ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	Προπτυχιακό		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**ECE_ELE840**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**8**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Κυκλώματα και Συστήματα Κρυπτογραφίας και Ασφάλειας		

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	
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 *γενικού υποβάθρου, ειδικού υποβάθρου, ειδίκευσης γενικών γνώσεων, ανάπτυξης δεξιοτήτων*	Ειδίκευσης
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	Όχι. Συνιστάται στους φοιτητές να έχουν ήδη παρακολουθήσει το μάθημα: Ασφάλεια Υπολογιστικών Συστημάτων (ECE_K740)
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνικά
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Ναι
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*

Το μάθημα πραγματεύεται την ανάλυση αρχιτεκτονικών αλγορίθμων κρυπτογράφησης τόσο μυστικού όσο και δημοσίου κλειδιού με στόχο τον σχεδιασμό επεξεργαστών και συν-επεξεργαστών κρυπτογραφίας. Ιδιαίτερη μνεία γίνεται σε επιταχυντές υλικού πρωτοκόλλων ασφαλείας ενώ αναλύονται τρόποι σχεδιασμού για γεννήτριες τυχαίων και ψευδοτυχαίων αριθμών. Επίσης, παρουσιάζονται και αναλύονται οι φυσικές μη κλωνοποιημένες συναρτήσεις και η χρήση τους στην ασφάλεια. Ακόμα, αναλύονται ενσωματωμένοι επεξεργαστές ασφαλείας και σχολιάζονται οι εφαρμογές τους. Ορίζονται και αναλύονται επιθέσεις πλευρικού καναλιού και αντίμετρα καθώς και περιγράφεται τι είναι και πως λειτουργεί το ιομορφικό υλικό. Επίσης, περιγράφονται μέτρα για αντοχή στις παραπάνω επιθέσεις και σε παρεμβάσεις γενικότερα. Παρουσιάζεται και αναλύεται η χρήση έξυπνων καρτών σε συστήματα ασφαλείας και εμπορικές εφαρμογές. Επίσης, αναλύεται τι είναι και πως χρησιμοποιούνται τα FPGAs για εφαρμογές στη κρυπτογραφία καθώς και τι είναι οι πλατφόρμες υπολογιστικής εμπιστοσύνης. Τέλος, παρουσιάζονται κάποια βασικά πρακτικά ζητήματα των παραπάνω πεδίων μέσω εργαστηριακών ασκήσεων.

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

- Σχεδιάζει μέσω μεθοδολογιών σχεδιασμού συστήματα κρυπτογραφίας σε υλισμικό
- Διαχωρίζει τις επιθέσεις υλικού (επιθέσεις πλάγιου μονοπατιού, ιομορφικό υλισμικό κλπ)
- Σχεδιάζει συστήματα ενάντια σε επιθέσεις υλικού
- Μελετά και σχεδιάζει σύγχρονους μηχανισμούς ασφάλειας σε συστήματα υλισμικού
- Σχεδιάζει αποδοτικές αρχιτεκτονικές συστημάτων κρυπτογραφίας και ασφάλειας συστημάτων

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

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

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

1η : Εισαγωγή στην ασφάλεια υλικού – Μετρικές απόδοσης μιας υλοποίησης σε υλισμικό

Εισαγωγή στην ασφάλεια υλικού

Επιθέσεις σε συστήματα ασφάλειας

Μετρικές απόδοσης μιας υλοποίησης

Μετρικές χρονισμού

Ελάχιστη περίοδος ρολογιού

Διοχέτευση

2η: Αρχιτεκτονικές αλγορίθμων κρυπτογράφησης μυστικού κλειδιού

Υλοποιήσεις υψηλής ταχύτητας επεξεργασίας και Υλοποιήσεις με μικρό αριθμό πόρων υλικού

Αρχιτεκτονικές υλισμικού αλγόριθμων μυστικού κλειδιού (DES, 3DES, AES, MISTY1, KASUMI)

3η : Πρακτικά θέματα υλοποιήσεων αλγορίθμων μυστικού κλειδιού

Κώδικας VHDL του DES και του AES

4η: Αρχιτεκτονικές αλγορίθμων κρυπτογράφησης δημοσίου κλειδιού

Αρχιτεκτονικές υλισμικού αλγόριθμων δημοσίου κλειδιού (RSA, Ελλειπτικές Καμπύλες)

5η : Επεξεργαστές και συν-επεξεργαστές κρυπτογραφίας

IBM 4758

AEGIS: MIT Research Project

6η : Γεννήτριες τυχαίων και ψευδοτυχαίων αριθμών, φυσικές μη κλωνοποιημένες συναρτήσεις

Εισαγωγή – Χρήση τυχαίων αριθμών

Απαιτήσεις γεννητριών τυχαίων αριθμών

Ταξινόμηση - Ντετερμινιστικές έναντι μη ντετερμινιστικές γεννήτριες τυχαίων αριθμών

7η: Επιθέσεις σε υλισμικό

Η ανάγκη για ασφαλές υλικό (HardWare-HW)

Ορολογία

Cryptographic coprocessors/accelerators

Cryptographic chip cards/smart cards

8η : Ιομορφικό υλισμικό Εισαγωγή Τι είναι το Ιομορφικό υλισμικό Μέθοδοι ανίχνευσης Ιομορφικού υλισμικού 9η : Πρακτικά θέματα Ιόμορφου υλισμικού Παραδείγματα υλοποιήσεων Ιόμορφου υλισμικού Μέθοδοι ανίχνευσης σε FPGA 10η : Ασφαλής Σχεδιασμός σε FPGA (Μέρος Α) Εισαγωγή στα FPFA 11η : Ασφαλής Σχεδιασμός σε FPGA (Μέρος Β) Ασφάλεια στα FPGAs Τύποι Επιθέσεων Τρόποι Αντιμετώπισης 12^{η}: Πρακτικά θέματα ασφαλούς σχεδιασμού σε FPGA Μέθοδοι σχεδίασης και υλοποίησης ασφαλούς FPGA 13η : Φυσικές μη κλωνοποιημένες συναρτήσεις Ορισμός Είδη Εφαρμογές

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Πρόσωπο με πρόσωπο στην τάξη και στο εργαστήριο. Εξ΄ αποστάσεως μέσω του συστήματος e-Class
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	• 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 ενδιάμεσης και της τελικής εξέτασης κλπ).

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
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

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. Ενδιάμεση εξέταση (πρόοδος) (40%) που περιλαμβάνει:
   a. Επίλυση ασκήσεων
   b. Ερωτήσεις πολλαπλής επιλογής

II. Γραπτή τελική εξέταση (60%) που περιλαμβάνει:
   a. Επίλυση ασκήσεων
   b. Ερωτήσεις πολλαπλής επιλογής
   c. Συγκριτική αξιολόγηση στοιχείων θεωρίας

Παρατηρήσεις:

1) Ο τελικός βαθμός προκύπτει από την στάθμιση των βαθμών των δύο εξετάσεων θεωρίας με συντελεστές βαρύτητας 40% και 60%, αντίστοιχα.
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) Patric R. Shaumont, "Ένας Πρακτικός Οδηγός για τη Συσχεδίαση Υλικού και Λογισμικού», Εκδόσεις Νέων Τεχνολογιών, 2019.
2) Paris Kitsos and yan Zhang, "RFID Security: Techniques, Protocols and System-on-chip Design", Springer, 2008.
3) William Stallings, "Κρυπτογραφία για Ασφάλεια Δικτύων: Αρχές και Εφαρμογές", ΙΩΝ, 2011.