Κρυπτογραφία: Οργανωτικά

Χειμερινό Εξάμηνο 2015 - 2016

Οργανωτικά

- Μαθήματα:
  - Τρίτη: 17:00 - 19:00
  - Παρασκευή: 16:00 - 18:00
  - Αίθουσα 005, Νέα Κτήρια ΗΜΜΥ
- Έναρξη μαθημάτων: 2015-10-06
- 13 εβδομάδες, 26 μαθήματα

Υπεύθυνοι καθηγητές

- Άρης Παγουρτζής (σε εκπαιδευτική άδεια)
- Παναγιώτης Τσανάκας
- Στάθος Ζάχος

Διδασκαλία

- Παναγιώτης Γροντάς pgrontas@gmail.com
- Πέτρος Ποτίκας ppotik@cs.ntua.gr
- Διονύσης Ζήνδρος dionyziz@gmail.com

Βοηθοί διδασκαλίας: crypto-class.gr project

- Αλέξης Μπρέζας abresas@gmail.com
- Κωνσταντίνος Κανελλής kkanelli@gmail.com
- Κωστής Καραντίας karantiaskostis@gmail.com
- Πλάτων Κιορπελίδης platwnace@gmail.com
- Σωκράτης Βίδρος sokratis.vidros@gmail.com

Βοηθοί διδασκαλίας: Θεωρητικές ασκήσεις

- Ζέτα Αβαρικιώτη zavarikioti@gmail.com
- Χαρά Ποδηματά charapod@gmail.com

Βοηθοί διδασκαλίας: Πρακτικές ασκήσεις

- Δημήτρης Καρακώστας dimit.karakostas@gmail.com
- Λευτέρης Ιωαννίδης elefthei@mit.edu

Επισκέπτης διδάσκοντας

- Γιώργος Τσουκαλάς (ψηφιακές ψηφοφορίες)

Βοηθοί διδασκαλίας: Βιντεοσκόπηση

- Νικόλας Κορασίδης renelvon@gmail.com
- Βασίλης Γκούμας bgoumas@gmail.com
- Κωνσταντίνος Μόι

Προαπαιτούμενες γνώσεις

- Μαθηματική ωριμότητα
  - Διακριτά μαθηματικά
  - Λογική
  - Επαγωγή
- Αλγόριθμοι
  - Πολυπλοκότητα και O(.)
  - Γράφους
- Προγραμματισμός
  - Άνεση σε μία γλώσσα της επιλογής σου
- Επικοινωνίες
  - Πώς δουλεύουν πρωτόκολλα επικοινωνιών και δίκτυα

Κοινό

Επίσημο μάθημα

- Φοιτητές ΗΜΜΥ ΕΜΠ
  - Ακόμη και μικρότερων ετών
- Φοιτητές ΜΠΛΑ
- Φοιτητές ΣΕΜΦΕ ΕΜΠ

Ως crypto-class.gr project

- Ανοιχτό σε όλους: Φοιτητές, μαθητές, επαγγελματίες...
- Στόχος η δημιουργία υλικού που θα είναι επαναχρησιμοποιήσιμο

Ροές

- Το μάθημα πλέον ανήκει στη ροή Λ
- Για εισακτέους πριν από φέτος, το μάθημα εντάσσεται ακόμη στο ροή Μ

Αλλαγές στο μάθημα

- Το μάθημα διατηρεί το δυνατό θεωρητικό και ακαδημαϊκό του χαρακτήρα
- Προστίθενται **εφαρμογές** της κρυπτογραφίας
  - Κρυπτογραφία στο web (HTTPS, HSTS)
  - Επιθέσεις side-channel
  - Κρυπτογράφηση επικοινωνιών (GPG, OTR)
  - Ψηφιακές ψηφοφορίες
  - Blockchain και bitcoin

Ασκήσεις

- Δύο ειδών
  - Πρακτικές ασκήσεις
  - Θεωρητικές ασκήσεις
- Περίπου 1 άσκηση για κάθε μάθημα

Θεωρητικές ασκήσεις

- Παραδοσιακές μαθηματικές «αποδεικτικές» ασκήσεις
- Θεωρητικός σχεδιασμός πρωτοκόλλων
- Παραδίδονται σε μορφή PDF
  - Σκανάρισμα χειρόγραφων λύσεων που έχουν μετατραπεί σε PDF επιτρέπονται
- Συνεργασίες πρέπει να αναγράφονται στη λύση
- Κάθε μαθητής που θα συνεργαστεί πρέπει να στείλει την κοινή λύση

Πρακτικές ασκήσεις

- Απαιτούν να γράψετε κώδικα για να βρείτε τη λύση
- Συχνά χρειάζονται τη χρήση μεγάλων αριθμών
- Μπορείτε να χρησιμοποιήσετε έτοιμες βιβλιοθήκες
- Οι συνεργασίες επιτρέπονται και ενθαρρύνονται
- Διαδραστικό σύστημα: Ξέρετε αν έχετε στείλει τη σωστή λύση

crypto-class.gr project

- Φέτος υλοποιείται το crypto-class.gr project
- Για την παρακολούθηση του μαθήματος απαιτείται η εγγραφή στο website
  - Επισκευθείτε το www.crypto-class.gr και γραφτείτε με τον αριθμό μητρώου σας
- Οι εργασίες παραδίδονται **μόνο** μέσω του website. **Δεν** γίνονται δεκτές:
  - Λύσεις στο χαρτί (τυπωμένες ή χειρόγραφες)
  - Λύσεις μέσω e-mail, CD, κλπ.

Deadlines

- Τα deadlines θα τηρηθούν αυστηρά
- Παρατάσεις δεν θα δοθούν
- Θα έχετε 1 - 2 εβδομάδες για κάθε άσκηση
- Μετά το deadline:
  - 2 επιπλέον μέρες για παράδοση για το 80% του βαθμού
  - Δυνατότητα παράδοσης αργότερα για το 0% του βαθμού (test mode)

Βαθμολογικό σχήμα

- ΒΘΑ: Βαθμός θεωρητικών ασκήσεων (στα 5)
- ΒΠΑ: Βαθμός πρακτικών ασκήσεων (στα 5)
- ΒΕ: Γραπτός βαθμός τελικής εξέτασης (στα 10)
- ΤΒ: Τελικός βαθμός στο μάθημα (στα 15)

ΤΒ = ΒΕ * (1 + (ΒΘΑ + ΒΠΑ) / 20)

- Δεν απαιτούνται ειδικά κατώφλια για το 5

Άδεια χρήσης

- Το υλικό μας δημοσιεύεται δωρεάν εντός και εκτός πολυτεχνείου
- Υπό Creative Commons 4.0 BY
  - Διαφάνειες (PDF)
  - Βίντεο
  - Εκφωνήσεις ασκήσεων
- Υπό MIT
  - Πρότυπες λύσεις ασκήσεων

Βιβλιογραφία

Επίσημη βιβλιογραφία

- Σημειώσεις Κρυπτογραφίας
  - Στάθης Ζάχου, Άρης Παγουρτζής
- Θεωρία αριθμών
  - Victor Shoup
  - Διαθέσιμο δωρεάν online

Βιβλιογραφία

Επίσης χρήσιμα

- Cryptography I, Coursera
  - Dan Boneh
  - https://www.coursera.org/course/crypto
- https://crypto101.io/ (ημιτελές)
  - CC BY NC 4.0
  - Μπορείτε να βοηθήσετε
- Wikipedia
- Wikis αποκεντρωμένων συστημάτων
  - π.χ. bitcoin wiki https://en.bitcoin.it

Ύλη του εξαμηνιαίου μαθήματος

- Συμμετρική κρυπτογραφία
  - Παραδοσιακά συστήματα
  - One-time pad
  - Block ciphers, AES
  - Stream ciphers, RC4
  - Μαθηματική μοντελοποίηση ασφάλειας μέσω παιγνίων
- Συναρτήσεις hash
  - md5, SHA1, SHA256, δέντρα Merkle
  - HMAC για πιστοποίηση

Ύλη του εξαμηνιαίου μαθήματος

- Ασύμμετρη κρυπτογραφία
  - RSA
  - DSA, ElGamal
  - Ελλειπτικές καμπύλες / ECDSA
- Θεωρία αριθμών
- Θεωρία ομάδων
- Αποδείξεις μηδενικής γνώσης

Ύλη του εξαμηνιαίου μαθήματος

- Εφαρμογές
  - Οικονομική κρυπτογραφία: Blockchain & bitcoin
  - Διασφάλιση επικοινωνιών: GPG, OTR
  - Ελευθερία του λόγου και του τύπου: Tor
  - Ηλεκτρονική διακυβέρνηση: Εκλογές και ψηφοφορίες
  - Αποκεντρωμένα συστήματα και πολιτικές εφαρμογές

Στόχοι του εξαμηνιαίου μαθήματος

- Να καταλάβετε τις βασικές έννοιες της κρυπτογραφίας
- Να μπορείτε να επιχειρηματολογήσετε για την κρυπτογραφική ασφάλεια ενός συστήματος
- Να μπορείτε να αναλύσετε θεωρητικά ένα κρυπτογραφικό σύστημα
- Να μπορείτε να υλοποιήσετε σε κώδικα τα συστήματα που περιγράφουμε

Ανοιχτά προβλήματα και διπλωματικές

- Η περιοχή είναι ιδιαίτερα ενεργή ερευνητικά
- Αν ενδιαφέρεστε για διπλωματικές, υπάρχουν πολλά θέματα όπως:
  - Βυζαντινό πρόβλημα και επεκτάσεις
  - Ενοποίηση συστημάτων όπως tor + namecoin
  - Πρακτικό «σπάσιμο» αληθινών κρυπτογραφικών πρωτοκόλλων με side-channel μεθόδους
  - Υλοποίηση αμυνών στο παραπάνω