994 Κρυπτογραφία και Blockchain Εφαρμογές

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΠΡΟΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	994	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	9
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**Κρυπτογραφία και Blockchain Εφαρμογές**		
ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ		**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Διάφορες μορφές διδασκαλίας		5	5
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ	Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων		
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	--		
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική ή/και Αγγλική		
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Ναι		
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ	https://eclass.chania.teicrete.gr/courses/		

2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα

Το μάθημα φιλοδοξεί να μυήσει τον φοιτητή στην κρυπτογραφία, η οποία αποτελεί επιστημονικό κλάδο της Κρυπτολογίας, και κατά συνέπεια πραγματεύεται την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης/αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Έτσι, στόχος του μαθήματος είναι η κατανόηση των αντιπροσωπευτικότερων κλασσικών και μοντέρνων τεχνικών κρυπτογραφίας και κρυπτανάλυσης, η κατανόηση των μαθηματικών εννοιών που θα αποτελέσουν τα θεμέλια για την περιγραφή των κρυπτογραφικών τεχνικών κρυπτογράφησης και ψηφιακής υπογραφής, αλλά και των αρχών λειτουργίας των μοντέρνων κρυπτοσυστημάτων, όπως και η εξοικείωση με τους μηχανισμούς δημόσιου κλειδιού (ΔΚ) που χρησιμοποιούνται για την προστασία της εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας των μηνυμάτων που ανταλλάσσονται μεταξύ απομακρυσμένων οντοτήτων σε μη ασφαλή δίκτυα.

Με την επιτυχή ολοκλήρωση του μαθήματος ο φοιτητής θα είναι σε θέση:

- Να περιγράφει και να εξηγεί τις βασικές έννοιες της κρυπτογραφίας.
- Να κρυπτογραφεί και αποκρυπτογραφεί μηνύματα με αλγορίθμους αντικατάστασης ή/και αλγορίθμους αναδιάταξης.
- Να κρυπταναλύει έναν κλασσικό κρυπτογραφικό αλγόριθμο ώστε να αποκτήσει πρόσβαση στο αρχικό μήνυμα ή/και στο κρυπτογραφικό κλειδί.
- Να κατανοεί τις αρχές λειτουργίας, την δομή και την ασφάλεια των μοντέρνων συμμετρικών αλγορίθμων για την προστασία της εμπιστευτικότητας και της ακεραιότητας/αυθεντικότητας των μηνυμάτων που ανταλλάσσονται σε ένα δίκτυο επικοινωνίας
- Να καθορίζει τις προϋποθέσεις για την επίτευξη απόλυτης ασφάλειας σε ένα κρυπτογραφικό πρωτόκολλο.
- Να μετατρέπει έναν κρυπτογραφικό αλγόριθμο σε απολύτως ασφαλή και να αποδεικνύει την ασφάλεια του.
- Να διατυπώνει και να εξηγεί τα σημαντικότερα μαθηματικά προβλήματα στα οποία βασίζεται σήμερα η κρυπτογραφία ΔΚ
- Να περιγράφει και να υλοποιεί τις τεχνικές που χρησιμοποιούν οι συμμετρικοί αλγόριθμοι για την κρυπτογράφηση μηνυμάτων και τον υπολογισμό της τιμής Hash η MAC τους,
- Να κρυπτογραφεί / αποκρυπτογραφεί μηνύματα με τον Αλγόριθμο DES,
- Να χρησιμοποιεί τον κατάλληλο τρόπο λειτουργίας για την κρυπτογράφηση μηνυμάτων, οποιουδήποτε μήκους, με έναν αλγόριθμο τμήματος ή ροής,
- Να χρησιμοποιεί έναν αλγόριθμο τμήματος για τον υπολογισμό της τιμής hash ή MAC ενός μηνύματος,
- Να συνδυάζει τεχνικές προστασίας της εμπιστευτικότητας και της αυθεντικότητας για την προστασία ενός καναλιού επικοινωνίας.
- Να περιγράφει και να υλοποιεί τις τεχνικές που χρησιμοποιούν οι αλγόριθμοι ΔΚ για την κρυπτογράφηση και ψηφιακή υπογραφή μηνυμάτων,
- Να εντοπίζει τις αδυναμίες ενός κρυπτογραφικού αλγόριθμου ΔΚ, καθώς και τους τρόπους αντιμετώπισης των,

Γενικές Ικανότητες

Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
Λήψη αποφάσεων
Αυτόνομη εργασία
Ομαδική εργασία
Σχεδιασμός και διαχείριση έργων
Άσκηση κριτικής και αυτοκριτικής
Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Ιστορική αναδρομή, θεμελιώδεις έννοιες και ορολογία.
Κλασσικοί Αλγόριθμοι – Ασφάλεια και Κρυπτανάλυση. Μονοαλφαβητικοί Αλγόριθμοι Αντικατάστασης: Αλγόριθμος Ολίσθησης, Γενικευμένος Αλγόριθμος Αντικατάστασης, Αλγόριθμος Affine. Πολυαλφαβητικοί Αλγόριθμοι Αντικατάστασης: Αλγόριθμος Vigenere, Αλγόριθμος Hill. Κλασσικοί Αλγόριθμοι Αναδιάταξης: Αλγόριθμος Μετάθεσης. Απόλυτη και Υπολογιστική Ασφάλεια. Ο Αλγόριθμος One-Time-Pad (OTP). Εντροπία και Ασφάλεια Κρυπτοαλγορίθμων. Πλεονασμός Φυσικής Γλώσσας και Ασφάλεια. Απόσταση Ενοποίησης. Τυχαιότητα και Ψευδοτυχαιότητα: Γεννήτριες ψευδοτυχαίων αριθμών.
Μοντέρνα Συμμετρικά Κρυπτοσυστήματα: Αλγόριθμοι Τμήματος ή Ομάδας ή Δέσμης (Block Ciphers) και Αλγόριθμοι Ροής ή Στοιχειοσειράς (Stream Ciphers). Αλγόριθμος DES, Αλγόριθμος Triple-DES, Αλγόριθμος S/DES. Τρόποι ή παραλλαγές λειτουργίας συμμετρικών αλγορίθμων: Τρόποι ECB, CBC, OFB, CFB, CTR. Ακεραιότητα με Μονόδρομες Συναρτήσεις Hash: Σχεδίαση και Ασφάλεια συναρτήσεων Hash, εφαρμογές στην ασφάλεια συστημάτων και δικτύων. Αυθεντικότητα με Συναρτήσεις MAC: Σχεδίαση και ασφάλεια συναρτήσεων MAC, εφαρμογές στην ασφάλεια συστημάτων και δικτύων. Τεχνική Χρησιμοποίησης Περεταίρω Πληροφορίας (Salt)
Μοντέρνα Ασύμμετρα Συστήματα Δημόσιου Κλειδιού (ΔΚ). Κρυπτογράφηση με τον Αλγόριθμο RSA. Ο Αλγόριθμος Rabin. Ο Αλγόριθμος κρυπτογράφησης Elgamal. Ο Αλγόριθμος Κρυπτογράφησης Goldwasser-Micali. Ψηφιακή Υπογραφή με αλγορίθμους ΔΚ. Ψηφιακή Υπογραφή με τον Αλγόριθμο RSA.
Διαχείριση Δημόσιου Κλειδιού: Κεντρικά Μοντέλα Εμπιστοσύνης – Υποδομές ΔΚ: Ιεραρχική πιστοποίηση, Δια-πιστοποίηση, Ιεραρχίες Πολλών Επιπέδων. Μοντέλα Κατανεμημένης Εμπιστοσύνης. Το μοντέλο PGP.
Κρυπτογραφικές υπηρεσίες: Μυστικότητα (Secrecy), Εμπιστευτικότητα (Confidentiality), Πιστοποίηση ή Αυθεντικότητα (Authentication), Ακεραιότητα (Integrity) και Αδυναμία αποκήρυξης (Non-Repudiation), τόσο με συμμετρικά όσο και με κρυπτοσυστήματα ΔΚ.

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

<table>
<tr><td>ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ</td><td>Πρόσωπο με πρόσωπο θεωρητική διδασκαλία.
Εργαστηριακή εκπαίδευση σε ομάδες φοιτητών (ανά 20).
Ασκήσεις πράξης σε μικρές ομάδες φοιτητών.</td></tr>
<tr><td>ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ</td><td>Χρήση λογισμικού παρουσίασης διαφανειών
Επικοινωνία με τους φοιτητές μέσω πλατφόρμας ασύγχρονης τηλεκπαίδευσης.</td></tr>
<tr><td>ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ</td><td>
<table>
<tr><th>Δραστηριότητα</th><th>Φόρτος Εργασίας Εξαμήνου</th></tr>
<tr><td>Διαλέξεις</td><td>26</td></tr>
<tr><td>Εργαστηριακές ασκήσεις (υποχρεωτική παρουσία)</td><td>13</td></tr>
<tr><td>Ασκήσεις Πράξης (υποχρεωτική παρουσία)</td><td>13</td></tr>
<tr><td>Εκπόνηση εργαστηριακών εργασιών / τεχνικών αναφορών σε μικρές ομάδες</td><td>26</td></tr>
<tr><td>Εκπόνηση ατομικών εργασιών εξάσκησης</td><td>26</td></tr>
<tr><td>Ατομική μελέτη</td><td>33</td></tr>
<tr><td>Σύνολο Μαθήματος</td><td>137</td></tr>
</table>
</td></tr>
<tr><td>ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ</td><td>I. Γραπτή τελική εξέταση (ΓΕ) (70%)
- Επίλυση προβλημάτων/υπολογισμοί
- Συγκριτική αξιολόγηση στοιχείων θεωρίας
II. Εργαστηριακή εξέταση (ΕΕ) (15%)
- Εργαστηριακές εργασίες/τεχνικές αναφορές/μετρήσεις σε μικρές ομάδες
III. Εξέταση σε ασκήσεις πράξης (ΑΠ) (15%)
- Ατομικές εργασίες εξάσκησης
Ο βαθμός του μαθήματος (ΓΕ*0,7 + ΕΕ*0,15+ ΑΠ*0,15) πρέπει να είναι τουλάχιστον πέντε (5).
Ο βαθμός καθενός από τα I, II, III πρέπει να είναι τουλάχιστον τρία (3).
Τα κριτήρια αξιολόγησης είναι προσβάσιμα στους φοιτητές από την ηλεκτρονική σελίδα του μαθήματος και ανακοινώνονται στο πρώτο μάθημα.</td></tr>
</table>

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- *Προτεινόμενη Βιβλιογραφία:*

Ελληνικά ή μεταφρασμένα διδακτικά συγγράμματα:

- Κωνσταντίνος Πατσάκης, Ευάγγελος Φούντας, *Κρυπτογραφία και Εφαρμογές*, Εκδόσεις Βαρβαρήγου, 2016 (ISBN: 978-960-7996-57-2, Κωδικός στον Εύδοξο: 59395497)
- William Stallings, *Κρυπτογραφία και Ασφάλεια Δικτύων – Αρχές και Εφαρμογές*, Εκδόσεις ΜΑΡΙΑ ΠΑΡΙΚΟΥ & ΣΙΑ ΕΠΕ, 2011, (ISBN: 9789604117307, Κωδικός Βιβλίου στον Εύδοξο: 12777632)
- M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας. Β. Χρυσικόπουλος, *Σύγχρονη Κρυπτογραφία – Θεωρία και Εφαρμογές*, Παπασωτηρίου, 2010. (ISBN: 978-960-7182-76-0, Κωδικός Βιβλίου στον Εύδοξο: 9771)
- Δημήτριος Πουλάκης, *Κρυπτογραφία – Η επιστήμη της ασφαλούς επικοινωνίας*, Εκδόσεις Ζήτη Πελαγία & Σια Ι.Κ.Ε., 2004. (ISBN: 960-431-926-4, Κωδικός Βιβλίου στον Εύδοξο: 11068)
- Δημήτρης Βούκαλης, *Εφαρμοσμένη Κρυπτογραφία – θεωρία - πράξη*, Εκδόσεις ΣΥΓΧΡΟΝΗ ΕΚΔΟΤΙΚΗ ΕΠΕ, 2007. (ISBN 978-960-6674-09-9, Κωδικός Βιβλίου στον Εύδοξο: 15628)

Ξενόγλωσσα διδακτικά συγγράμματα:

- Behrouz A. Forouzan, *Cryptography and Network Security,* McGraw Hill, 2007. (ISBN:0073327530 9780073327532)
- Schneier, Bruce, *Applied Cryptography*, 2 ed, Wiley, 1996.(ISBN 0-471-11709-9)
- A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, 1996, (ISBN 0-8493-8523-7).
- Mike Rosulek, *The Joy of Cryptography*, 2018. {Presents modern cryptography at a level appropriate for undergraduates}.