ΚΡΥΠΤΟΓΡΑΦΙΑ (ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ – ΕΠ)

ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ		
ΤΜΗΜΑ	ΜΑΘΗΜΑΤΙΚΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ		**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**ΧΕΙΜΕΡΙΝΟ**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	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	3	7.5
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (δ).		

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *γενικού υποβάθρου, ειδικού υποβάθρου, ειδίκευσης γενικών γνώσεων, ανάπτυξης δεξιοτήτων*	Επιλογής
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	Όχι
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Όχι
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	

(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*

Μετά την επιτυχή ολοκλήρωση του μαθήματος οι φοιτητές θα γνωρίζουν:

- να γνωρίζουν τους σκοπούς της κρυπτογραφίας δημόσιου κλειδιού και των ειδικών χρήσεών της (ανταλλαγή κλειδιών, ψηφιακή υπογραφή κτλ.),
- να γνωρίζουν τις αρχές λειτουργίας δημοφιλών κρυπτοσυστημάτων (RSA, ElGamal κτλ.),
- να γνωρίζουν στοιχεία της Θεωρίας Αριθμών απαραίτητα για την Κρυπτογραφία,
- να χρησιμοποιούν ελλειπτικές καμπύλες για κρυπτογραφικούς σκοπούς.

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

Με την επιτυχή παρακολούθηση και ολοκλήρωση του μαθήματος η φοιτήτρια/ο φοιτητής θα έχει αποκτήσει τις ακόλουθες ικανότητες:

- Αυτόνομη εργασία
- Ομαδική εργασία
- Προαγωγή της ελεύθερης και επαγωγικής σκέψης.
- Επίλυση προβλημάτων
- Προσαρμογή σε νέες καταστάσεις
- Κριτική σκέψη

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

- **Κρυπτογραφία ιδιωτικού κλειδιού.** Κρυπτοσυστήματα Καίσαρα, μονοαλφαβητική, διαλφαβητική και πολυαλφαβητική αντικατάσταση, πίνακες κρυπτογράφησης, το σημειωματάριο μιας χρήσης.
- **Κρυπτογραφία δημόσιου κλειδιού.** Στόχοι της κρυπτογραφίας δημόσιου κλειδιού, το σύστημα RSA, το πρόβλημα του διακριτού λογαρίθμου, η ανταλλαγή κλειδιών Diffie-Hellman, το κρυπτοσύστημα ElGamal, ψηφιακές υπογραφές (DES, DSS, Schnorr, ElGamal, RSA), κρυπτοσυστήματα σακιδίου, επιθέσεις σε κρυπτοσυστήματα δημόσιου κλειδιού.
- **Η Θεωρία αριθμών στην κρυπτογραφία.** Πρώτοι και ψευδοπρώτοι, Η μέθοδος παραγοντοποίησης ρ του Pollard, παραγοντοποίηση του Fermat.
- **Ελλειπτικές καμπύλες και κρυπτογραφία.** Εισαγωγή στις ελλειπτικές καμπύλες, Θεωρήματα Hasse και Weil, χρήση των ελλειπτικών καμπυλών στην κρυπτογραφία (διακριτός λογάριθμος, Diffie-Hellman, ElGamal).

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Πρόσωπο με πρόσωπο/Εξ αποστάσεως εκπαίδευση (το μάθημα είναι σχεδιασμένο έτσι ώστε να μπορεί να προσφέρεται κατά περίσταση και με εξ αποστάσεως διδασκαλία)
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 τις φοιτήτριες/τους φοιτητές (e-mail, ανακοινώσεις μέσω της ηλεκτρονικής πλατφόρμας e-class) Υποστήριξη Μαθησιακής διαδικασίας μέσω της ηλεκτρονικής πλατφόρμας e-class. Σε περίπτωση εξ' αποστάσεως διδασκαλίας χρησιμοποιούνται επιπλέον οι ιδρυματικές πλατφόρμες MS-TEAMS, MS-OFFICE (Forms κ.ο.κ.) και το BigBlueButton.
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ *Περιγράφονται αναλυτικά ο τρόπος και μέθοδοι διδασκαλίας.* *Διαλέξεις, Σεμινάρια, Εργαστηριακή Άσκηση, Άσκηση Πεδίου, Μελέτη & ανάλυση βιβλιογραφίας, Φροντιστήριο, Πρακτική*	

Δραστηριότητα	*Φόρτος Εργασίας Εξαμήνου*
Διαλέξεις	30
Ασκήσεις	9

(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*	Αυτοτελή μελέτη κατα τη διάρκεια του εξαμήνου: 74.25 Αυτοτελή μελέτη για την προετοιμασία για τις εξετάσεις: 74.25 Σύνολο Μαθήματος: 187.5
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.*	Ο τελικός βαθμός προκύπτει από την τελική εξέταση (100%). Ο τρόπος και τα κριτήρια αξιολόγησης είναι προσβάσιμα από τους φοιτητές μέσω της πλατφόρμας eclass.

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- N. Koblitz. *A Course in Number Theory and Cryptography* (Second Edition). Springer-Verlag, New York, 1994.
- R. Mollin. *An Introduction to Cryptography* (Second Edition). CRC Press, Boca-Raton, 2007.
- J. Katz and Y. Lindell. *Introduction to Modern Cryptography* (Second Edition). CRC Press, Boca Raton, 2015.