

**ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ**  
**ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ #1**

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

- (1) Δίνεται ο πρώτος αριθμός  $p = 101$ .
- (α') Βρείτε ένα γεννήτορα της ομάδας  $\mathbb{Z}_p^*$ . Πόσοι είναι οι γεννήτορες της  $\mathbb{Z}_p^*$ ; Υπολογίστε 5 γεννήτορες.
  - (β') Υπολογίστε τον αντίστροφο του  $\overline{83}$  στην ομάδα  $\mathbb{Z}_p^*$ .
  - (γ') Λύστε την εξίσωση  $\overline{83} \cdot x = \overline{10}$  στην ομάδα  $\mathbb{Z}_p^*$ .
- (2) Δίνεται ο πρώτος  $p = 67$ .
- (α') Δείξτε ότι το  $g = \overline{2}$  είναι γεννήτορας της ομάδας  $\mathbb{Z}_p^*$ .
  - (β') Υπολογίστε το διακριτό λογάριθμο του  $y = \overline{3}$  ως προς τη βάση  $g$  με τον αλγόριθμο του Shanks.
  - (γ') Υπολογίστε τον ίδιο διακριτό λογάριθμο κάνοντας διάσπαση Pohlig-Hellman.
- (3) Η Αλίκη και ο Βασίλης χρησιμοποιούν το πρωτόκολλο Diffie-Hellman στην ομάδα  $\mathbb{Z}_{61}^*$  με βάση το  $g = \overline{2}$  (είναι γεννήτορας). Η Αλίκη στέλνει στο Βασίλη την τιμή  $y_A = \overline{38}$  και ο Βασίλης στέλνει την τιμή  $y_B = \overline{50}$ . Εσείς παρακολουθείτε την επικοινωνία και γνωρίζετε τις τιμές αυτές. Υπολογίστε το κοινό κλειδί που δημιουργούν.
- (4) Έστω  $n > 1$  φυσικός αριθμός και  $g \in \mathbb{Z}$ .
- (α') Δείξτε ότι το  $\overline{g}$  είναι γεννήτορας της ομάδας  $\mathbb{Z}_n$  αν και μόνο αν  $(n, g) = 1$ .
  - (β') Διατυπώστε το πρόβλημα του διακριτού λογαρίθμου για την ομάδα  $\mathbb{Z}_n$  και δώστε ένα γρήγορο αλγόριθμο για τον υπολογισμό του.