THEMELIOSEIS KAI EFARMOGES TIS SYGCHRONIS KRYPTOGRAFIAS

ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ		
ΤΜΗΜΑ	ΜΑΘΗΜΑΤΙΚΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ **Σπουδές στα Μαθηματικά**		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**Β9**	**ΕΞΑΜΗΝΟ ΜΑΘΗΜΑΤΟΣ**	
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**Θεμελιώσεις και Εφαρμογές στη Σύγχρονη Κρυπτογραφία**		
ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**		**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
	3		10
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ	ΕΙΔΙΚΕΥΣΗΣ ΓΕΝΙΚΩΝ ΓΝΩΣΕΩΝ		
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	ΟΧΙ		
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	ΕΛΛΗΝΙΚΗ		
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	ΝΑΙ		
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	http://www.math.aegean.gr/index.php/el/academics-el/postgraduate-programs-el		

(1) ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα
Να καταστεί κάτοχος των εννοιών και τεχνικών που παρουσιάζονται στα περιεχόμενα του μαθήματος (βλ. (3) παρακάτω).
Γενικές Ικανότητες
Αυτόνομη Εργασία, Εργασία σε διεπιστημονικό περιβάλλον, Εργασία σε διεθνές περιβάλλον.

(2) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Κλασικά και σύγχρονα υπολογιστικά μοντέλα (κλασικές TMs, evolutionary TMs και κβαντικά μοντέλα υπολογισμού). Αλγόριθμοι και κρυπτογραφία. Γρήγορα επιλύσιμα προβλήματα και η κλάση πολυπλοκότητας P, δύσκολα υπολογιστικά προβλήματα και η κλάση πολυπλοκότητας NP, NP-πλήρη προβλήματα.

Μοντέλα Αξιολόγησης Ασφάλειας. Ορισμός Κρυπτογράφησης και Κρυπτανάλυσης, Μηχανισμοί κατακερματισμού (hash functions).

Βασικές Αρχές Σχεδίασης κρυπτογραφικών σχημάτων διαμοιραζόμενου κλειδιού. Κρυπταγραφικό γινόμενο. Κρυπταλγόριθμος τμήματος. Αρχές διάχυσης (diffusion) και σύγχυσης (confusion).

Δίκτυα Αντικατάστασης Μετάθεσης (SPN), AES (Advanced Encryption Standard). Δίκτυα Feistel. Ασφάλεια Δικτύων Feistel, DES (Data Encryption Standard)

Σχεδίαση Κουτιών Αντικατάστασης (SBoxes).

Τρόποι διασύνδεσης κρυπταλγόριθμων διαμοιραζόμενου κλειδιού. Τριπλή Κρυπτογράφηση και η επίθεση meet-in-the-middle. Αλγόριθμοι Προγράμματος Κλειδιού. Γραμμική και Διαφορική Κρυπτανάλυση.

Σχήματα κρυπτογράφησης δημόσιου κλειδιού. Η ιδέα των Diffie-Hellman, το κρυπτογραφικό σχήμα δημόσιου κλειδιού RSA. Κρυπτογραφικό Σύστημα ElGamal στο Zp*. Κρυπτογραφικά συστήματα ElGamal σε ελλειπτικές καμπύλες.

Ψηφιακές υπογραφές (Digital Signature Algorithm, blind digital signatures). Zero knowledge proofs. Κρυπτογραφία και Κρυπτονομίσματα.Post-Quantum κρυπτογραφία.

(3) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ	Πρόσωπο με πρόσωπο
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ	• Επικοινωνία με φοιτητές μέσω email • Χρήση ΤΠΕ στη διδασκαλία • Ανάρτηση διαφανειών και υλικού μαθήματος στην πλατφόρμα moodle
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ	***Δραστηριότητα*** — ***Φόρτος Εργασίας Εξαμήνου*** Διαλέξεις — 39 Αυτοτελής Μελέτη — 148.5 Εκπόνηση Εργασιών — 62.5 Σύνολο Μαθήματος (25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα) — ***250***
ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ	Η αξιολόγηση των φοιτητών γίνεται μέσω γραπτής εξέτασης η οποία περιλαμβάνει ερωτήσεις σύντομης απάντησης και επίλυση προβλημάτων. Οι φοιτητές με μαθησιακές δυσκολίες εξετάζονται προφορικά.

(4) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Handbook of Applied Cryptography, Alfred Menezes, Paul Oorschot, Scot Vanstone.
- Cryptography and Network Security, Principles and Practices, William Stallings Prentice Hall.
- Introduction to the theory of computation, Michael Sipser, Cengage Learning.
- Understanding Bitcoin, Cryptography, Engineering and Economics, Pedro Franco, Wiley.
- Quantum Computing, Mik Hirvensalo, Springer.