ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ		
ΤΜΗΜΑ	ΜΑΘΗΜΑΤΙΚΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΠΡΟΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**62203**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**6^{ο}**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	ΠΕΠΕΡΑΣΜΕΝΑ ΣΩΜΑΤΑ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΙΑ		

ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ *σε περίπτωση που οι πιστωτικές μονάδες απονέμονται σε διακριτά μέρη του μαθήματος π.χ. Διαλέξεις, Εργαστηριακές Ασκήσεις κ.λπ. Αν οι πιστωτικές μονάδες απονέμονται ενιαία για το σύνολο του μαθήματος αναγράψτε τις εβδομαδιαίες ώρες διδασκαλίας και το σύνολο των πιστωτικών μονάδων*	**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Διαλέξεις	4	5
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (δ).	4	5

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *γενικού υποβάθρου, ειδικού υποβάθρου, ειδίκευσης γενικών γνώσεων, ανάπτυξης δεξιοτήτων*	Ειδικού Υποβάθρου (μάθημα επιλογής στην επιστημονική περιοχή «Άλγεβρα & Γεωμετρία»)
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	Όχι
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Ναι (στην αγγλική γλώσσα, για φοιτητές Erasmus)
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	http://math.uth.gr/?page_id=721

(2) ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα

Περιγράφονται τα μαθησιακά αποτελέσματα του μαθήματος οι συγκεκριμένες γνώσεις, δεξιότητες και ικανότητες καταλλήλου επιπέδου που θα αποκτήσουν οι φοιτητές μετά την επιτυχή ολοκλήρωση του μαθήματος.

Συμβουλευτείτε το Παράρτημα Α

- *Περιγραφή του Επιπέδου των Μαθησιακών Αποτελεσμάτων για κάθε ένα κύκλο σπουδών σύμφωνα με το Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης*
- *Περιγραφικοί Δείκτες Επιπέδων 6, 7 & 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης και το Παράρτημα Β*
- *Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων*

Στο μάθημα γίνεται συστηματική και σε βάθος ανάπτυξη της Θεωρίας Αριθμών, της Θεωρίας Πεπερσμένων Σωμάτων καθώς και ορισμένων εφαρμογών τους, όπως η Κρυπτογραφία.

Με την επιτυχή παρακολούθηση και ολοκλήρωση του μαθήματος η φοιτήτρια/ο φοιτητής θα είναι σε θέση:

- Να γνωρίζει βασικές έννοιες και αποτελέσματα της Θεωρίας Πεπερασμένων Σωμάτων.
- Να κατασκευάσει και να χρησιμοποιήσει, συμμετρικά κρυπτοσυστήματα τύπου Feistel (όπως το DES).
- Να γνωρίζει το πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman.

- Να κατασκευάζει συστήματα κρυπτογράφησης δημόσιου κλειδιού (όπως το RSA και το ElGamal), συστήματα ψηφιακών υπογραφών (όπως το RSA και το ElGamal).
- Να αντιλαμβάνεται τα βασικά προβλήματα που σχετίζονται με τα παραπάνω συστήματα.

Γενικές Ικανότητες

Λαμβάνοντας υπόψη τις γενικές ικανότητες που πρέπει να έχει αποκτήσει ο πτυχιούχος (όπως αυτές αναγράφονται στο Παράρτημα Διπλώματος και παρατίθενται ακολούθως) σε ποια / ποιες από αυτές αποσκοπεί το μάθημα;.

Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών	*Σχεδιασμός και διαχείριση έργων*
Προσαρμογή σε νέες καταστάσεις	*Σεβασμός στη διαφορετικότητα και στην πολυπολιτισμικότητα*
Λήψη αποφάσεων	*Σεβασμός στο φυσικό περιβάλλον*
Αυτόνομη εργασία	*Επίδειξη κοινωνικής, επαγγελματικής και ηθικής υπευθυνότητας και ευαισθησίας σε θέματα φύλου*
Ομαδική εργασία	*Άσκηση κριτικής και αυτοκριτικής*
Εργασία σε διεθνές περιβάλλον	*Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης*
Εργασία σε διεπιστημονικό περιβάλλον	*……*
Παράγωγή νέων ερευνητικών ιδεών	*Άλλες…*
	…….

Με την επιτυχή παρακολούθηση και ολοκλήρωσή του, το μάθημα αποσκοπεί στο να έχει αποκτήσει η φοιτήτρια/ο φοιτητής τις παρακάτω ικανότητες:

- Αυτόνομη εργασία
- Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης
- Αναλυτική και συνθετική σκέψη
- Κριτική σκέψη
- Επίλυση προβλημάτων

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

- Στοιχειώδης Θεωρία αριθμών στους ακέραιους, βασικά στοιχεία θεωρίας δακτυλίων, δακτύλιος πηλίκο, ομομορφισμοί, ιδεώδη.
- Νόμος τετραγωνικής αντιστροφής, τετραγωνικά υπόλοιπα, αθροίσματα Gauss.
- Επεκτάσεις σωμάτων, στοιχεία θεωρίας Galois.
- Ο τελεστής του Frobenius, N-στες ρίζες της μονάδες.
- Ανάγωγα πολυώνυμα σε πεπερασμένα σώματα, ο κυκλοτομικός νόμος αντιστροφής, προσθετικά πολυώνυμα.
- Απλά κρυπτοσυστήματα, Vigenere, Hill, μεταθέσεων, ροής. Κρυπτανάλυση.
- Κρυπτοσυστήματα ανοικτού κλειδιού, RSA, baby step-giant step.
- Ελλειπτικές καμπύλες, τάξεις σημείων, το θεώρημα του Mordel.
- Ελλειπτικά κρυπτοσυστήματα, παραγοντοποίηση με ελλειπτικές καμπύλες.
- Κατασκευή ελλειπτικών καμπυλών με δεδομένη τάξη.

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Πρόσωπο με πρόσωπο, στο αμφιθέατρο.
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	Υποστήριξη εκπαιδευτικής διαδικασίας μέσω της ηλεκτρονικής πλατφόρμας e-class Χρήση Τ.Π.Ε. στην επικοινωνία με τους φοιτητές (e-mail, ανακοινώσεις μέσω της ηλεκτρονικής πλατφόρμας e-class) Υποστήριξη Μαθησιακής διαδικασίας μέσω της ηλεκτρονικής πλατφόρμας e-class

ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ

Περιγράφονται αναλυτικά ο τρόπος και μέθοδοι διδασκαλίας.
Διαλέξεις, Σεμινάρια, Εργαστηριακή Άσκηση, Άσκηση Πεδίου, Μελέτη & ανάλυση βιβλιογραφίας, Φροντιστήριο, Πρακτική (Τοποθέτηση), Κλινική Άσκηση, Καλλιτεχνικό Εργαστήριο, Διαδραστική διδασκαλία, Εκπαιδευτικές επισκέψεις, Εκπόνηση μελέτης (project), Συγγραφή εργασίας / εργασιών, Καλλιτεχνική δημιουργία, κ.λπ.

Αναγράφονται οι ώρες μελέτης του φοιτητή για κάθε μαθησιακή δραστηριότητα καθώς και οι ώρες μη καθοδηγούμενης μελέτης σύμφωνα με τις αρχές του ECTS

Δραστηριότητα	***Φόρτος Εργασίας Εξαμήνου***
Διαλέξεις	52
Μελέτη θεωρίας	25
Μελέτη, προετοιμασία και συγγραφή εργασιών	23
Μελέτη για τελική εξέταση	25
Σύνολο Μαθήματος (25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα)	125

ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ

Περιγραφή της διαδικασίας αξιολόγησης

Γλώσσα Αξιολόγησης, Μέθοδοι αξιολόγησης, Διαμορφωτική ή Συμπερασματική, Δοκιμασία Πολλαπλής Επιλογής, Ερωτήσεις Σύντομης Απάντησης, Ερωτήσεις Ανάπτυξης Δοκιμίων, Επίλυση Προβλημάτων, Γραπτή Εργασία, Έκθεση / Αναφορά, Προφορική Εξέταση, Δημόσια Παρουσίαση, Εργαστηριακή Εργασία, Κλινική Εξέταση Ασθενούς, Καλλιτεχνική Ερμηνεία, Άλλη / Άλλες

Αναφέρονται ρητά προσδιορισμένα κριτήρια αξιολόγησης και εάν και που είναι προσβάσιμα από τους φοιτητές.

1. Γραπτή τελική εξέταση (100% του τελικού βαθμού) στην ελληνική γλώσσα με τη μορφή:
   - Ερωτήσεων ανάπτυξης.
   - Ερωτήσεων ανοιχτού τύπου/Σύντομης απάντησης/ πολλαπλής επιλογής με πλήρη τεκμηρίωση των απαντήσεων.
2. Ατομικές εργασίες, η βαθμολογία των οποίων συνυπολογίζεται στον τελικό βαθμό.
3. Προφορικές εξετάσεις (όταν προβλέπεται).
4. Ο τρόπος και τα κριτήρια αξιολόγησης είναι προσβάσιμα από τους φοιτητές μέσω της πλατφόρμας e-class.

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Βάρσος Δ., Στοιχεία Αλγεβρικής Θεωρίας Κωδίκων, Εκδ. Σοφία, 2009. Κωδικός βιβλίου στον Εύδοξο: 522
2. Πουλάκης Δ.Μ., Αλγεβρικοί κώδικες, Εκδ. Ζήτη, 2010. Κωδικός βιβλίου στον Εύδοξο: 10953
3. Πουλάκης Δ.Μ., Κρυπτογραφία, Εκδ. Ζήτη, 2004. Κωδικός βιβλίου στον Εύδοξο: 11068

Πρόσθετο Διδακτικό Υλικό

4. Κοντογεώργης Α., Αντωνιάδης Ι., Πεπερασμένα Σώματα και Κρυπτογραφία, Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα, - Αποθετήριο Κάλλιπος, 2016. Κωδικός βιβλίου στον Εύδοξο: 320009
5. Βάρσος Δ., Μια εισαγωγή στην Αλγεβρική Θεωρία Κωδίκων, Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα - Αποθετήριο Κάλλιπος, 2016. Κωδικός βιβλίου στον Εύδοξο: 320044