

**ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ**  
**ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ #2**

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

- (1) Δώστε ένα μάρτυρα Fermat της συνθετότητας του  $n = 21$ .
- (2) Δώστε ένα μάρτυρα Rabin-Miller της συνθετότητας του  $n = 57$ .
- (3) Κατασκευάστε ένα σύστημα κρυπτογράφησης RSA όπου οι πρώτοι  $p$  και  $q$  θα έχουν δύο δεκαδικά ψηφία. Περιγράψτε αναλυτικά πώς υπολογίζεται ένα ιδιωτικό και ένα δημόσιο κλειδί. Στη συνέχεια κρυπτογραφήστε και αποκρυπτογραφήστε ένα μήνυμα της επιλογής σας.
- (4) Κατασκευάστε ένα σύστημα κρυπτογράφησης ElGamal στην ομάδα  $\mathbb{Z}_{19}^*$ . Ως βάση, μπορείτε να χρησιμοποιήσετε το  $g = \bar{2}$ , το οποίο γεννά την ομάδα. Περιγράψτε την κατασκευή ενός ζεύγους ιδιωτικού/δημόσιου κλειδιού και στη συνέχεια κρυπτογραφήστε το μήνυμα  $m = \bar{5}$ .
- (5) Σε ένα σύστημα κρυπτογράφησης ElGamal στην ομάδα  $\mathbb{Z}_{787}^*$  με βάση  $g = \bar{2}$  (είναι γεννήτορας) το δημόσιο κλειδί της Αλίκης είναι  $y = \bar{5}$ . Βλέπετε δύο κρυπτογραφήματα  $(r_1, c_1) = (318, 191)$  του (άγνωστου) μηνύματος  $m_1$  και  $(r_2, c_2) = (79, 118)$  του (άγνωστου) μηνύματος  $m_2$ . Υποδείξτε πώς μπορείτε να υπολογίσετε το κρυπτογράφημα του μηνύματος  $m_1 \cdot m_2 \pmod{p}$  (χωρίς φυσικά να υπολογίσετε τα  $m_1$  και  $m_2$ ).