# ΚΡΥΠΤΟΓΡΑΦΙΑ

## 1. ΓΕΝΙΚΑ

| | | | |
|---|---|---|---|
| **ΣΧΟΛΗ** | ΜΗΧΑΝΙΚΩΝ | | |
| **ΤΜΗΜΑ** | ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ | | |
| **ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ** | ΠΡΟΠΤΥΧΙΑΚΟ | | |
| **ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ** | ICE-7307 | **ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ** | 7ο, 9ο |
| **ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ** | ΚΡΥΠΤΟΓΡΑΦΙΑ | | |

| **ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ**<br>*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 | 2 | |
| Ασκήσεις Πράξης | 2 | |
| *Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο 4.* | **4** | **5** |

| | |
|---|---|
| **ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ**<br>*Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων* | Επιστημονικής Περιοχής<br>**Εμβάθυνσης/Ειδικότητας** |
| **ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:** | - |
| **ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:** | Ελληνική |
| **ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS** | Ναι (στα Αγγλικά) |
| **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 καλύπτει βασικές τεχνικές σύγχρονων κρυπτογραφικών αλγόριθμων για ασφαλή συστήματα και μετάδοση της πληροφορίας. Σκοπός του μαθήματος είναι η δημιουργία ενός πλαισίου θεωρητικών και πρακτικών γνώσεων κρυπτογραφικών τεχνικών, της σημαντικής χρήσης τους και της εκτίμησης της επάρκειάς τους και του επιπέδου της ασφάλειας που παρέχουν. Οι γνώσεις αυτές θα αποτελέσουν για το φοιτητή εξειδικευμένο εφόδιο στην αγορά εργασίας στον τομέα της Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων.

Με την επιτυχή ολοκλήρωση του μαθήματος αυτού, ο φοιτητής:

- θα γνωρίζει τα προβλήματα ασφάλειας που επιλύει η κρυπτογραφία,
- θα γνωρίζει σύγχρονους συμμετρικούς κρυπτογραφικούς αλγόριθμους (permutations, block ciphers, stream ciphers, Affine, Vigenere, Hill, AES),
- θα γνωρίζει σύγχρονους ασύμμετρους κρυπτογραφικούς αλγόριθμους (public key encryption, RSA, Diffie-Helman, ElGamal),
- θα γνωρίζει μονόδρομες κρυπτογραφικές συναρτήσεις κατακερματισμού (hash functions),
- θα γνωρίζει ψηφιακές υπογραφές και τις εφαρμογές τους,
- θα γνωρίζει μεθόδους αναγνώρισης (π.χ. passwords)
- θα γνωρίζει υποδομές δημοσίου κλειδιού,

- θα γνωρίζει ανεκτικότητα όλων των παραπάνω κρυπτογραφικών αλγόριθμων και δυνατές μεθόδους κρυπτανάλυσης αυτών,
- και τέλος, θα είναι σε θέση να αξιολογήσει, ανάλογα το επίπεδο ασφάλειας που απαιτείται, τον κρυπτογραφικό αλγόριθμο που πρέπει να επιλεγεί.

**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* |
| *Ομαδική εργασία* | *υπευθυνότητας και ευαισθησίας σε θέματα φύλου* |
| *Εργασία σε διεθνές περιβάλλον* | *Άσκηση κριτικής και αυτοκριτικής* |
| *Εργασία σε διεπιστημονικό περιβάλλον* | *Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης* |
| *Παραγωγή νέων ερευνητικών ιδεών* | |

- Αυτόνομη Εργασία,
- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών και εργαλείων,
- Προγραμματισμός απλών μηχανισμών ασφάλειας,
- Παραγωγή νέων ερευνητικών ιδεών

## 3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

- Στοιχεία από τη θεωρία των αριθμών,
- Σχήματα Κρυπτογράφησης,
- Συμμετρικά Κρυπτοσυστήματα (permutations, block ciphers, stream ciphers, Affine, Vigenere, Hill, AES),
- Ασύμμετρα Κρυπτοσυστήματα, (public key encryption, RSA, Diffie-Helman, ElGamal),
- Το Παράδοξο των Γενεθλίων,
- Τέλεια Μυστικότητα,
- Advanced Encryption System (AES),
- RSA,
- Diffie-Helman,
- ElGamal,
- Κρυπτογραφικές Συναρτήσεις Κατακερματισμού (SHA1, MAC,),
- Ψηφιακές Υπογραφές (RSA signatures, ElGamal signatures, DSA, Blind Signatures),
- Elliptic Curves,
- Passwords, One-Time passwords,
- PKI.

## 4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

| | |
|---|---|
| **ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ**<br>*Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.* | Πρόσωπο με πρόσωπο |
| **ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ**<br>*Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές* | • Ανάρτηση μαθησιακού υλικού (σημειώσεις, διαφάνειες διαλέξεων, ασκήσεις, θέματα εξετάσεων, κ.λπ.) στην πλατφόρμα ηλεκτρονικής μάθησης (e-class).<br>• Χρήση ηλεκτρονικού ταχυδρομείου και ανακοινώσεων στην πλατφόρμα ηλεκτρονικής μάθησης για την επικοινωνία με τους φοιτητές. |
| **ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ**<br>*Περιγράφονται αναλυτικά ο τρόπος και μέθοδοι διδασκαλίας.*<br>*Διαλέξεις, Σεμινάρια, Εργαστηριακή Άσκηση, Άσκηση Πεδίου, Μελέτη & ανάλυση βιβλιογραφίας, Φροντιστήριο, Πρακτική (Τοποθέτηση), Κλινική Άσκηση, Καλλιτεχνικό* | |

| ***Δραστηριότητα*** | ***Φόρτος Εργασίας Εξαμήνου*** |
|---|---|
| Διαλέξεις | 26 |
| Φροντιστήριο | 26 |
| Εκπόνηση Εργασιών | 30 |

| | |
|---|---|
| *Εργαστήριο, Διαδραστική διδασκαλία, Εκπαιδευτικές επισκέψεις, Εκπόνηση μελέτης (project), Συγγραφή εργασίας / εργασιών, Καλλιτεχνική δημιουργία, κ.λπ.*<br><br>*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* | Αυτοτελής Μελέτη: 43<br>**Σύνολο Μαθήματος** (25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα): **125** |
| **ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ**<br>*Περιγραφή της διαδικασίας αξιολόγησης*<br><br>*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*<br><br>*Αναφέρονται ρητά προσδιορισμένα κριτήρια αξιολόγησης και εάν και που είναι προσβάσιμα από τους φοιτητές.* | **I.** Γραπτή τελική εξέταση (100%) που περιλαμβάνει:<br>- Ερωτήσεις σύντομης απάντησης<br>- Επίλυση προβλημάτων<br><br>Για την επιτυχή ολοκλήρωση απαιτείται βαθμός τουλάχιστον 5/10 στη Γραπτή Τελική Εξέταση.<br><br>Η εξεταστέα ύλη και η διαδικασία αξιολόγησης γνωστοποιούνται στους φοιτητές στην αίθουσα διαλέξεων και στην πλατφόρμα ηλεκτρονικής μάθησης (e-class). |

## 5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

*- Προτεινόμενη Βιβλιογραφία:*


1. Stallings, Κρυπτογραφία για Ασφάλεια Δικτύων Αρχές και Εφαρμογές, ΜΑΡΙΑ ΠΑΡΙΚΟΥ & ΣΙΑ ΕΠΕ, 2011, ISBN: 9789604117307.
2. Κάττος Β., Στεφανίδης Γ., Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης, ΖΥΓΟΣ, 2003.
3. Buchmann J., Introduction to Cyptography, 2nd Ed., Springer, 2004.
4. Paul Erdos and Janos Suranyi. Topics in the Theory of Numbers. Springer-Verlag, New York, 2003.
5. Joseph H. Silverman. A Friendly Introduction to Number Theory. Prentice-Hall, 2001.
6. James J. Tettersall. Elementary Number Theory in Nine Chapters. Cambridge University Press, 2005.


## 6. ΒΙΒΛΙΑ ΕΥΔΟΞΟΣ

1. Βιβλίο [59395497]: Κρυπτογραφία και Εφαρμογές, Πατσάκης Κωνσταντίνος, Φούντας Ευάγγελος Λεπτομέρειες

2. Βιβλίο [9771]: Σύγχρονη κρυπτογραφία, Γκρίτζαλης Στέφανος Λεπτομέρειες

3. Βιβλίο [12777632]: Κρυπτογραφία για Ασφάλεια Δικτύων Αρχές και Εφαρμογές, Stallings Λεπτομέρειες

4. Βιβλίο [59374208]: Εισαγωγή στη θεωρία Πληροφοριών, Κωδίκων και Κρυπτογραφίας, Ν. Αλεξανδρής, Β. Χρυσικόπουλος, Κ. Πατσάκης Λεπτομέρειες

5. Βιβλίο [1746]: ΤΕΧΝΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ & ΚΡΥΠΤΑΝΑΛΥΣΗΣ, ΚΑΤΟΣ Β., ΣΤΕΦΑΝΙΔΗΣ Γ. Λεπτομέρειες