Προστασία δεδομένων και κρυπτογραφία

ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	Επιστήμης και Τεχνολογίας		
ΤΜΗΜΑ	Επιστήμης και Τεχνολογίας		
ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ	ΠΜΣ «Κυβερνοασφάλειας»		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	Μεταπτυχιακό		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	CC04	**ΕΞΆΜΗΝΟ**	2
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Προστασία δεδομένων και κρυπτογραφία		
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Επιλογής, υποχρεωτικό*	Υποχρεωτικό / Βασικό		
ΔΙΔΑΣΚΩΝ/ΟΥΣΑ (ΔΙΔΑΣΚΟΝΤΕΣ/ΟΥΣΕΣ)	Θεωρία: Καθηγητής Σταύρος Σταυρινίδης Εργαστήριο: Καθηγητής Σταύρος Σταυρινίδης		

ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ *σε περίπτωση που οι πς 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*	**ΕΒΔΟΜΑΔΙΑΙΕΣΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
	30h/13w=2.31	6
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (δ).		
ΑΝΑΛΥΣΗ ΔΙΔΑΚΤΙΚΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ	**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ**	
Θεωρία	2.00	
Εργαστήριο	0.31	
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*	Ειδικού Υπόβαθρου Ανάπτυξης Δεξιοτήτων
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	-
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Αγγλική
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Ναι
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://www.ihu.gr/ucips/postgraduate-programmes/cybersecurity

(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 ολοκλήρωση του μαθήματος, ο/η φοιτητής/τρια θα είναι σε θέση να:

- Αναπτύξει τις γνώσεις, την κατανόηση και τις δεξιότητες για να εργαστεί ως επαγγελματίας ασφάλειας υπολογιστών.
- Μάθει τις έννοιες, τις αρχές, τις τεχνικές και τις μεθοδολογίες που χρειάζεται για να σχεδιάσει και να αξιολογήσει πολύπλοκα δίκτυα, συστήματα και εφαρμογές, από την άποψη της ασφάλειας.
- Αναπτύξει την πρακτική εμπειρία που χρειάζεται για να σχεδιάσει, να εκτελέσει και να αξιολογήσει διαδικασίες προστασίας δεδομένων και κρυπτογράφησης.

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

Μαθησιακά Αποτελέσματα **Μαθησιακά Αποτελέσματα**

- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών.
- Λήψη αποφάσεων.
- Ομαδική εργασία.
- Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης.

(3) ΠΕΡΙΓΡΑΦΗ/ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Το μάθημα εισάγει θεμελιώδεις έννοιες Κρυπτογραφίας και εκτείνεται μέχρι εξειδικευμένα θέματα. Τα θέματα που καλύπτονται περιλαμβάνουν:

- Εισαγωγή.
- Θεωρία Αριθμών.
- Συμμετρική κρυπτογραφία.
- Ασύμμετρη κρυπτογραφία.
- Κρυπτογραφία δημόσιου κλειδιού.
- Ψηφιακές υπογραφές.
- Συναρτήσεις Hash.
- Χαοτική και κβαντική κρυπτογραφία

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Υβριδική διδασκαλία: Πρόσωπο με πρόσωπο και σύγχρονη εξ αποστάσεως εκπαίδευση
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	**Χρήση Τ.Π.Ε. στη Διδασκαλία** Κατά τη διδακτική διαδικασία αξιοποιούνται διάφορα ψηφιακά εργαλεία προσομοίωσης κυκλωμάτων και προγραμματισμού μαζί με το υλικό στην πλατφόρμα τηλεκπαίδευσης. Η μέθοδος υβριδικής διδασκαλίας πραγματοποιείται μέσα από σύγχρονες διαλέξεις με την υποστήριξη του εργαλείου τηλεδιασκέψεων Zoom. Οι φοιτητές διδάσκονται πληθώρα εργαλείων σχετικών με το περιεχόμενο και την ύλη του μαθήματος, ενώ κάνουν και εφαρμογή στα πλαίσια εργαστηρίου. **Χρήση Τ.Π.Ε. στην Επικοινωνία με τους φοιτητές**

<table>
<tr><td></td><td>

- Ανάρτηση εκπαιδευτικού υλικού (διαφάνειες, επιστημονικά άρθρα, ασκήσεις, κτλ.) στη σελίδα του μαθήματος στην ηλεκτρονική πλατφόρμα (Moodle).
- Χρήση ανακοινώσεων μέσω Forum στο Moodle.
- Ζωντανές συναντήσεις μέσω Zoom/Teams. Επικοινωνία μέσω email.

</td></tr>
<tr><td>

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

</td><td>

Δραστηριότητα	**Φόρτος εργασίας εξαμήνου**
Διαλέξεις	30 ώρες.
Φροντιστήριο	9 ώρες.
Συγγραφή Ομαδικλης Εργασίας	8 ώρες.
Εξετάσεις	2 ώρες.
Μη Καθοδηγούμενη Μελέτη	86 ώρες.
Σύνολο μαθήματος	**135 ώρες.**

</td></tr>
<tr><td>

ΚΑΤΑΝΟΜΗ ΥΛΗΣ

</td><td>

Θεωρία/Φροντιστήριο

Θεωρητικές και πρακτικές σύγχρονες αρχές κρυπτογραφίας.	
Τεχνικές και μεθοδολογίες προστασίας δεδομένων.	
Τεχνικές κρυπτογράφησης (συμμετρικά και ασύμμετρα κλειδιά, κρυπτογράφηση δημόσιου και μυστικού κλειδιού, ψηφιακές υπογραφές κ.λπ.).	

Εργαστήριο

Αξιολόγηση απειλών και τρωτών σημείων.	

</td></tr>
<tr><td>

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.

</td><td>

Γλώσσα αξιολόγησης: Αγγλική
Η αξιολόγηση συνίσταται σε:

- Γραπτή εξέταση στο τέλος του εξαμήνου (30%). Μέθοδοι Γραπτής Αξιολόγησης:
  - Ερωτήσεις Κλειστού Τύπου
  - Ερωτήσεις Πολλαπλής Επιλογής
- Αξιολόγηση ομαδικής εργασίας (70%):
  - Εκπαίδευση στη δημιουργία εφαρμογής σε οικοσύστημα IoT.
  - Οι φοιτητές θα πρέπει να επιτύχουν προβιβάσιμο βαθμό προκειμένου να πάρουν μέρος στις γραπτές εξετάσεις

Τα κριτήρια αξιολόγησης ανακοινώνονται στους φοιτητές κατά την πρώτη διάλεξη και είναι προσβάσιμα στην πλατφόρμα τηλεκπαίδευσης καθ' όλη τη διάρκεια του εξαμήνου.

</td></tr>
<tr><td>

ΥΠΟΧΡΕΩΣΕΙΣ ΦΟΙΤΗΤΩΝ

Υποχρεωτική: παρακολούθηση διαλέξεων, εργαστηρίων, φροντιστηρίων, συμμετοχή σε προόδους, εξετάσεις, παράδοση ασκήσεων, παράδοση εργασιών (project) κ.λπ.

</td><td>

- Υποχρεωτική παρακολούθηση διαλέξεων
- Υποχρεωτική παρακολούθηση εργαστηρίων
- Υποχρεωτική συμμετοχή σε εξετάσεις
- Υποχρεωτική παράδοση εργασιών

</td></tr>
</table>

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- *Προτεινόμενα διδακτικά βιβλία*

1. Understanding Cryptography: A Textbook for Students and Practitioners, Christof Paar, Jan Pelzl, Springer.
2. Contemporary cryptography, Oppliger Rolf, Artech House.

- *Πρόσθετη βιβλιογραφία:*

1. Real-World Cryptography, David Wong, Manning Publications.