ΜΕΤΑΔΕΔΟΜΕΝΑ

Τίτλος: Υπολογιστική Κρυπτογραφία

Υπότιτλος: -

Γλώσσα: Ελληνικά

ISBN: 978-960-603-276-9

Θεματικές Κατηγορίες: ΜΑΘΗΜΑΤΙΚΑ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ, ΦΥΣΙΚΕΣ ΚΑΙ ΓΕΩΠΟΝΙΚΕΣ ΕΠΙΣΤΗΜΕΣ, ΕΠΙΣΤΗΜΕΣ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑ

Λέξεις-κλειδιά: Υπολογιστική Πολυπλοκότητα / Υπολογιστική Θεωρία Αριθμών / Συμμετρική Κρυπτογραφία / Κρυπτογραφία Δημόσιου Κλειδιού / Κρυπτογραφικά Πρωτόκολλα

Βιβλιογραφική Αναφορά: Ζάχος, Ε., Παγουρτζής, Α., & Γροντάς, Π. (2015). Υπολογιστική Κρυπτογραφία [Προπτυχιακό εγχειρίδιο]. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. http://dx.doi.org/10.57713/kallipos-492

Περίληψη

Το βιβλίο αποσκοπεί να εισαγάγει τον αναγνώστη στις θεμελιώδεις έννοιες και τεχνικές της κρυπτογραφίας, με έμφαση στην αλγοριθμική και υπολογιστική διάστασή τους. Τα περιεχόμενα συνοπτικά: - Εισαγωγή σε βασικές έννοιες αλγορίθμων και πολυπλοκότητας: ανάλυση αλγορίθμων, αποδοτικότητα, πολυωνυμικός χρόνος, πιθανοτικοί αλγόριθμοι, κλάσεις πολυπλοκότητας. - Στοιχεία θεωρίας αριθμών και θεωρίας ομάδων: αριθμητική modulo, ομάδες, δακτύλιοι, σώματα, Κινέζικο Θεώρημα Υπολοίπων, Θεωρήματα Fermat, Euler, Lagrange, πρωταρχικές ρίζες, συνάρτηση φ του Euler, τετραγωνικά υπόλοιπα, σύμβολα Legendre και Jacobi. - Υπολογιστική πολυπλοκότητα και αλγόριθμοι για βασικά αριθμοθεωρητικά προβλημάτων: επαναλαμβανόμενος τετραγωνισμός, Ευκλείδειος, επεκτεταμένος Ευκλείδειος, υπολογισμός συμβόλου Jacobi, ρίζες modulo n, έλεγχοι πρώτων αριθμών (Fermat, Solovay-Strassen, Miller-Rabin, αλγόριθμος AKS), παραγοντοποίηση (μέθοδος ρ, μέθοδος Dixon), διακριτός λογάριθμος (Shanks, Pohling-Hellman, index-calculus). - Συμμετρικά κρυπτοσυστήματα: πακέτου (DES, AES), ροής (stream ciphers). Τρόποι λειτουργίας. Κρυπτοσυστήματα δημοσίου κλειδιού: RSA, ElGamal. Ανταλλαγή κλειδιού Diffie-Hellman. - Σχήματα ψηφιακών υπογραφών (RSA, DSS), υπογραφές ειδικού σκοπού (μιας χρήσης, τυφλές, αδιαμφισβήτητες). - Κρυπτογραφικά πρωτόκολλα (διαμοιρασμού μυστικού, ρίψης νομίσματος, ανταλλαγής κλειδιού). - Αποδείξεις ασφάλειας βασισμένες σε γενικά παραδεκτές υποθέσεις υπολογιστικής δυσκολίας, μοντέλα ασφάλειας (KPA, CPA, CCA, IND-CPA, IND-CCA), κρυπτογραφικές αναγωγές. - Συναρτήσεις σύνοψης (hash functions) και συναρτήσεις μονής κατεύθυνσης. Ψευδοτυχαιότητα. - Αποδείξεις μηδενικής γνώσης. Πρωτόκολλα ταυτοποίησης. - Προηγμένα θέματα: κβαντική και μετα-κβαντική κρυπτογραφία, ελλειπτικές καμπύλες, σύνθεση πρωτοκόλλων, διγραμμικές απεικονίσεις, κρυπτογραφία με lattices.

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 και τον Σύνδεσμο Ελληνικών Ακαδημαϊκών Βιβλιοθηκών.