

ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ - ΚΡΥΠΤΟΓΡΑΦΙΑ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΕΠΙΣΤΗΜΩΝ ΠΛΗΡΟΦΟΡΙΑΣ		
ΤΜΗΜΑ	ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΠΡΟΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	ΠΛ0618	ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ	Z
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Κρυπτογραφία		
ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ 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	5
Εργαστηριακές Ασκήσεις		1	
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (δ).			
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ γενικού υποβάθρου, ειδικού υποβάθρου, ειδικευσης γενικών γνώσεων, ανάπτυξης δεξιοτήτων	ΕΙΔΙΚΟΥ ΥΠΟΒΑΘΡΟΥ		
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	ΔΙΑΚΡΙΤΑ ΜΑΘΗΜΑΤΙΚΑ		
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	ΕΛΛΗΝΙΚΗ		
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	ΟΧΙ		
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://classroom.google.com/c/NzE5MjcxOTg0MTQ5 Κωδικός τάξης: quscwm6		

(2) ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα Περιγράφονται τα μαθησιακά αποτελέσματα του μαθήματος οι συγκεκριμένες γνώσεις, δεξιότητες και ικανότητες κατάλληλου 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 το Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης - Περιγραφικοί Δείκτες Επιπέδων 6, 7 & 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης και το Παράρτημα Β - Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων
Με την ολοκλήρωση του μαθήματος, οι φοιτητές θα είναι σε θέση να: - διακρίνουν την κλασσική από τη μοντέρνα κρυπτογραφία, - περιγράφουν τις αρχές λειτουργίας ενός κρυπτοσυστήματος, - προσδιορίζουν τους διαφορετικούς στόχους της κρυπτογραφίας, όπως εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα και μη-απάρνηση, - αναγνωρίζουν και να εξηγούν τη διαφορά μεταξύ συμμετρικής και ασύμμετρης κρυπτογραφίας, - απαριθμούν διαφορετικά κρυπτοσυστήματα, - περιγράφουν βασικούς κρυπταλγόριθμους, όπως AES, Diffie-Hellman, RSA, Ελλειπτικές καμπύλες,

- προσδιορίζουν τα υπολογιστικά προβλήματα στα οποία βασίζουν τη λειτουργία τους τα μοντέρνα κρυπτοσυστήματα,
- εξετάζουν την ασφάλεια κρυπτοσυστημάτων,
- περιγράφουν βασικές επιθέσεις,
- να προσομοιώνουν με προγραμματισμό τη λειτουργία βασικών κρυπτοσυστημάτων ή επιθέσεων, και
- αξιοποιούν τη γνώση τους στην επίλυση πραγματικών προβλημάτων

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

Προσαρμογή σε νέες καταστάσεις

Λήψη αποφάσεων

Αυτόνομη εργασία

Ομαδική εργασία

Εργασία σε διεθνές περιβάλλον

Εργασία σε διεπιστημονικό περιβάλλον

Παραγωγή νέων ερευνητικών ιδεών

Σχεδιασμός και διαχείριση έργων

Σεβασμός στη διαφορετικότητα και στην πολυπολιτισμικότητα

Σεβασμός στο φυσικό περιβάλλον

Επίδειξη κοινωνικής, επαγγελματικής και ηθικής υπευθυνότητας και

ευαισθησίας σε θέματα φύλου

Άσκηση κριτικής και αυτοκριτικής

Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

.....

Άλλες...

.....

- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και
- των απαραίτητων τεχνολογιών
- Αυτόνομη εργασία
- Παραγωγή νέων ερευνητικών ιδεών

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Το περίγραμμα ύλης του μαθήματος περιλαμβάνει:

- Κλασσική Κρυπτογραφία - Απλά κρυπτοσυστήματα
- Κρυπτανάλυση και Κρυπτογραφικές Συναρτήσεις
- Συμμετρική Κρυπτογραφία - Κρυπταλγόριθμοι τμήματος - Advanced Encryption Standard (AES)
- Ασύμμετρη Κρυπτογραφία - Τα κρυπτοσυστήματα RSA και ElGamal
- Κρυπτογραφία ελλειπτικών καμπυλών (ECC) - κρυπτοσυστήματα EC (ElGamal, ανταλλαγή κλειδιών Diffie-Hellman)
- Ψηφιακές υπογραφές
- Συναρτήσεις διασποράς

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ <i>Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.</i>	Πρόσωπο με πρόσωπο (διαλέξεις με φυσική παρουσία)
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ <i>Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές</i>	Οι Τεχνολογίες Πληροφορίας και Επικοινωνιών (ΤΠΕ) που χρησιμοποιούνται στα πλαίσια του μαθήματος είναι τα εξής: • χρήση διαφανειών για την υποστήριξη των διαλέξεων, • χρήση λογισμικού ανοιχτού κώδικα για προγραμματισμό (SageMath) για την επίδειξη βασικής λειτουργικότητας κρυπταλγορίθμων,

	• διαμοιρασμός αρχείων (π.χ. ασκήσεις, εργασίες, λύσεις, εκπαιδευτικό υλικό) μέσω του ολοκληρωμένου συστήματος ασύγχρονης τηλεεκπαίδευσης Google classroom • ηλεκτρονική αλληλογραφία (email) και ανακοινώσεις.																						
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ Περιγράφονται αναλυτικά ο τρόπος και μέθοδοι διδασκαλίας. Διαλέξεις, Σεμινάρια, Εργαστηριακή Άσκηση, Άσκηση Πεδίου, Μελέτη & ανάλυση βιβλιογραφίας, Φροντιστήριο, Πρακτική (Τοποθέτηση), Κλινική Άσκηση, Καλλιτεχνικό Εργαστήριο, Διαδραστική διδασκαλία, Εκπαιδευτικές επισκέψεις, Εκπόνηση μελέτης (project), Συγγραφή εργασίας / εργασιών, Καλλιτεχνική δημιουργία, κ.λπ. Αναγράφονται οι ώρες μελέτης του φοιτητή για κάθε μαθησιακή δραστηριότητα καθώς και οι ώρες μη καθοδηγούμενης μελέτης σύμφωνα με τις αρχές του ECTS	<table> <tr> <th>Δραστηριότητα</th><th>Φόρτος Εργασίας Εξαμήνου</th></tr> <tr> <td>Διαλέξεις</td><td>26 ώρες</td></tr> <tr> <td>Εργαστηριακό μάθημα</td><td>13 ώρες</td></tr> <tr> <td>Εβδομαδιαίες εργασίες</td><td>48 ώρες</td></tr> <tr> <td>Μελέτη / προετοιμασία για τις εξετάσεις</td><td>60 ώρες</td></tr> <tr> <td></td><td></td></tr> <tr> <td></td><td></td></tr> <tr> <td></td><td></td></tr> <tr> <td></td><td></td></tr> <tr> <td></td><td></td></tr> <tr> <td>Σύνολο Μαθήματος:</td><td>147 ώρες</td></tr> </table>	Δραστηριότητα	Φόρτος Εργασίας Εξαμήνου	Διαλέξεις	26 ώρες	Εργαστηριακό μάθημα	13 ώρες	Εβδομαδιαίες εργασίες	48 ώρες	Μελέτη / προετοιμασία για τις εξετάσεις	60 ώρες											Σύνολο Μαθήματος:	147 ώρες
Δραστηριότητα	Φόρτος Εργασίας Εξαμήνου																						
Διαλέξεις	26 ώρες																						
Εργαστηριακό μάθημα	13 ώρες																						
Εβδομαδιαίες εργασίες	48 ώρες																						
Μελέτη / προετοιμασία για τις εξετάσεις	60 ώρες																						
Σύνολο Μαθήματος:	147 ώρες																						
ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ Περιγραφή της διαδικασίας αξιολόγησης 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 Αναφέρονται ρητά προσδιορισμένα κριτήρια αξιολόγησης και εάν και που είναι προσβάσιμα από τους φοιτητές.	(1) Γλώσσα Αξιολόγησης: Ελληνική (2) Μέθοδοι Αξιολόγησης: (i) Γραπτή τελική εξέταση που δύναται να περιλαμβάνει: • θεωρητικές ερωτήσεις, • ερωτήσεις σύντομης απάντησης, • ερωτήσεις πολλαπλής επιλογής, • ασκήσεις, και • επίλυση προβλημάτων (ii) Αξιολόγηση ατομικών εβδομαδιαίων εργασιών (3) Ο τελικός βαθμός προκύπτει κατά 80% από το βαθμό της τελικής γραπτής/εργαστηριακής εξέτασης (κλίμακα 0 – 10) και κατά 20% από το βαθμό των ατομικών εβδομαδιαίων ασκήσεων (κλίμακα 0 – 10), μόνο στην περίπτωση που ο βαθμός της τελικής εξέτασης είναι προβιβάσιμος (≥ 5). Διαφορετικά, ο τελικός βαθμός ισοδυναμεί με το 80% του βαθμού της τελικής εξέτασης. Οι βαθμοί των εβδομαδιαίων εργασιών και η βαθμολογία της γραπτής αξιολόγησης ανακοινώνονται στο Google Classroom.																						

--	--

(5) ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

1. Βασίλειος Κάτος, Γεώργιος Στεφανίδης, Τεχνικές κρυπτογραφίας & κρυπτανάλυσης, Θεσσαλονίκη: Ζυγός, 2003.
2. Δημήτριος Πουλάκης, Κρυπτογραφία: η επιστήμη της ασφαλούς επικοινωνίας, Θεσσαλονίκη: Εκδόσεις Ζήτη, 2006.
3. Christof Paar, Jan Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.
4. A. McAndrew, *Introduction to Cryptography with open-source software*. CRC Press, 2016.
5. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*. CRC press, 1996

- Συναφή επιστημονικά περιοδικά:

1. *Designs, Codes, and Cryptography*, Kluwer Academic Publishers
2. *Cryptography and Communications*, Springer
3. *IEEE Transactions on Information Forensics and Security*
4. *ACM Computing Surveys*
5. *Mathematics of Computation*, American Mathematical Society
6. *SIAM Journal on Computing*, Society for Industrial and Applied Mathematics