ΚΡΥΠΤΟΓΡΑΦΙΑ

ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	**ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**			
ΤΜΗΜΑ	**ΠΛΗΡΟΦΟΡΙΚΗΣ**			
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	**ΠΡΟΠΤΥΧΙΑΚΟ**			
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**607ΕΔΥΕ**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**6ο**	
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΚΡΥΠΤΟΓΡΑΦΙΑ**			
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 & Φροντιστηριακές Ασκήσεις			**2Θ + 1ΦΑ**	**5**
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο 4.				
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων*	Επιστημονικής Περιοχής			
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	-			
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική			
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	-			
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	-			

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 Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης*
- *Περιγραφικοί Δείκτες Επιπέδων 6, 7 & 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης*

και Παράρτημα Β

- *Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων*

Το μάθημα αυτό ασχολείται με θέματα κρυπτογραφίας. Πέραν της απαραίτητης εννοιολογικής θεμελίωσης σχετικά με την ασφάλεια πληροφοριών, αναλύονται θέματα κρυπτογραφίας και αλγορίθμων που χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων αλλά και των πρόσθετων μηχανισμών έχουν ως σκοπό την εξασφάλιση της ακεραιότητας δεδομένων.

Αντικείμενο του μαθήματος αποτελούν επίσης τα θέματα της αυθεντικοποίησης μηνυμάτων και οντοτήτων και οι υποδομές δημοσίου κλειδιού.

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

- Εξηγεί τις διάφορες μεταξύ των διαφόρων τύπων αλγορίθμων.
- Αναλύει την ορθή χρήση αλγορίθμων κρυπτογράφησης

- Αναλύει τρόπους προστασίας ακεραιότητας δεδομένων και αυθεντικοποίησης δεδομένων και οντοτήτων.
- Σχεδιάζει βασικά πρωτόκολλα αυθεντικοποίησης

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

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

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

1. Εννοιολογική θεμελίωση – βασικές αρχές ασφάλειας πληροφοριών
2. Κρυπτογραφία – συμμετρικοί αλγόριθμοι
3. Κρυπτογραφία δημοσίου κλειδιού
4. Συναρτήσεις κατακερματισμού
5. Ψηφιακές υπογραφές
6. Ψηφιακά πιστοποιητικά και υποδομές δημοσίων κλειδιών
7. Ακεραιότητα δεδομένων, αυθεντικοποίηση μηνύματος
8. Αυθεντικοποίηση οντότητας – μέθοδοι και πρωτόκολλα
9. Μελέτες περίπτωσης

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Στην αίθουσα και σε εργαστήριο
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	Υποστήριξη Μαθησιακής διαδικασίας μέσω της ηλεκτρονικής πλατφόρμας e-class Χρήση ιστοσελίδας μαθήματος Ανακοινώσεις μέσω κεντρικής ιστοσελίδας τμήματος Χρήση email για επικοινωνία
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 ώστε ο συνολικός φόρτος εργασίας σε επίπεδο εξαμήνου να αντιστοιχεί στα standards του ECTS*	

Δραστηριότητα	***Φόρτος Εργασίας Εξαμήνου***
Διαλέξεις	26 x 2 = 52 ώρες
Φροντιστηριακές Ασκήσεις	13 x 2 = 26 ώρες
Γραπτές Εξετάσεις	2 x 1 = 2 ώρες
Αυτοτελής Μελέτη	45 ώρες
Σύνολο Μαθήματος (25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα)	**125 ώρες**

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.*	Τελικός Βαθμός = 100% του Βαθμού Τελικής Εξέτασης

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

-Προτεινόμενη Βιβλιογραφία :
-Συναφή επιστημονικά περιοδικά:

- Ασφάλεια Δικτύων Υπολογιστών, Σ. Γκρίτζαλης, Δ. Γκρίτζαλης, Σ. Κάτσικας, Εκδόσεις Παπασωτηρίου, 2003, ISBN: 978-960-7530-45-4
- Βασικές Αρχές Ασφάλειας Δικτύων: Εφαρμογές και Πρότυπα, W. Stallings, Εκδόσεις Κλειδάριθμος, Έκδοση 3η, 2008, ISBN: 978-960-461-117-1
- Cryptography and Network Security: Principles and Practice, W. Stallings, 2010, Prentice Hall, ISBN-10: 0136097049
- Ασφάλεια Πληροφοριακών Συστημάτων, Σ. Κάτσικα, Δ. Γκρίτζαλη, Σ. Γκρίτζαλη (Επιστημονική Επιμέλεια), 2004, ISBN: 9608105579
- Handbook of Applied Cryptography, A. Menezes, P. V. Oorschot, S. Vanstone, 2001, CRC Press, ISBN-10: 0849385237
- Πρακτικά θέματα ασφάλειας πληροφοριακών συστημάτων και εφαρμογών, Ν. Πολέμη, Εκδόσεις Νέων Τεχνολογιών, 2008, ISBN: 9606759156
- Computer Security, D. Gollmann, J. Wiley & Sons, 1999