ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ		
ΤΜΗΜΑ	ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**M122**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**2**
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+ Εργαστηριακές ασκήσεις (Φροντιστήριο)		3+1=4	
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*			
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:			
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνικά ή/και Αγγλικά		
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS			
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://crypto.di.uoa.gr/class/Kryptographia/index.html		

(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*

- **Γνωρίζει τους βασικούς ορισμούς της σύγχρονης κρυπτογραφίας, τις συμβάσεις που επικρατούν στο χώρο και κατανοεί τον τρόπο μοντελοποίησης της ασφάλειας μέσω ενός αντιπάλου.**
- **Γνωρίζει σύγχρονα κρυπτογραφικά εργαλεία, το είδος και το επίπεδο ασφάλειας που παρέχουν, και τις προϋποθέσεις υπό τις οποίες το παρέχουν.**
- **Είναι σε θέση να εξετάσει την ένταξη ενός κρυπτογραφικού αντικειμένου σε ένα σύστημα, και να εκτιμήσει την απόδοσή του**

μέσα σε αυτό.

- **Είναι σε θέση να εκτιμήσει την επίπτωση αλλαγών σε κάποιο αντικείμενο ή την λειτουργία ενός συνδυασμού αντικειμένων.**
- **Είναι σε θέση να αναλύσει και να αξιολογήσει νέα κρυπτογραφικά εργαλεία όμοια με όσα ήδη γνωρίζει.**
- **Είναι σε θέση να κατανοήσει και να εξηγήσει καινούριες έννοιες ασφάλειας και λειτουργικότητας καθώς και τα ανάλογα εργαλεία.**

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…*
	…….

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

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

- Βασική θεωρία πιθανοτήτων, Στατιστική απόσταση, έννοια αμελητέας ποσότητας
- Εισαγωγή στη θεωρία Ομάδων
- Στοιχεία θεωρίας αριθμών (Ομάδες ακεραίων modp, modN)
- Στοιχεία πολυπλοκότητας (κόστος πράξεων σε ομάδα, αλγόριθμος Ευκλείδη για αντιστροφή στοιχείων, αλγόριθμος square & multiply)
- Υπολογιστικά προβλήματα (Διακριτός λογάριθμος, παραγοντοποίηση ακεραίων, προβλήματα DDH, CDH)
- Στοιχειώδεις εφαρμογές (Coin Tossing)
- Σχήματα δέσμευσης (Ορισμοί, παραλλαγές, σχήμα Pedersen)
- Σχήματα Συμφωνίας Κλειδιών (Ορισμοί, Diffie Hellman)
- Στοιχεία συμμετρικής κρυπτογραφίας (Συναρτήσεις κατακερματισμού, κρυπτογράφησης)
- Ψηφιακές Υπογραφές (Ορισμοί, RSA,ECDSA)
- Κρυπτογραφία δημοσίου κλειδιού (Ορισμοί, ασφάλεια IND-CPA, IND-CCA, RSA, Elgamal)
- Πρωτόκολλα μηδενικής γνώσης (Ορισμοί, εγκυρότητα γνώσης & ειδική εγκυρότητα, πρωτόκολο Schnorr, μη διαδραστικά πρωτόκολα, μετασχηματισμός Fiat Shamir, λογική σύζευξη και διάζευξη - Μετασχηματισμοί CDS, πρωτόκολα για το NP)
- Ειδικά θέματα επιλεγμένα ανάλογα με την επικαιρότητα και τα ενδιαφέροντα των φοιτητών (Ενδεικτικά: διαμοίραση μυστικών, κατανεμημένοι υπολογισμοί με πολλαπλούς παίκτες, ευπάθειες σε υλοποιήσεις του ECDSA, ασθενής μετασχηματισμός Fiat-Shamir και ευπάθειες σε υλοποιήσεις συστημάτων μηδενικής γνώσης)

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ

Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.

Διαλέξεις θεωρίας: πρόσωπο με πρόσωπο

Ασκήσεις Φροντιστηρίου: πρόσωπο με πρόσωπο

Συζήτηση eclass: εξ αποστάσεως

Σχολιασμός εργασιών: μικτά

ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές

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
Ανακεφαλαίωση Διαλέξεων	19
Μελέτη σημειώσεων	50
Μελέτη βιβλιογραφίας	10
Συμμετοχή στο eclass	3
Φροντιστήριο	11
Προετοιμασία Ασκήσεων	16
Μελέτη Λυμένων Ασκήσεων	11
Γραπτές Εργασίες	20
Σύνολο Μαθήματος	

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.

- 2 Γραπτές εργασίες επίλυσης προβλημάτων.
- Γραπτή εξέταση με συνδιασμό:
  - Ερωτημάτων πολλαπλής επιλογής
  - Ερωτήσεων σύντομης απάντησης
  - Επίλυσης προβλημάτων/ ανοικτού τύπου.

Ο βαθμός προκύπτει από το άθροισμα των δύο εργασιών με συντελεστή 1, και της γραπτής εξέτασης με συντελεστή 9, με μέγιστο το 10.

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

-Προτεινόμενη Βιβλιογραφία:

- *Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές των Burmester, Γκρίτζαλη , Κάτσικα , Χρυσικόπουλου*
- *Βασικές αρχές θεωρίας κωδικοποίησης και κρυπτογραφίας των C. A. Rodger, C. C. Lindner, D. A. Leonard, D. G. Hoffman, D. R. Hankerson, J.R. Wall, K. T. Phelps*
- *Introduction to Modern Cryptography: Third Edition, των Katz και Lindell*
- *A Computational Introduction to Number Theory and Algebra του V. Shoup*
- *Mathematics of Public Key Cryptography του S. Galbraith*
- *Handbook of Applied Cryptography, των A. Menezes, P. van Oorschot, and S. A. Vanstone.*

- Συναφή επιστημονικά περιοδικά:

- *Journal of Cryptology, Springer*