## ΜΕΜ-245 ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ

### 1. ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

| | | | |
|---|---|---|---|
| **ΣΧΟΛΗ** | ΘΕΤΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΠΙΣΤΗΜΩΝ | | |
| **ΤΜΗΜΑ** | ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ | | |
| **ΠΠΣ** | ΚΑΤΕΥΘΥΝΣΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ | | |
| **ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ** | ΠΡΟΠΤΥΧΙΑΚΟ | | |
| **ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ** | ΜΕΜ-245 | | |
| **ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ** | ΕΑΡΙΝΟ | | |
| **ΠΡΟΤΕΙΝΟΜΕΝΟ ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ** | 8ο | | |
| **ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ** | ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ | | |
| **ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ** | | **ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ** | **ECTS** |
| Διαλέξεις | | 4 | 8 |
| **ΑΝΑΛΥΣΗ ΑΥΤΟΤΕΛΩΝ ΔΙΔΑΚΤΙΚΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ** | | **ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ** | |
| Διαλέξεις | | 4 | |
| ΣΥΝΟΛΟ ΜΑΘΗΜΑΤΟΣ | | 4 | |
| **ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ:** | Επιστημονικής Περιοχής | | |
| **ΕΙΔΟΣ ΜΑΘΗΜΑΤΟΣ:** | ΕΠΙΛΟΓΗΣ ΜΑΘΗΜΑΤΙΚΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ | | |
| **ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:** | | | |
| **ΣΥΝΙΣΤΩΜΕΝΑ ΜΑΘΗΜΑΤΑ:** | ΜΕΜ-221 ΑΛΓΕΒΡΑ Ι | | |
| **ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:** | ΕΛΛΗΝΙΚΗ | | |
| **ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS** | ΝΑΙ (ΕΛΛΗΝΙΚΗ/ΑΓΓΛΙΚΗ) | | |
| **ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ:** | Η ηλεκτρονική σελίδα διαμορφώνεται με ευθύνη του διδάσκοντα. | | |

### 2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

**ΕΠΙΠΕΔΟ ΕΘΝΙΚΟΥ & ΕΥΡΩΠΑΪΚΟΥ ΠΛΑΙΣΙΟΥ ΠΡΟΣΟΝΤΩΝ: 6**

**Μαθησιακά Αποτελέσματα**

Μετά την επιτυχή ολοκλήρωση του μαθήματος οι φοιτητές θα γνωρίζουν και θα μπορούν να κατασκευάσουν και να χρησιμοποιήσουν:
1) Βασικά ιστορικά κρυπτοσυστήματα
2) Συμμετρικά κρυπτοσυστήματα τύπου Feistel (όπως το DES)
3) Το πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman
4) Συστήματα κρυπτογράφησης δημόσιου κλειδιού (όπως το RSA και το ElGamal)
5) Συστήματα ψηφιακών υπογραφών (όπως το RSA και το ElGamal)
Επίσης οι φοιτητές θα κατανοούν τα βασικά μαθηματικά προβλήματα τα οποία σχετίζονται με τα παραπάνω συστήματα:
1) Το πρόβλημα της πιστοποίηση πρώτων αριθμών
2) Τα προβλήματα υπολογισμού και απόφασης Diffie-Hellman
3) Το πρόβλημα του διακριτού λογαρίθμου
4) το πρόβλημα της παραγοντοποίησης ακεραίων

**Γενικές Ικανότητες**

Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών.
Προσαρμογή σε νέες καταστάσεις.
Λήψη αποφάσεων.
Αυτόνομη εργασία.
Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης.

## 3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

1) Βασικά ιστορικά κρυπτοσυστήματα
2) Συμμετρικά κρυπτοσυστήματα τύπου Feistel (όπως το DES), μονόδρομες συναρτήσεις
3) Το πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman
4) Το πρόβλημα της πιστοποίηση πρώτων αριθμών
5) Τα προβλήματα υπολογισμού και απόφασης Diffie-Hellman
6) Το πρόβλημα του διακριτού λογαρίθμου
7) Συστήματα κρυπτογράφησης δημόσιου κλειδιού (όπως το RSA και το ElGamal)
8) το πρόβλημα της παραγοντοποίησης ακεραίων
9) Συστήματα ψηφιακών υπογραφών (όπως το RSA και το ElGamal)
10) Ειδικά θέματα (όπως κρυπτοσυστήματα τύπου σακιδίου, κρυπτογραφία ελλειπτικών καμπύλων)

## 4. ΔΙΔΑΚΤΙΚΕΣ ΚΑΙ ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ-ΑΞΙΟΛΟΓΗΣΗ

**ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ:**

Πρόσωπο με πρόσωπο.
Παρουσίαση της ύλης στον πίνακα, εντός αίθουσας, με ακροατήριο.

**ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ:**

Παροχή υλικού μελέτης και πληροφοριών μέσω ιστοσελίδας.
Δυνατότητα επικοινωνίας των φοιτητών με τον διδάσκοντα με ηλεκτρονικό τρόπο (e-mail).

**ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ:**

| Δραστηριότητα | Φόρτος Εργασίας Εξαμήνου |
|---|---|
| Διαλέξεις | 52 |
| Μη καθοδηγούμενη μελέτη βιβλιογραφίας | 52 |
| Μη καθοδηγούμενη μελέτη α-σκήσεων εφαρμογής | 90 |
| Συμβουλευτική μελέτης | 6 |
| | |
| **Σύνολο Μαθήματος** | **200** |

**ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ:**

Η αξιολόγηση στηρίζεται στο αποτέλεσμα μίας ή περισσοτέρων γραπτών εξετάσεων. Η συμμετοχή του αποτελέσματος κάθε εξέτασης στον τελικό βαθμό αποφασίζεται από τον εκάστοτε διδάσκοντα του μαθήματος. Κάθε γραπτή εξέταση στοχεύει στην πιστοποίηση των γνώσεων που έχουν αποκτηθεί με θέματα ανάπτυξης.

Η διαδικασία αξιολόγησης ανακοινώνεται από τον διδάσκοντα στην αρχή του εξαμήνου και είναι αναρτημένη μόνιμα στην ιστοσελίδα του μαθήματος.

Σε συνεργασία με το Συμβουλευτικό Κέντρο του Πανεπιστημίου Κρήτης, η διαδικασία αξιολόγησης προσαρμόζεται κατάλληλα στους φοιτητές με ειδικές εκπαιδευτικές ανάγκες.

## 5. ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Α. Κοντογεώργης, Ι. Αντωνιάδης, Πεπερασμένα σώματα και κρυπτογραφία, Εκδόσεις Κάλλιππος.
2. N. Smart, Cryptography Made Simple, Springer, 2015.