

## Κρυπτογραφία

### Σύντομη περιγραφή μαθήματος

**Στόχος του μαθήματος:** Περιγραφή των προβλημάτων που απασχολούν την κρυπτογραφία. Περιγραφή αλγορίθμων που επιλύουν τα προβλήματα αυτά. Ορισμός και εκτίμηση της ασφάλειας που παρέχουν οι αλγόριθμοι που περιγράφουμε.

**Προαπαιτούμενα:** Το μάθημα δεν έχει τυπικά προαπαιτούμενα. Ουσιαστικό προαπαιτούμενο είναι βασικές γνώσεις άλγεβρας, θεωρίας αριθμών και υπολογιστικής πολυπλοκότητας.

**Αξιολόγηση:** Θα δοθούν κάποιες σειρές ασκήσεων και (ίσως) ένα τελικό διαγώνισμα. Οι λεπτομέρειες θα ανακοινωθούν στο μάθημα.

### Υλη του μαθήματος:

- Ιστορικοί κώδικες
  - Κώδικας του Καίσαρα
  - Μονοαλφαβητική αντικατάσταση
  - One-Time-Pad
- Block Ciphers
  - Feistel ciphers
  - DES
  - MACs
- Συστήματα δημόσιου κλειδιού
  - Πρωτόκολλο δημιουργίας κοινού κλειδιού
  - Αλγόριθμοι κρυπτογράφησης
  - Αλγόριθμοι υπογραφής
  - Αλγόριθμοι υπογραφής με επιπλέον ιδιότητες
- Ορισμοί ασφάλειας
- Βασικά αριθμοθεωρητικά προβλήματα
  - Το πρόβλημα του διακριτού λογάριθμου
  - Τα προβλήματα των Diffie και Hellman
  - Το πρόβλημα της παραγοντοποίησης ακεραίων
- Ειδικά θέματα (αν υπάρχει χρόνος)

### Προτεινόμενα συγγράμματα:

Την ύλη του μαθήματος καλύπτουν τα παρακάτω βιβλία:

Nigel Smart, *Cryptography: An Introduction*, McGraw-Hill Education, November 2002.

Douglas Stinson, *Cryptography: Theory and Practice (Discrete Mathematics & Its Applications S.)*, CRC Press, February 27, 2002.

Richard A. Mollin, *An Introduction to Cryptography*, CRC Press, August 10, 2000.

Μια εγκυκλοπαίδεια της κρυπτογραφίας, με πολύ καλή βιβλιογραφία:

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 16, 1996. (Ελεύθερα διαθέσιμο στο <http://www.cacr.math.uwaterloo.ca/hac/>)

Σε περισσότερο αλγεβρικό/αριθμοθεωρητικό πνεύμα είναι τα:

Neal Koblitz, *A Course in Number Theory and Cryptography*, GTM 114, Springer-Verlag, 1987. Second edition, 1994.

Neal Koblitz, *Algebraic Aspects of Cryptography*, Algorithms and Computation in Mathematics Vol. 3, Springer-Verlag, 1998.

Δύο πολύ καλά βιβλία πάνω σε αλγεβρικούς και αριθμοθεωρητικούς αλγόριθμους είναι τα:

Joachim von zur Gathen, Jürgen Gerhard, *Modern Computer Algebra*, Cambridge University Press, 1999.

Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, 2005 (ελπίζουμε). (Το βιβλίο είναι διαθέσιμο ελεύθερα στο <http://shoup.net/ntb/>)

Μια θεμελίωση της κρυπτογραφίας στα πλαίσια της θεωρίας πολυπλοκότητας δίνεται στους παρακάτω δύο τόμους:

Oded Goldreich, *Foundations of Cryptography (Volume I: Basic Tools)*, Cambridge University Press, 2001.

Oded Goldreich, *Foundations of Cryptography (Volume II: Basic Applications)*, Cambridge University Press, 2001.