Τίτλος Μαθήματος:	Εισαγωγή στην Κρυπτογραφία
Κωδικός Μαθήματος:	MAT363
Κατηγορία Μαθήματος: **(Υποχρεωτικό/Επιλεγόμενο)**	Επιλεγόμενο
Επίπεδο Μαθήματος: **(πρώτου, δεύτερου ή τρίτου κύκλου)**	Πτυχίο (1ος κύκλος)
Έτος Σπουδών:	3 ή 4
Τετράμηνο προσφοράς Μαθήματος:	5, 6, 7 ή 8
Αριθμός ECTS:	6
Όνομα Διδάσκοντος:	Θα ανακοινωθεί

Μαθησιακά Αποτελέσματα Μαθήματος:

Με την ολοκλήρωση του μαθήματος ο διδασκόμενος αναμένεται να είναι σε θέση να:

- Ανακαλεί και να προσδιορίσει τις βασικές αρχές κρυπτογραφίας
- Κάνει χρήση των βασικών δομών και των εργαλείων από την αφηρημένη άλγεβρα και την θεωρία αριθμών που σχετίζονται με την κρυπτογραφία
- Προσδιορίσει και να αναγνωρίσει διάφορες μεθόδους κρυπτογράφησης
- Υλοποιεί κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων χρησιμοποιώντας συμμετρική κρυπτογραφία και κρυπτογραφία δημόσιου κλειδιού

Τρόπος Διδασκαλίας:	Διδασκαλία στην τάξη
Προαπαιτούμενο(α) και Συναπαιτούμενο(α) Μάθημα(τα):	MAT223
Προτεινόμενα/προαιρετικά μέρη του προγράμματος:	Κανένα

Περιεχόμενο Μαθήματος:

Σκοπός:
Να εισαγάγει τον φοιτητή σε βασικές έννοιες και αποτελέσματα από τον χώρο της κρυπτογραφίας. Παρουσιάζονται συστήματα κρυπτογράφησης και αποκρυπτογράφησης και αναπτύσσονται όλες οι μαθηματικές δομές και τα εργαλεία που χρειάζονται για την αξιόπιστη κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων.

Περιγραφή:
Εισαγωγή και ιστορική αναδρομή στην κρυπτογραφία, θεμελιώδεις στόχοι.
Πεδία ορισμού και τιμών κρυπτογράφησης, μετασχηματισμοί κρυπτογράφησης και

αποκρυπτογράφησης, επίτευξη εμπιστευτικότητας, ασφάλεια.
Κρυπτογράφηση συμμετρικού κλειδιού:
Ανασκόπηση των κρυπτοσυστημάτων πακέτου (blockciphers) και ρεύματος (streamciphers), κρυπτοσυστήματα αντικατάστασης, ομοφωνικά και πολυαλφαβητικά κρυπτοσυστήματα, το κρυπτοσύστημα Vinegere, κρυπτοσυστήματα αντιμετάθεσης (transpositionciphers), σύνθεση και γινόμενα κρυπτοσυστημάτων, το κρυπτοσύστημα Vernam, one-timepad.
Προαπαιτούμενες γνώσεις μαθηματικών:
Διαιρετότητα ακεραίων, αναπαραστάσεις ακεραίων, χρήση Ο-συμβολισμού, κόστος της πρόσθεσης, του πολλαπλασιασμού και της διαίρεσης με υπόλοιπο, μέγιστος κοινός διαιρέτης, Ευκλείδειος και γενικευμένος Ευκλείδειος αλγόριθμος, θεμελιώδες θεώρημα της αριθμητικής, θεώρημα πρώτων αριθμών, αριθμητική των ακεραίων modulo n.
Ημιομάδες, ομάδες, δακτύλιοι, η πολλαπλασιαστική ομάδα των ακεραίων modulo n, η συνάρτηση φ του Euler, τάξη στοιχείου και γεννήτορες στην πολλαπλασιαστική ομάδα των ακεραίων modulo n, δομή της πολλαπλασιαστικής ομάδας των υπολοίπων modulo έναν πρώτο αριθμό, τετραγωνικά υπόλοιπα modulo n, τετραγωνικές ρίζες modulo n, το θεώρημα του Euler, το μικρό θεώρημα του Fermat, ταχεία εκθετικοποίηση, Κινέζικο θεώρημα υπολοίπων.
Κρυπτογράφηση δημόσιου κλειδιού: Κρυπτοσυστήματα RSA, γεννήτορας κλειδιού, ασφάλεια μυστικού κλειδιού, κρυπτογράφηση Rabin, ανταλλαγή κλειδιού Diffie-Hellman, διακριτοί λογάριθμοι, κρυπτογράφηση ElGamal.

Απαιτούμενα ή Προτεινόμενα Εγχειρίδια:	A.Menezes, P. van Oorschot & S. Vanstone, Handbook of Applied Cryptography, CRC Press. J. A. Buchmann, Introduction to Cryptography, Springer. B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, Wiley. S. Singh, Code Book, Fourth Estate
Διδακτική Μεθοδολογία:	Διδασκαλία / θεωρία 28 ώρες Πρακτική / Ασκήσεις 14 ώρες Καθοδήγηση 15 ώρες
Αξιολόγηση:	Εξετάσεις 95% Συμμετοχή στο μάθημα 5% 100%
Γλώσσα Διδασκαλίας:	Ελληνική

Πρακτική Άσκηση:	Όχι
Χώρος Διδασκαλίας:	Αίθουσα Διδασκαλίας Ευρωπαϊκό Πανεπιστήμιο Κύπρου, Λευκωσία