ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ		
ΤΜΗΜΑ	ΜΑΘΗΜΑΤΙΚΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΠΡΟΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ		**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**ΕΚΤΟ**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	ΚΡΥΠΤΟΓΡΑΦΙΑ		
ΔΙΔΑΣΚΩΝ	Παναγιώτης Νάστου		
ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ		**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
		4	6
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ	ΕΙΔΙΚΟΥ ΥΠΟΒΑΘΡΟΥ		
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/undergraduate-programs-el		

(2) ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα
Στα πλαίσια του μαθήματος αυτού, ο/η φοιτητής/τρια αρχικά εμπεδώνει τις βασικές αρχές της θεωρίας πολυπλοκότητας και στο πως υπολογιστικά δύσκολα προβλήματα μπορούν να αποτελέσουν τη βάση κρυπτογραφικά ασφαλών πρωτοκόλλων. Στη συνέχεια αφού κατανοήσει και εφαρμόσει μερικά από τα ποιο κλασικά κρυπτογραφικά σχήματα (κρυπταλγόριθμοι αντικατάστασης, μετατόπισης, μετάθεσης) ο/η φοιτητής/τρια εισάγεται στη θεωρία πληροφορίας καθώς και στις βασικές αρχές της σύγχυσης και της διάχυσης και μαθαίνει στο πως εφαρμόζονται στη σχεδίαση συμμετρικών κρυπταλγορίθμων. Μέσα από την ανάλυση της γραμμικής και διαφορικής κρυπτανάλυσης, ο/η φοιτητής/τρια αποκτά τη γνώση να σχηματίζει κρυπταναλυτικές επιθέσεις σε συμμετρικούς κρυπταλγόριθμους και να αποτιμά το βαθμό ασφάλειας αυτών. Ως ειδικές περιπτώσεις συμμετρικών κρυπταλγορίθμων αναλύονται οι κρυπταλγόριθμοι DES και AES και ο/η φοιτητής/τρια μαθαίνει πως να τους χρησιμοποιεί στην ασφάλεια δικτύων. Στο δεύτερο μέρος, οι φοιτητές/τριες μαθαίνουν να αναλύουν τη λειτουργία των ασύμμετρων κρυπταλγορίθμων με έμφαση στον RSA, στο ElGamal στο Z_p και στο ElGamal σε ελλειπτικές καμπύλες. Εμπεδώνουν τους αλγόριθμους παραγοντοποίησης μεγάλων ακεραίων και τους αλγόριθμους εύρεσης του διακριτού λογάριθμου σε οποιαδήποτε πολλαπλασιαστική ομάδα και στη συνέχεια μαθαίνουν στο να τους εφαρμόζουν στο σχηματισμό επιθέσεων. Στο τέλος οι φοιτητές/τριες μπορούν να κρυπτογραφήσουν και αποκρυπτογραφήσουν μηνύματα με τη χρήση των παραπάνω κρυπταλγορίθμων, να κρυπταναλύουν κρυπταλγόριθμους αλλά και να επιλέγουν τις παραμέτρους αυτών κατά τέτοιο τρόπο ώστε να αποφεύγονται γνωστές απειλές.
Γενικές Ικανότητες
Αυτόνομη εργασία. Ομαδική εργασία. Εργασία σε διεπιστημονικό περιβάλλον. Εργασία σε διεθνές περιβάλλον.

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Αλγόριθμοι και κρυπτογραφία. Εισαγωγή στη θεωρία πολυπλοκότητας, γρήγορα επιλύσιμα προβλήματα και η κλάση πολυπλοκότητας P, δύσκολα υπολογιστικά προβλήματα και η κλάση πολυπλοκότητας NP, NP-πλήρη προβλήματα (το πρόβλημα SAT), το ερώτημα εάν P≠NP.

Μοντέλα Αξιολόγησης Ασφάλειας. Σχεδίαση Ασφαλών Κρυπτογραφικών Συστημάτων. Ορισμός Κρυπτογράφησης και Κρυπτανάλυσης. Θεωρία Πληροφορίας: Πιθανότητες, Εντροπία, Αμοιβαία Πληροφορία.

Διαρροή Πληροφορίας από το κρυπτοκείμενο. Τέλεια Μυστικότητα. Περίσσεια Γλώσσας. Ασάφεια Κλειδιού. Υπολογισμός μέσου αριθμού ψευδοκλειδιών (spurious keys). Εύρεση μήκους κρυπτοκειμένου που μηδενίζει το πλήθος των ψευδοκλειδιών (unicity Distance). Κρυπταλγόριθμοι ροής και τμήματος.

Κρυπτογραφικές Πράξεις. Κρυπταλγόριθμος Αναδιάταξης. Κρυπταλγόριθμος Μετατόπισης και Κρυπταλγόριθμος του Καίσαρα. Κρυπταλγόριθμος Αντικατάστασης. Ασφάλεια Μονοαλφαβητικής Αντικατάστασης. Γραμμικός Κρυπταλγόριθμος. Κρυπτανάλυση Γραμμικού Κρυπταλγόριθμου.

Κρυπταλγόριθμος Vigenere. Κρυπτανάλυση Vigenere: Έλεγχος Kassiski και δείκτης σύμπτωσης. Κρυπτοσύστημα σημειωματαρίου μιας χρήσης. Κρυπτοσύστημα Vernam. Κρυπταλγόριθμος Hill. Κρυπτανάλυση Hill. Κρυπτογράφηση γινομένου.

Κρυπτογραφικά σχήματα διαμοιραζόμενου κλειδιού. Δίκτυα Αντικατάστασης Μετάθεσης (SPN). Σχεδίαση Κουτιών Αντικατάστασης (sboxes). Αρχές διάχυσης (diffusion) και σύγχυσης (confusion). Κρυπταλγόριθμος τμήματος.

Δίκτυα Feistel. Ασφάλεια Δικτύων Feistel: Μεταθέσεις, Αντίπαλος, Μαντείο, Ψευδοτυχαίες Μεταθέσεις και Συναρτήσεις. Αναλυτική παρουσίαση της σχεδίασης και της λειτουργίας των κρυπταλγορίθμων DES (Data Encryption Standard) και AES (Advanced Encryption Standared).

Τρόποι διασύνδεσης κρυπταλγόριθμων τμήματος. 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, τρόποι δημιουργίας του ζεύγους κλειδιών, αλγόριθμος κατασκευής τυχαίων πρώτων αριθμών, αλγόριθμος γρήγορης ύψωσης σε δύναμη και υπολογισμού υπολοίπου από διαίρεση.

Κρυπτογραφικό Σύστημα ElGamal. Το πρόβλημα του Διακριτού Λογάριθμου. Αλγόριθμοι επίλυσης του Διακριτού λογάριθμου: Αλγόριθμος του Shank (Baby-Step-Giant-Step), αλγόριθμος του Pollard Rho, αλγόριθμος των Pohling-Hellman και ο αλγόριθμος Index Calculus.

Κρυπτογραφικά συστήματα βασισμένα στις ελλειπτικές καμπύλες. Τι είναι οι ελλειπτικές καμπύλες, δημιουργία σώματος με σημεία τους, βασικές αλγεβρικές πράξεις και αλγόριθμοι υλοποίησής τους, γιατί οι ελλειπτικές καμπύλες είναι ασφαλέστερες από το σχήμα RSA για ίδιο μήκος κλειδιού: το πρόβλημα του διακριτού λογαρίθμου στις ελλειπτικές καμπύλες.

Τρόποι κατασκευής ελλειπτικών καμπυλών, βασικά κρυπτογραφικά πρωτόκολλα (ανταλλαγή κλειδιών – ο αλγόριθμος Diffie-Hellman, κρυπτογράφηση δεδομένων, ηλεκτρονικές υπογραφές).

Ψηφιακές υπογραφές και ταυτοποίηση προσώπων, υποδομές δημόσιου κλειδιού (Public Key Infrastructures – PKIs).

ΚΑΤΑΝΟΜΗ ΤΗΣ ΥΛΗΣ	Η διδακτέα ύλη κατανέμεται ομοιόμορφα καθ' όλη τη διάρκεια του εξαμήνου.

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ	Πρόσωπο με πρόσωπο
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ	• Χρήση Τ.Π.Ε. στη Διδασκαλία • Επικοινωνία με φοιτητές μέσω email • Ανάρτηση διαφανειών και υλικού μαθήματος στην πλατφόρμα moodle.
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ	

Δραστηριότητα	***Φόρτος Εργασίας Εξαμήνου***
Διαλέξεις	52
Αυτόνομη Μελέτη	98
Σύνολο Μαθήματος (25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα)	***150***

ΥΠΟΧΡΕΩΣΕΙΣ ΦΟΙΤΗΤΩΝ/ΤΡΙΩΝ	Η παρακολούθηση των διαλέξεων του μαθήματος δεν είναι υποχρεωτική.

ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ	Η αξιολόγηση των φοιτητών γίνεται στην ελληνική γλώσσα μέσω γραπτής εξέτασης με Ερωτήσεις Σύντομης Απάντησης και Επίλυση Προβλημάτων. Οι φοιτητές με μαθησιακές δυσκολίες εξετάζονται προφορικά.

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Σύγχρονη Κρυπτογραφία, Γκρίτζαλης Στέφανος, Εκδόσεις Παπασωτηρίου, Μάρτιος 2011.
2. Διάφορα άρθρα που έχουν δημοσιευθεί σε διεθνή συνέδρια και περιοδικά.