ΜΕΤΑΔΕΔΟΜΕΝΑ

Τίτλος: Εισαγωγή στην Κρυπτογραφία

Υπότιτλος: -

Γλώσσα: Ελληνικά

Συγγραφείς: Δραζιώτης, Κ., Επίκουρος Καθηγητής, ΑΠΘ

ISBN: 978-618-85820-5-7

Θεματικές Κατηγορίες: ΜΑΘΗΜΑΤΙΚΑ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Λέξεις-κλειδιά: Κρυπτογραφία / Θεωρία αριθμών / Ασφάλεια υπολογιστικών συστημάτων / Συμμετρική κρυπτογραφία / Κρυπτογραφία δημοσίου κλειδιού

Βιβλιογραφική Αναφορά: Δραζιώτης, Κ. (2022). Εισαγωγή στην Κρυπτογραφία [Προπτυχιακό εγχειρίδιο]. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. http://dx.doi.org/10.57713/kallipos-17

Περίληψη

Το βιβλίο καλύπτει βασικά θέματα της Κρυπτογραφίας. Ειδικότερα, στο Κεφάλαιο 1, δίνεται μια Εισαγωγή, καθώς και εφαρμογές που έχει σήμερα η Κρυπτογραφία. Στα Κεφάλαια 2, 3 και 4 παρουσιάζεται μια Εισαγωγή στην Κρυπτογραφία ιδιωτικού κλειδιού όπου περιγράφονται τα κρυπτοσυστήματα ροής και τμήματος. Επίσης, δίνονται κάποιοι βασικοί ορισμοί ασφάλειας. Στο Κεφάλαιο 5 παρουσιάζονται οι συναρτήσεις κατακερματισμού και οι κώδικες αυθεντικοποίησης. Από το Κεφάλαιο 6 ξεκινά η παρουσίαση της Κρυπτογραφίας δημόσιου κλειδιού. Το Κεφάλαιο 6 είναι αφιερωμένο στο σύστημα ανταλλαγής κλειδιού Diffie-Hellman, και στο Κεφάλαιο 7 παρουσιάζεται μια σύντομη εισαγωγή στη θεωρία πολυπλοκότητας και στη Μηχανή Turing. Στα Κεφάλαια 8, 9 και 10 παρέχεται μια Εισαγωγή στη βασική θεωρία αριθμών, που είναι απαραίτητη στην κατανόηση του RSA και των ψηφιακών υπογραφών. Στο Κεφάλαιο 11 παρουσιάζεται η trapdoor RSA, και στο Κεφάλαιο 12 δίνονται κάποιες επιθέσεις στο RSA, όπως η επίθεση του Wiener. Στο Κεφάλαιο 13 γίνεται μια Εισαγωγή στις ψηφιακές υπογραφές. Στο Κεφάλαιο 14 δίνονται βασικοί ορισμοί που αφορούν τα πλέγματα και παρουσιάζονται μερικοί βασικοί αλγόριθμοι, όπως ο LLL, ο αλγόριθμος απαρίθμησης με κλάδεμα και ο αλγόριθμος του Babai. Στο Κεφάλαιο 15 παρουσιάζονται τα πρωτόκολλα SSL/TLS και PGP, παράλληλα με κάποιες εφαρμογές.

Το Έργο χρηματοδοτείται από το Εθνικό Πρόγραμμα Ανάπτυξης 2021-2025 του Υπουργείου Παιδείας και Θρησκευμάτων και υλοποιείται από τον Ειδικό Λογαριασμό Κονδυλίων Έρευνας του Εθνικού Μετσόβιου Πολυτεχνείου