



METADATA

Title: COMPUTATIONAL CRYPTOGRAPHY

Other Titles: -

Language: Greek

ISBN: 978-960-603-276-9

Subject: MATHEMATICS AND COMPUTER SCIENCE,
NATURAL SCIENCES AND AGRICULTURAL SCIENCES,
ENGINEERING AND TECHNOLOGY

Keywords: Cryptography / Computational Complexity /
Computational Number Theory / Symmetric Cryptography /
Public Key Cryptography

Bibliographic Reference: Pagourtzis, A., & Zachos, E. (2015). COMPUTATIONAL CRYPTOGRAPHY [Undergraduate textbook]. Kallipos, Open Academic Editions. <http://dx.doi.org/10.57713/kallipos-492>

Abstract

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.