ΘΠ05 Κρυπτογραφία

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ		
ΤΜΗΜΑ	ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΠΡΟΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**ΘΠ05**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**8**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Κρυπτογραφία		

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-Φροντιστήριο	4 (3+1)	6
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (4).		

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *γενικού υποβάθρου, ειδικού υποβάθρου, ειδίκευσης γενικών γνώσεων, ανάπτυξης δεξιοτήτων*	ειδίκευσης γενικών γνώσεων
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	Κ17
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνικά
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Ναι
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://crypto.di.uoa.gr/class/

(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*

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

- αναφέρει τις βασικές έννοιες της κρυπτογραφίας
- περιγράφει βασικές κρυπτογραφικές εργασίες καθώς και κατασκευές που τις υλοποιούν, και να προσδιορίζει τα επίπεδα ασφάλειας στα οποία στοχεύουν
- αναγνωρίζει τα υπολογιστικά προβλήματα στα οποία στηρίζονται αυτές οι κατασκευές
- αναφέρει και να παράγει κρυπτογραφικούς ορισμούς για νέες κατασκευές, και να αναλύει ή να διαμορφώνει μαθηματικές αποδείξεις για την ασφάλεια αυτών
- συγκρίνει κρυπτογραφικές κατασκευές για την ίδια εργασία ως προς την ασφάλεια, απόδοση, απαιτήσεις και πολυπλοκότητα
- αναγνωρίζει τις προκλήσεις ως προς τη χρήση της κρυπτογραφίας σε εφαρμογές, και ιδιαίτερα τη σημασία και δυσκολία της ικανοποίησης των προϋποθέσεων ασφαλείας μιας θεωρητικής απόδειξης στην πράξη.

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	*……*
Παραγωγή νέων ερευνητικών ιδεών	*Άλλες…*

Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
Αυτόνομη εργασία
Άσκηση κριτικής και αυτοκριτικής
Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Έννοια της ασφάλειας, κρυπτογραφικά πρωτόκολλα και ορισμοί ασφάλειας, κρυπτανάλυση και επιθέσεις.
Στοιχεία θεωρίας ομάδων και πιθανοτήτων και θεωρίας πολυπλοκότητας.
Δύσκολα υπολογιστικά προβλήματα (RSA, Διακριτός Λογάριθμος).
Σχήματα ανταλλαγής κλειδιών (key exchange) (Diffie-Hellman).
Σχήματα κρυπτογράφησης, ορισμοί ασφάλειας και κατασκευές (ElGamal, RSA).
Σχήματα δέσμευσης, ορισμοί ασφάλειας και κατασκευές (Pedersen).

Ψηφιακές Υπογραφές, ορισμοί ασφάλειας και κατασκευές (RSA, Schnorr).
Μονόδρομες (one-way) συναρτήσεις και συναρτήσεις κρυφής εισόδου (trapdoor).
Πρωτόκολλα Μηδενικής γνώσης, ορισμοί ασφάλειας και κατασκευές (Schnorr, Chaum Pedersen, CDS).

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Πρόσωπο με πρόσωπο στην τάξη
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	Επικοινωνία μέσω email Ζωντανή μετάδοση διαλέξεων Ηλεκτρονική πλατφόρμα eclass για ερωτήσεις φοιτητών, ομάδες συζητήσεων, υποβολή και διόρθωση εργασιών και ανακοινώσεις.
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	39
Φροντιστήρια	13
Προετοιμασία για Διαλέξεις	13
Προετοιμασία για Φροντιστήρια	26
Εργασίες	10
Ατομική Μελέτη	26
Επανάληψη για εξετάσεις.	23
Σύνολο Μαθήματος	**150**

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.*	Γραπτή Εξέταση (τελική) 80% Εργασίες (2 μέσα στο εξάμηνο) 20%

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

J. Katz and Y. Lindel Introduction to Modern Cryptography

I. Damgard On Σ-Protocols

V. Shoup A Computational Introduction to Number Theory and Algebra

S. Galbraith Mathematics of Public Key Cryptography

A. Menezes, P. van Oorschot, and S. A. Vanstone Handbook of Applied Cryptography

Σημειώσεις σε μορφή PDF (Διαθέσιμες στην αρχή του μαθήματος)