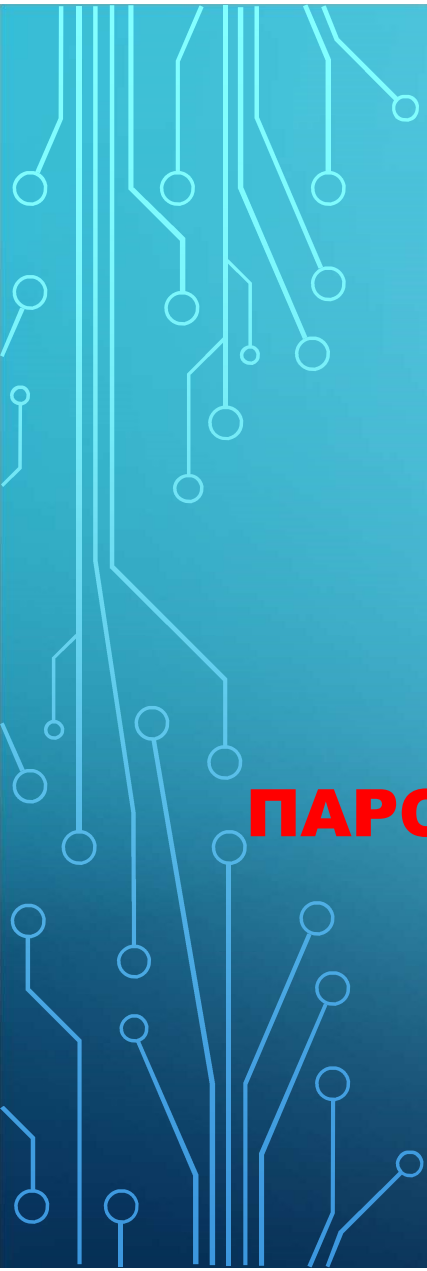




994- ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ BLOCKCHAIN ΕΦΑΡΜΟΓΕΣ

ΠΑΡΟΥΣΙΑΣΗ ΜΑΘΗΜΑΤΟΣ ΚΑΙ ΤΡΟΠΟΣ ΕΞΕΤΑΣΗΣ

ΣΚΟΠΟΣ ΤΟΥ ΜΑΘΗΜΑΤΟΣ

Το μάθημα φιλοδοξεί να μυήσει τον φοιτητή στην κρυπτογραφία, η οποία αποτελεί επιστημονικό κλάδο της Κρυπτολογίας, και κατά συνέπεια πραγματεύεται την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης/αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

ΣΚΟΠΟΣ ΤΟΥ ΜΑΘΗΜΑΤΟΣ

Έτσι, στόχος του μαθήματος είναι η κατανόηση των αντιπροσωπευτικότερων κλασσικών και μοντέρνων τεχνικών κρυπτογραφίας και κρυπτανάλυσης, η κατανόηση των μαθηματικών εννοιών που θα αποτελέσουν τα θεμέλια για την περιγραφή των κρυπτογραφικών τεχνικών κρυπτογράφησης και ψηφιακής υπογραφής, αλλά και των αρχών λειτουργίας των μοντέρνων κρυπτοσυστημάτων.

ΣΚΟΠΟΣ ΤΟΥ ΜΑΘΗΜΑΤΟΣ

Επίσης, στόχος είναι η εξοικείωση με τους μηχανισμούς δημόσιου κλειδιού (ΔΚ) που χρησιμοποιούνται για την προστασία της εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας των μηνυμάτων που ανταλλάσσονται μεταξύ απομακρυσμένων οντοτήτων σε μη ασφαλή δίκτυα.

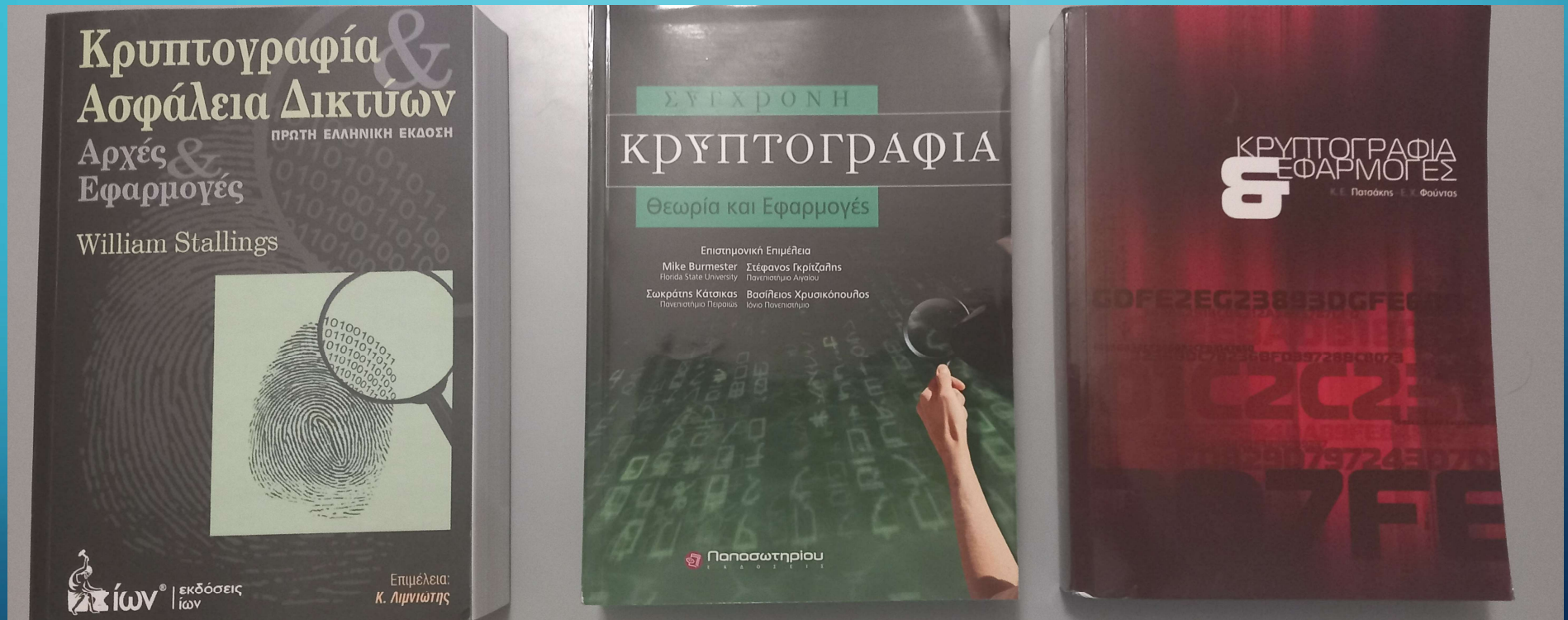
Τέλος θα μελετήσουμε την σύγχρονη τάση της κβαντικής κρυπτογραφίας και κβαντικής υπολογιστικής, η οποία υπόσχεται ένα πολύ γρηγορότερο, ικανότερο και ασφαλέστερο (ή επικινδυνότερο) ψηφιακό περιβάλλον.

ΕΝΔΕΙΚΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

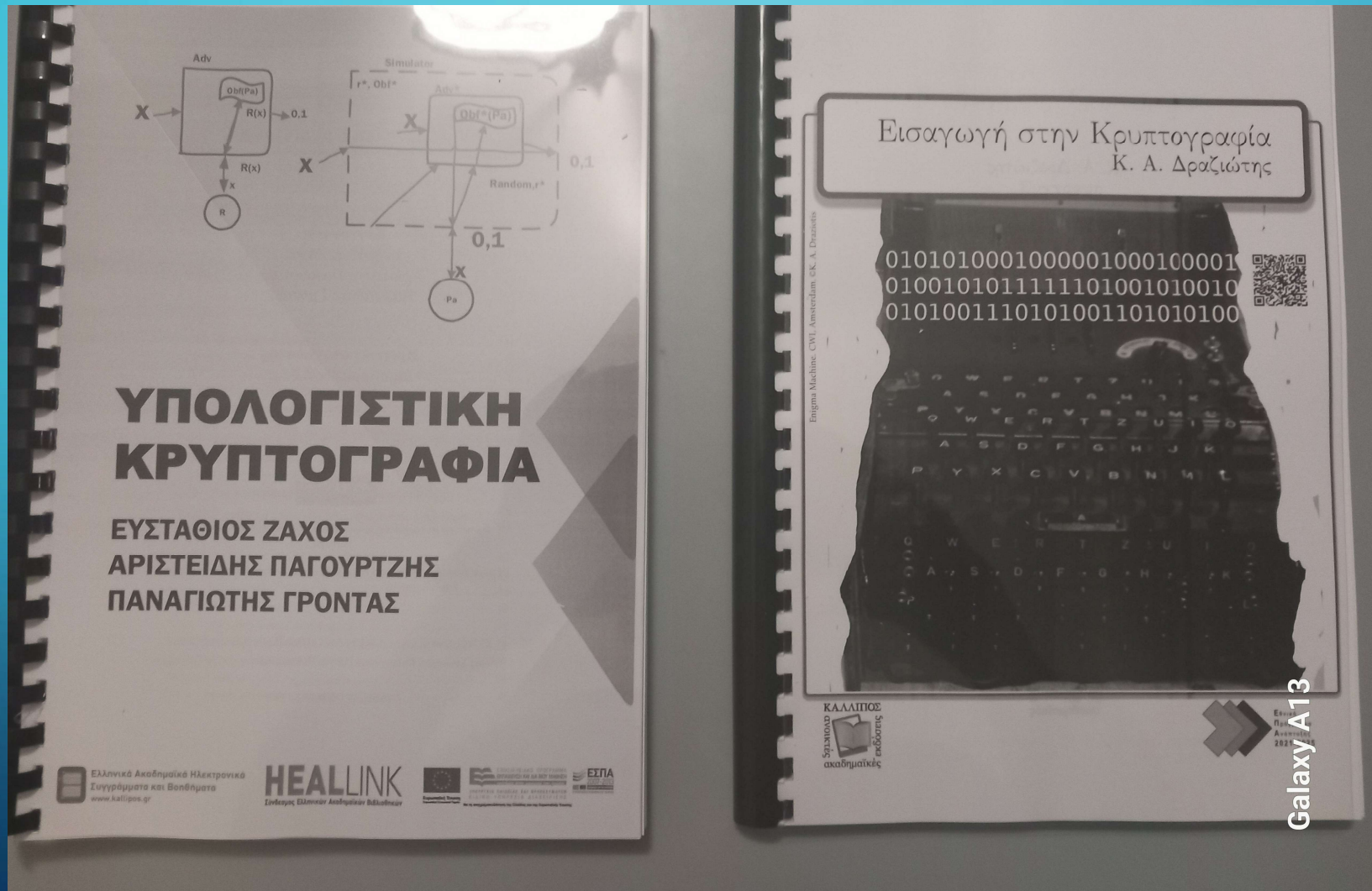
- Κωνσταντίνος Πατσάκης, Ευάγγελος Φούντας, *Κρυπτογραφία και Εφαρμογές*, Εκδόσεις Βαρβαρήγου, 2016 (*)
- William Stallings, *Κρυπτογραφία και Ασφάλεια Δικτύων – Αρχές και Εφαρμογές*, Εκδόσεις ΜΑΡΙΑ ΠΑΡΙΚΟΥ & ΣΙΑ ΕΠΕ, 2011 (*)
- M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας. Β. Χρυσικόπουλος, *Σύγχρονη Κρυπτογραφία – Θεωρία και Εφαρμογές*, Παπασωτηρίου
- Σημειώσεις διδάσκοντα στο e-class και αναρτημένα ηλεκτρονικά συγγράμματα (βλέπε μεθεπόμενη διαφάνεια)

(* Προτεινόμενο από τον διδάσκοντα)

ΕΝΔΕΙΚΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ



ΕΝΔΕΙΚΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ



ΒΑΘΜΟΛΟΓΙΑ ΣΤΟ ΜΑΘΗΜΑ

- Η αξιολόγηση στο μάθημα θα διαμορφωθεί από τη συμμετοχή σε ασκήσεις που θα αξιολογηθούν εντός της διάρκειας των διαλέξεων και από την εξέταση στο τέλος του εξαμήνου.
- **ΒΑΘΜΟΣ = 80% γραπτή εξέταση + 20% ασκήσεις (φυσική παρουσία)**

ΚΑΛΗ ΑΡΧΗ !!!