Α31 ΚΡΥΠΤΟΓΡΑΦΙΑ

10 Φεβρουαρίου 2022

1. Εισαγωγή
    - Ιστορικοί κώδικες
    - Τι είναι κρυπτοσύστημα;
    - Τι σημαίνει ασφάλεια;
2. One-Time-Pad
    - Ορισμός ασφάλειας
    - Απόδειξη ασφάλειας
3. Κρυπτοσυστήματα ροής (Stream Ciphers)
    - Ψευδοτυχαίες γεννήτριες αριθμών (PRG)
    - Κρυπτοσυστήματα ροής
    - Two-Time-Pad
    - Ορισμός ασφάλειας PRG
    - Ορισμός ασφάλειας Steam Cipher
    - Παραδείγματα
4. Τμηματικά Κρυπτοσυστήματα (Block Ciphers)
    - Ψευδοτυχαίες γεννήτριες συναρτήσεων (PRF)
    - Ψευδοτυχαίες γεννήτριες μεταθέσεων (PRP)
    - Ορισμοί ασφαλείας
    - Θεωρήματα ισοδυναμίας PRF, PRP, PRG
    - Feistel networks
    - DES, AES

- Θέσεις λειτουργίας (modes of operation)
- Ορισμός ασφάλειας

5. Κώδικες πιστοποίησης αυθεντικότητας (MAC)
    - Ορισμός MAC
    - Ορισμός ασφάλειας
    - ECBC-MAC, PMAC
    - Collision resistant hash functions
6. Πρωτόκολλο δημιουργίας κοινού κλειδιού
    - Το πρωτόκολλο Diffie-Hellman
    - Τα προβλήματα DL, DH, DDH
7. Πιστοποίηση πρώτων
    - Fermat test
    - Rabin-Miller test
8. Το πρόβλημα του διακριτού λογαρίθμου (DL)
    - Αλγόριμος Baby Step/Giant Step
    - Διάσπαση Pohlig-Hellman
    - Index Calculus method
9. Κρυπτογράφηση δημοσίου κλειδιού
    - Κρυπτοσύστημα ElGamal
    - Κρυπτοσύστημα RSA
10. Το πρόβλημα της παραγοντοποίησης
    - Μέθοδος ρ του Pollard
    - Μέθοδος του Fermat
    - Γραμμικό κόσκινο
    - Μέθοδος p-1
11. Ψηφιακές υπογραφές
    - Υπογραφές ElGamal
    - Υπογραφές RSA