

ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	Προπτυχιακό		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	ECE_K740	ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ	7
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Ασφάλεια Υπολογιστικών Συστημάτων		
ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ <i>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</i>		ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ	ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ
Διαλέξεις		3	
Φροντιστήριο / Ασκήσεις Πράξης		1	
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (4).		4	5
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ <i>γενικού υποβάθρου, ειδικού υποβάθρου, ειδικευσης γενικών γνώσεων, ανάπτυξης δεξιοτήτων</i>	Ειδικού Υποβάθρου		
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:			
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνικά		
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Όχι		
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://www.ece.uop.gr		

(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 αυτό δίνονται οι βασικές έννοιες για την κρυπτογραφία και πως οι έννοιες αυτές χρησιμοποιούνται γενικότερα στην ασφάλεια των υπολογιστικών συστημάτων. Πιο συγκεκριμένα δίνονται οι έννοιες των συμμετρικών και ασύμμετρων αλγορίθμων κρυπτογραφίας, αναφέρονται πολύ βασικές έννοιες της θεωρίας αριθμών που είναι απαραίτητες για την κατανόηση των αλγορίθμων κρυπτογραφίας, έπειτα αναλύονται οι ιδιότητες των αλγορίθμων κρυπτογραφίας και οι βασικές δομές που χρησιμοποιούνται στο σχεδιασμό ασφαλών αλγορίθμων κρυπτογραφίας. Μετά γίνεται εκτενής αναφορά στους συμμετρικούς, ασύμμετρους αλγορίθμους και στις συναρτήσεις κατακερματισμού και δίνονται αρκετά παραδείγματα τέτοιων αλγορίθμων που έχουν χρησιμοποιηθεί και χρησιμοποιούνται σήμερα. Ακολουθεί ο τρόπος διαχείρισης των κλειδιών σε ένα σύστημα ασφάλειας καθώς επίσης αναλύονται οι ψηφιακές υπογραφές. Επιπρόσθετα, δίνονται

αρκετά στοιχεία για σύγχρονα κρυπτογραφικά πρωτόκολλα και μεθόδους που χρησιμοποιούνται σε σύγχρονα συστήματα ασφάλειας υπολογιστικών συστημάτων.

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

Σε επίπεδο Γνώσεων:

- Γνωρίζει πλήρως όλες τις βασικές έννοιες που είναι απαραίτητες για την κατανόηση της κρυπτογραφίας
- Κατέχει τις βασικές έννοιες της ασφάλειας υπολογιστικών συστημάτων
- Γνωρίζει όλα τα είδη των κρυπτογραφικών συναρτήσεων καθώς και τις ιδιότητές τους
- Υλοποιεί αλγορίθμους κρυπτογραφίας και κρυπτογραφικά πρωτόκολλα τόσο σε software όσο και σε hardware
- Επιλέγει τις κατάλληλες μεθοδολογίες ενάντια σε ευπάθειες ενός πληροφοριακού συστήματος

Σε επίπεδο Δεξιοτήτων:

- Εφαρμόζει τα κρυπτογραφικά πρωτόκολλα
- Χρησιμοποιεί τα κρυπτογραφικά πρωτόκολλα και τις εφαρμογές τους
- Διαχειρίζεται σύγχρονες μεθόδους και τεχνικές για την ασφάλεια επικοινωνιών (κυψελοειδών, ασύρματων-ενσύρματων δικτύων κλπ)
- Αναλύει ένα πρόβλημα ασφάλειας και βρίσκει αντίμετρα

Σε επίπεδο Ικανοτήτων:

- Επιλογή των κατάλληλων συστατικών στοιχείων για τον σχεδιασμό ενός ασφαλούς συστήματος
- Συνδυάζει τα παραπάνω για την επίτευξη υψηλού επιπέδου ασφάλειας σε ένα πληροφοριακό σύστημα

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...

- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
- Λήψη αποφάσεων
- Αυτόνομη εργασία
- Ομαδική εργασία

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

1η εβδομάδα

Εισαγωγή- Βασικές Έννοιες Ασφάλειας

Βασική ορολογία

Γενικές κατευθύνσεις ασφάλειας

Επιθέσεις - Υπηρεσίες – Μηχανισμοί ασφάλειας

2η εβδομάδα

Επιλεκτικά Θέματα Θεωρίας Αριθμών και Ιδιότητες των Αλγορίθμων Κρυπτογραφίας

Αριθμητική modulus

Αλγόριθμος του Ευκλείδη

Πρώτοι αριθμοί

Πεπερασμένα σώματα

3η εβδομάδα

Συμμετρική Κρυπτογράφηση

Αρχές και μοντέλο συμμετρικής Κρυπτογράφησης

Τεχνικές αντικατάστασης και αντιμετάθεσης

Συμμετρικοί Αλγόριθμοι (DES, Triple-DES)

4η εβδομάδα

Συμμετρικοί Αλγόριθμοι των 128-bit (AES) και των 64-bit (KASUMI)

Αλγόριθμοι Τμημάτων (Block Ciphers): Τρόποι Λειτουργίας

Εισαγωγή στους αλγορίθμους ροής

Οι αλγόριθμοι ροής SNOW3G και GRAIN

5η εβδομάδα

Ασύμμετρη Κρυπτογράφηση

Αρχές Κρυπτογράφησης Δημοσίου Κλειδιού

Θεωρήματα Fermat και Euler

Διακριτοί λογάριθμοι

Ο Αλγόριθμος RSA

6η εβδομάδα

Συναρτήσεις Κατακερματισμού

Βασικές ιδιότητες

Οι αλγόριθμοι της οικογένειας SHA και ο Whirlpool

Ο HMAC και ο CMAC

7η εβδομάδα

Ψηφιακή Υπογραφή και Αυθεντικοποίηση Μηνύματος

Πρωτόκολλα αυθεντικοποίησης

Πρότυπο ψηφιακής υπογραφής

8η εβδομάδα

Διαχείριση κλειδιών και κρυπτογραφικά πρωτόκολλα

Ο Αλγόριθμος DIFFIE-HELLMAN

Εισαγωγή στις Ελλειπτικές Καμπύλες

9η εβδομάδα

Εισαγωγή στην Ασφάλεια Δικτύων και Ασφάλεια Ηλεκτρονικού Ταχυδρομείου

Kerberos

Pretty Good Privacy

Επισκόπηση και αρχιτεκτονική IPSec

10η εβδομάδα

Ασφάλεια Ασύρματων Δικτύων

Ασφάλεια κινητών συσκευών

Ασφάλεια ασύρματων LAN τύπου IEEE 802.11i

11η εβδομάδα

Εισαγωγή στον ασφαλή σχεδιασμό συστημάτων IoT

Ευπάθειες

Προκλήσεις ασφάλειας και απορρήτου

Τεχνικές ασφάλισης δεδομένων

12η εβδομάδα

Βασικά ζητήματα ασφάλειας στο Industry 4.0

Κυβερνοφυσικά συστήματα

Επιθέσεις σε SCADA συστήματα

Μέτρα ασφάλισης δεδομένων

13η εβδομάδα

Εισαγωγή στον ασφαλή σχεδιασμού υλικού πληροφοριακών συστημάτων

Επεξεργαστές και συν-επεξεργαστές κρυπτογραφίας

Επιταχυντές υλικού πρωτοκόλλων ασφαλείας

Ενσωματωμένοι επεξεργαστές ασφαλείας

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ <i>Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.</i>	Πρόσωπο με πρόσωπο στην τάξη και στο εργαστήριο. Εξ' αποστάσεως μέσω του συστήματος e-Class	
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ <i>Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές</i>	<ul style="list-style-type: none"> • Διαφάνειες (ppt) για τη διδασκαλία του θεωρητικού μέρους, οι οποίες θα αναρτιούνται μετά από κάθε διάλεξη στο e-Class. • Υποστήριξη μαθησιακής διαδικασίας μέσω της πλατφόρμας e-Class (για γνωστοποίηση του κανονισμού λειτουργίας μαθήματος, για διανομή διαφανειών, συμπληρωματικού υλικού, ανακοινώσεων, συνδέσμων και βιβλιογραφίας, για τη διεξαγωγή της τελικής εξέτασης κλπ). 	
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ <i>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</i>	Δραστηριότητα	Φόρτος Εργασίας Εξαμήνου
	Διαλέξεις	39
	Ασκήσεις Πράξης – Φροντιστήριο, που εστιάζουν στην επίλυση παραδειγμάτων και ασκήσεων	13
	Εκπόνηση εργασιών (project)	20
	Αυτοτελής μελέτη	53
	Σύνολο Μαθήματος	125 (5 ECTS)
ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ <i>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.</i>	I. Ενδιάμεση εξέταση (πρόοδος) (30%) που περιλαμβάνει: <ol style="list-style-type: none"> Επίλυση ασκήσεων Ερωτήσεις πολλαπλής επιλογής II. Γραπτή τελική εξέταση (70 %) που περιλαμβάνει: <ol style="list-style-type: none"> Επίλυση ασκήσεων Ερωτήσεις πολλαπλής επιλογής Συγκριτική αξιολόγηση στοιχείων θεωρίας Παρατηρήσεις: <ol style="list-style-type: none"> 1) Ο τελικός βαθμός προκύπτει από την στάθμιση των βαθμών της προόδου και της τελικής γραπτής εξέτασης 2) Η αξιολόγηση γίνεται στην ελληνική γλώσσα. 3) Η διαδικασία αξιολόγησης και τα κριτήρια αξιολόγησης είναι δημοσιευμένα στην ιστοσελίδα του μαθήματος στο e-Class. 	

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

-Προτεινόμενη Βιβλιογραφία :
-Συναφή επιστημονικά περιοδικά:

- 1) William Stallings, "Κρυπτογραφία για Ασφάλεια Δικτύων: Αρχές και Εφαρμογές", ΙΩΝ, 2011.
- 2) William Stallings και Lawrie Brown, "Ασφάλεια Υπολογιστών: Αρχές και Πρακτικές», Κλειδάριθμος, 2016.
- 3) Σ. Γκρίτζαλης, "Σύγχρονη κρυπτογραφία: Θεωρία και εφαρμογές", Παπασωτηρίου, 2010.
- 4) Β. Κάτος, Γ. Στεφανίδης, "Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης ", Ζυγός, 2003.