2ο ΕΞΑΜΗΝΟ:

ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ «Κρυπτογραφία και ασφάλεια υπολογιστικών συστημάτων»

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ		
ΤΜΗΜΑ	ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	Μεταπτυχιακό		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	204	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	2ο
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Κρυπτογραφία και ασφάλεια υπολογιστικών συστημάτων		
ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ		**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Διαλέξεις		2	6
Εργαστηριακές Ασκήσεις		1	
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ	Ανάπτυξης δεξιοτήτων		
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:			
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική		
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	ΝΑΙ (Στην Αγγλική)		
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://ecourse.uoi.gr/course/view.php?id=3330		

2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα

Μετά την επιτυχή ολοκλήρωση του μαθήματος, οι φοιτητές θα έχουν αποκτήσει:

- Κατανόηση των θεμελίων και των βασικών εργαλείων Κρυπτογραφίας και Ασφάλειας Δικτύων.
- Βαθιά κατανόηση των θεμάτων/απειλών ασφαλείας τόσο σε επίπεδο υλικού επιθέσεις σφάλματος, Trojan Hawks) και λογισμικού (κακόβουλο λογισμικό, μη εξουσιοδοτημένες αλλαγές κώδικα) όσο και σε επίπεδο δικτύου (ασφάλεια δικτύου, πρωτόκολλα ασφαλείας ενσύρματου ή ασύρματου δικτύου και δίκτυα αισθητήρων).
- Βαθιά κατανόηση διαφόρων πρωτοκόλλων για την ενίσχυση της ασφάλειας του δικτύου και την προστασία από τις απειλές στα δίκτυα
- Εξοικείωση και ικανότητα εκμάθησης σχετικά με τον τρόπο διατήρησης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας δεδομένων.
- Εξοικείωση και ικανότητα κρυπτογράφησης και αποκρυπτογράφησης μηνυμάτων με χρήση κρυπτογράφησης μπλοκ, υπογραφής και επαλήθευσης μηνυμάτων χρησιμοποιώντας γνωστούς αλγόριθμους δημιουργίας υπογραφών και πιστοποίησης.
- Εξοικείωση και ικανότητα ανάλυσης υφιστάμενων πρωτοκόλλων ελέγχου ταυτότητας και εντοπισμό των αδυναμιών αυτών των πρωτοκόλλων.
- Κατανόηση των θεμάτων που σχετίζονται με την προστασία των προσωπικών δεδομένων και τη χρήση ανώνυμων πιστοποιητικών.

Γενικές Ικανότητες
• Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών. • Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης. • Ανάλυση και σύνθεση Μαθηματικών διαδικασιών και με τη χρήση του υπολογιστή.

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Αλγόριθμοι και Κρυπτογραφία. Μοντέλα Αξιολόγησης Ασφαλείας. Σχεδιασμός Ασφαλών Κρυπτογραφικών Συστημάτων. Cryptography και Cryptanalysis. Θεωρία Πληροφοριών. Διαδικασίες ανεύρεσης μη ισχυρών κλειδιών και κωδικών. Unicity Distance. Hash συναρτησεις. Διανομή κλειδιών, Block Ciphers, Συμμετρική και ασύμμετρη κρυπτογράφηση, Κρυπτογραφικοί αλγόριθμοι. Man on the Middle attack, αλγόριθμοι διανομής και δρομολόγησης κλειδιών. Γραμμική και Διαφορική Κρυπτανάλυση. Σχέδια κρυπτογραφίας δημόσιου κλειδιού. Η έννοια και η χρήση των σχημάτων ψηφιακής υπογραφής., Εφαρμογές ελέγχου ταυτότητας. Ασφάλεια IP και ασφάλεια Ιστού. Ασφάλεια ασύρματου δικτύου.

Εβδομ.	Τίτλος Ενότητας	Βιβλιογραφία	e-class
1	**Εισαγωγή στην Θεωρία Αριθμών** **:** Μεγάλοι Ακέραιοι Αριθμοι Αλγεβρικές δομές - Πρώτοι Αριθμοί - Θεώρημα Fermat και Euler - Βασικά στοιχεία Άλγεβρας και της Θεωρίας Αριθμών	[1-3][8]	https://ecourse.uoi.gr/course/view.php?id=3330
2	**Εισαγωγή στην Θεωρία Αριθμών** **:** Παραγοντοποίηση Αριθμών– Κινέζικο Θεώρημα, Διακριτοί λογάριθμοι, Γραμμική και κβαντική ακολουθία	[1-3][8]	https://ecourse.uoi.gr/course/view.php?id=3330
3	**Εισαγωγή στην Ασφάλεια:-** Στόχοι ασφαλείας – Υπηρεσίες ασφαλείας (Εμπιστευτικότητα, Ακεραιότητα, Έλεγχος ταυτότητας, Έλεγχος πρόσβασης	[1-3], [6-7]	https://ecourse.uoi.gr/course/view.php?id=3330
4	**Εισαγωγή στην Ασφάλεια:-** Κρυπτογράφηση Δεδομένων, Ακεραιότητα Δεδομένων, ψηφιακή υπογραφή, έλεγχος ταυτοποίησης χρηστών, Έλεγχος δρομολόγησης, Έπιθέσεις)	[1-3], [6-7]	https://ecourse.uoi.gr/course/view.php?id=3330
5	**Ασφάλεια Υπολογιστικών συστημάτων:** Αρχές	[1-3], [6-7]	https://ecourse.uoi.gr/course/view.php?id=3330

	Ασφάλειας. Εισαγωγή στην Κρυπτογραφία: Η αρχή του Kerckhoff - Ταξινόμηση κρυπτοσυστημάτων Κρυπταναλυτικές επιθέσεις - Ιδιότητες κρυπτογράφησης		
6	**Ασφάλεια Υπολογιστικών συστημάτων:** Αρχές ασφάλειας. Εισαγωγή στην Κρυπτογραφία: Η αρχή του Kerckhoff - Ταξινόμηση κρυπτοσυστημάτων Κρυπταναλυτικές επιθέσεις - Ιδιότητες κρυπτογράφησης68	[1-3], [3]	https://ecourse.uoi.gr/course/view.php?id=3330
7	**Συμμετρική κρυπτογράφηση:** Παραδοσιακά κρυπτοσυστήματα: - κρυπτογράφηση αντικατάστασης (μη-αλφαβητικά ciphers,πολύ αλφαβητικά ciphers), Ciphers-Stream και Block Ciphers.	[4], [6]	https://ecourse.uoi.gr/course/view.php?id=3330
8	**Συμμετρική κρυπτογράφηση:** Πρότυπο κρυπτογράφησης δεδομένων (DES) (Fiestel και Non-Fiestel Κρυπτογράφηση, Δομή DES, Επιθέσεις DES, 2-DES, 3-DES) - Προηγμένο Πρότυπο Κρυπτογράφησης (AES) (Δομή, Ανάλυση)- Κρυπτογραφικές συναρτήσεις hash ,Αλγόριθμος Αυθεντικοποίησης μηνύματος-Algorithm-Message Authentication Code (MAC)	[4], [4-5]	https://ecourse.uoi.gr/course/view.php?id=3330
9	**Κρυπτογραφία PKI:** Κρυπτοσυστήματα δημόσιου κλειδιού–Trapdoor - μονόδρομες συναρτήσεις -RSA Κρυπτοσυστήματα (Παραγοντοποίηση πρώτων Αριθμών, r, Δημιουργία κλειδιών,	[1-3], [4-5]	https://ecourse.uoi.gr/course/view.php?id=3330

	Κρυπτογράφηση, Αποκρυπτογράφηση)		
10	**Κρυπτογραφία PKI:** El Gamal Κρυπτοσύστημα (Συνάρτηση Κρυπτογράφησης διακριτού λογάριθμου, Κρυπτογράφηση, αποκρυπτογράφηση) - Ανταλλαγή κλειδιών Diffie-Hellman, Man in the Middle επίθεση στο Πρωτόκολλο Diffie-Hellman	[1-3], [4-5]	https://ecourse.uoi.gr/course/view.php?id=3330
11	**Υπογραφές PKI:** Ψηφιακή υπογραφή:-Υπογραφή – Επαλήθευση – Ψηφιακή υπογραφή πλαστογραφία - RSA Ψηφιακή υπογραφή - ElGamal Ψηφιακή υπογραφή	[1-3], [10-13]	https://ecourse.uoi.gr/course/view.php?id=3330
12	**Μελέτη, εγκατάσταση και παραμετροποίηση του πρωτοκόλλου ανταλλαγής κλειδιών SSL/TLS.**	[1-3], [10-13]	https://ecourse.uoi.gr/course/view.php?id=3330
13	**Ιδιωτικότητα :** Ανώνυμα διαπιστευτήρια/πιστοποιητικά για την διαχείριση ταυτότητας χρηστών	[14-19]	https://ecourse.uoi.gr/course/view.php?id=3330

4. ΔΙΔΑΚΤΙΚΕΣ ΚΑΙ ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ.	Πρόσωπο με πρόσωπο
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ	☒ Χρήση ηλεκτρονικών παρουσιάσεων, αναρτημένων στο e-class. ☒ Χρήση λογισμικού στον υπολογιστή κατά τη διάλεξη. ☒ Χρήση εξειδικευμένου λογισμικο.ύ ☒ Διάθεση εκπαιδευτικού υλικού μέσω e-class. ☐ Διαχείριση εργασιών/ασκήσεων μέσω δικτυακού τόπου. ☒ Επικοινωνία με φοιτητές μέσω e-mail. ☐ Ηλεκτρονικός χώρος συνομιλιών διδάσκοντος και φοιτητών.
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ	

Δραστηριότητα	***Φόρτος Εργασίας Εξαμήνου***
Διαλέξεις	26 ώρες
Εργαστηριακές Ασκήσεις	13 ώρες
Βιβλιογραφική Εργασία	31 ώρες
Υλοποίηση Project	40 ώρες

	Μη καθοδηγούμενη μελέτη	70 ώρες
	Σύνολο Μαθήματος	**180 ώρες**
ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ	Οι φοιτητές αναλαμβάνουν να παρουσιάσουν ατομικά μια συναφή εργασία (paper) από κάποιο έγκριτο περιοδικό ή συνέδριο που είναι συναφές με το αντικείμενο του μαθήματος (50%). Ατομική προγραμματιστική εργασία πάνω σε κάποιο αντικείμενο που θα επιλέξουν οι σπουδαστές σε συνεργασία με τον διδάσκοντα (50%). Τα κριτήρια αξιολόγησης γνωστοποιούνται στους φοιτητές στην πρώτη διάλεξη, τα οποία και αναφέρονται ρητά στο syllabus του μαθήματος, το οποίο είναι και διαθέσιμο στο e-class.	

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

1. D.R. Hankerson, D.G.Hoffman,D.A Leonard, C.C. Lindner,,K.T. Pheips,C.A, Βασικές αρχές θεωρίας κωδικοποίησης και κρυπτογραφίας ,εκδώσεις κλειδάριθμος.
2. W. Stallings, Κρυπτογραφία και ασφάλεια δικτύων 2004.
3. N. Sklavos, X. Zhang, Wireless Security & Cryptography: Specifications and Implementations, CRC-Press, A Taylor & Francis Group, ISBN: 084938771X, 2007.
4. Rodriguez-Henriquez, N.A. Saqib, A. Diaz Perez, C. Kaya Koc, Cryptographic Algorithms and Reconfigurable Computing, Springer, ISBN 0387338837, 2006.
5. Darrel Hankerson, Alfred Menezes, and Scott Vanstone, “Guide to Elliptic Curve Cryptography”, Springer, 2004.
6. Stefan Mangard, Elisabeth Oswald, Thomas Popp, “Power Analysis Attacks: Revealing the Secrets of Smart Cards”, Springer, 2007.
7. David Challener, Kent Yoder, Ryan Catherman , David Safford ,Leendert Van Doorn, “A practical guide to trusted computing”, IBM Press, 2007.
8. James S. Kraft, Lawrence C. Washington, “An Introduction to Number Theory with Cryptography”, Chapman and Hall/CRC, 2013.
9. Luther Martin, “Introduction to Identity-Based Encryption”, (Information Security and Privacy Series), Artech House, 2008.
10. Paris Kitsos and Yang Zhang, “RFID Security: Techniques, Protocols and System-On-Chip Design”, Springer, 2008.
11. Yang Zhang and Paris Kitsos, “Security in RFID and Sensor Networks”, Auerbach Publications, 2009.
12. James Joshi, “Network Security: Know It All”, Morgan Kaufmann, 2008.
13. Stefan Mangard, Elisabeth Oswald, Thomas Popp, “Power Analysis Attacks: Revealing the Secrets of Smart Cards”, Springer, 2007.
14. Mohammad Tehranipoor, Cliff Wang, “Introduction to Hardware Security and Trust”,
15. “Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology”, Andreas Pfitzmann and Marit Hanse
16. “Privacy-enhancing Technologies for the Internet”, I. Goldberg, D. Wagner, E. Brewer, IEEE Spring COMPCON, 1997.
17. “Privacy-enhancing technologies for the Internet, II: Five years later”, Ian Goldberg, PET 2002.
18. “Privacy-enhancing technologies for the Internet III: Ten years later”,Ian Goldberg, “Digital Privacy:

Theory, Technologies and Practices", Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis, and Sabrina De Capitani di Vimercati, editors, 2007

19. “Untraceable electronic mail, return addresses, and digital pseudonyms”, David Chaum, Communications of the ACM, 1981