

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ
ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ #3

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΛΑΚΗΣ

Άσκηση 1

Κατασκευάστε ένα σύστημα υπογραφής ElGamal με βάση την ομάδα $(\mathbb{Z}/23\mathbb{Z})^*$. Υπολογίστε την υπογραφή στο μήνυμα m , με $h(m) = 4$, όπου h είναι η συνάρτηση κατακερματισμού που χρησιμοποιούμε. Περιγράψτε την πιστοποίηση της υπογραφής.

Άσκηση 2

Έστω ένα σύστημα υπογραφής RSA με δημόσιο κλειδί (e, n) και ιδιωτικό κλειδί (d, p, q) , όπου p, q περιτοί πρώτοι, $n = pq$ και $ed \equiv 1 \pmod{\phi(n)}$. Μια συνηθισμένη τεχνική για να επιταχυνθεί ο υπολογισμός της υπογραφής είναι η εξής: ο υπογράφων υπολογίζει τα $s_1 \equiv h(m)^d \pmod{p}$ και $s_2 \equiv h(m)^d \pmod{q}$ και στη συνέχεια υπολογίζει την υπογραφή στο μήνυμα m συνδυάζοντας τα s_1 και s_2 με το Κινέζικο Θεώρημα Υπολοίπων. Δώστε ένα συγκεκριμένο παράδειγμα της παραπάνω μεθόδου.

Άσκηση 3

Η Αλίκη χρησιμοποιεί το σύστημα υπογραφής RSA με την παραπάνω τεχνική. Το δημόσιο κλειδί της είναι το $(e, n) = (3, 391)$. Κατά τον υπολογισμό της υπογραφής στο μήνυμα m με $h(m) = 9$ με την παραπάνω μέθοδο, υπολογίζει το s_1 σωστά, κάνει όμως λάθος στον υπολογισμό του s_2 . Έτσι παράγει την υπογραφή $s = 49$. Προφανώς η υπογραφή είναι λάθος και δεν πιστοποιείται. Δείξτε ότι σφάλμα της Αλίκης είναι πολύ μεγαλύτερο: με δεδομένο το δημόσιο κλειδί, το μήνυμα και την (λανθασμένη) υπογραφή μπορείτε να παραγοντοποιήσετε το $n = 391$.

Άσκηση 4

Η Αλίκη χρησιμοποιεί το σύστημα υπογραφής ElGamal για να υπογράψει μηνύματα. Το σύστημα βασίζεται στην ομάδα $(\mathbb{Z}/23\mathbb{Z})^*$, η βάση είναι το $g = 2$ και το δημόσιο κλειδί της είναι το $y = 6$. Η Αλίκη, από λάθος, χρησιμοποιεί τον ίδιο εκθέτη k για να υπογράψει δύο διαφορετικά μηνύματα, τα m_1 και m_2 , με $h(m_1) = 1$ και $h(m_2) = 3$. Οι αντίστοιχες υπογραφές είναι $(r_1, s_1) = (13, 9)$ και $(r_2, s_2) = (13, 3)$.

Δείξτε ότι το κρυφό κλειδί της Αλίκης μπορεί να υπολογιστεί εύκολα (υπολογίστε το).

Άσκηση 5

Έστω p πρώτος αριθμός και q πρώτος διαιρέτης του $p - 1$. Έστω g και h στοιχεία της ομάδας $(\mathbb{Z}/p\mathbb{Z})^*$ τάξης q . Δίνεται η απεικόνιση

$$H : \{0, 1, \dots, q - 1\}^2 \longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \\ (x, y) \mapsto g^x h^y \pmod{p}.$$

- (1) Αποδείξτε ότι όποιος μπορεί να λύνει το πρόβλημα του διακριτού λογαρίθμου (ως προς τη βάση g) στην ομάδα $(\mathbb{Z}/p\mathbb{Z})^*$, μπορεί να υπολογίζει προεικόνες της H .
- (2) Αποδείξτε ότι όποιος μπορεί να υπολογίζει προεικόνες της H μπορεί να υπολογίζει διακριτούς λογάριθμους στην ομάδα $(\mathbb{Z}/p\mathbb{Z})^*$ (ως προς τη βάση g).
- (3) Αποδείξτε ότι όποιος μπορεί να υπολογίζει συγκρούσεις της H , μπορεί να υπολογίσει το διακριτό λογάριθμο του h ως προς τη βάση g .