+\cfrac{1}{1+\cfrac{32}{50}}}}}}}}$$

$$= 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{13+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{1+\cfrac{18}{32}}}}}}}}} = 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{13+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{14}{18}}}}}}}}}}$$

$$= 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{13+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{4}{14}}}}}}}}}}} = 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{13+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3+\cfrac{2}{4}}}}}}}}}}}}$$

$$= 0 + \cfrac{1}{4 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{13+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2+0}}}}}}}}}}}}$$

Θέμα 7

Θέμα 8

Θέμα 9

(α)

Εφαρμόστηκε το τεστ του Fermat με τις συνθήκες που αναφέρονται στην εκφώνηση. Αυτό που παρατηρείται είναι ότι, κατά προσέγγιση, οι μισοί αριθμοί που παράγονται από την $f(x)$ είναι πρώτοι ενώ οι υπόλοιποι μισοί όχι.

(β)

Τα μόνα πολυώνυμα του Z που, για κάθε ακέραια τιμή, δίνουν πρώτο αριθμό είναι τα σταθερά πολυώνυμα με τιμή κάποιον πρώτο αριθμό.

$$P(x) = p$$

όπου p πρώτος αριθμός

Αντιθέτως, δεν υπάρχει μή σταθερό πολυώνυμο για το οποίο να ισχύει η παραπάνω συνθήκη.

Απόδειξη

Έστω ένα μη σταθερό πολυώνυμο $P(x)$ που μας δίνει πρώτο αριθμό για κάθε τιμή του $x \in Z$

Τότε ισχύει

$$P(1) = p$$

όπου π πρώτος αριθμός.

Επομένως ισχύει και

$$P(1 + np) \equiv 0 (\mathrm{mod} p), n \in Z$$

γιατί η παραπάνω τιμή του P διαιρείται με το p. Επομένως, αφού η τιμή του $P(1 + np)$ διαιρείται με το p, δεν είναι πρώτος αριθμός. Άτοπο, άρα η αρχική υπόθεση είναι εσφαλμένη και δεν υπάρχει τέτοιο μη σταθερό πολυώνυμο.