Διάταξη Θεματικής Ενότητας
ΑΥΔ621 / ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Σχολή	ΣΘΕΕ	ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΕΠΙΣΤΗΜΩΝ		
Πρόγραμμα Σπουδών	ΑΥΔ	ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ		
Θεματική Ενότητα	ΑΥΔ621	Κρυπτογραφία		
Επίπεδο	**Προπτυχιακό**	**Μεταπτυχιακό**		
		Μάστερ	**Διδακτορικό**	
		X		
Γλώσσα Διδασκαλίας	ΕΛΛΗΝΙΚΗ			
Τύπος Διδασκαλίας	Εξ αποστάσεως			
Τύπος Θεματικής Ενότητας	***Υποχρεωτική***	***Επιλογής***		
	X			
Αριθμός Ομαδικών Συμβουλευτικών Συναντήσεων	***Σύνολο***	***Φυσική Παρουσία***	***Τηλεσυναντήσεις***	
	13		**13**	
Αριθμός Εργασιών	*2*			
Υπολογισμός Τελικής Βαθμολογίας	**Εργασίες**	**Δραστηριότητες**	**Τελικές Εξετάσεις**	
	30 **%**	*20* **%**	*50* **%**	
Αριθμός Ευρωπαϊκών Πιστωτικών Μονάδων (ECTS)	*10*			

Περιγραφή Θεματικής Ενότητας

Αντικείμενο της Θ.Ε είναι οι βασικές έννοιες, αρχές και εφαρμογές των κρυπτογραφικών συστημάτων. Στο πλαίσιο της Θ.Ε θα καλυφθούν θέματα κρυπτογράφησης ιδιωτικού και δημόσιου κλειδιού, θα παρουσιαστούν οι πλέον διαδεδομένοι αλγόριθμοι κρυπτογράφησης, τα χαρακτηριστικά ασφαλείας τους, ενώ επίσης θα δοθεί έμφαση σε συναφή θέματα όπως οι συναρτήσεις κατακερματισμού και οι ψηφιακές υπογραφές. Περαιτέρω, θα γίνει επισκόπηση σε σύγχρονα ζητήματα που άπτονται του ευρύτερου πλαισίου της κρυπτολογίας, καθώς επίσης και παρουσίαση των ανοιχτών ερευνητικών προβλημάτων του χώρου. Με την επιτυχή ολοκλήρωση της ενότητας οι φοιτητές θα αποκτήσουν κατανόηση των σημαντικότερων κρυπτογραφικών αλγορίθμων και συστημάτων και την ικανότητα για την αξιολόγηση τους, με αναγνώριση των ευπαθειών αλλά και των τρόπων αντιμετώπισής τους.

Γνώσεις – δεξιότητες – στάσεις

Ο/Η φοιτητής/-τρια που θα ολοκληρώσει επιτυχώς την εν λόγω Θ.Ε, αναμένεται ότι θα είναι σε θέση να:

- Γνωρίσει την ιστορία της κρυπτογραφίας και το ρόλο που έχει διαδραματίσει σε διάφορες περιόδους
- Αποκτήσει το απαραίτητο θεωρητικό υπόβαθρο σχετικά με τους κρυπτογραφικούς αλγορίθμους και τις εφαρμογές τους.
- Αναλύει και εφαρμόζει βασικές αρχές σχεδίασης κρυπτογραφικών αλγορίθμων.
- Αξιολογεί προτεινόμενα κρυπτογραφικά σχήματα ως προς την ασφάλεια και απόδοσή τους.
- Αξιολογεί κρυπτογραφικές ακολουθίες ως προς χαρακτηριστικά τυχαιότητας
- Εφαρμόζει θεωρητικές γνώσεις στην πράξη, επιλύνοντας προβλήματα ασφάλειας επικοινωνιών που άπτονται της κρυπτογραφίας.
- Αναγνωρίζει τη βέλτιστη κρυπτογραφική λύση που απαιτείται σε κάθε εφαρμογή.
- Αναγνωρίζει την αναγκαιότητα της αυθεντικοποιημένης κρυπτογράφησης

- Αξιοποιεί τις κρυπτογραφικές λύσεις που παρέχονται στην τεχνολογία του Διαδικτύου (ψηφιακά πιστοποιητικά, πρωτόκολλο SSL/TLS κτλ.), έχοντας πλήρη κατανόηση του τρόπου λειτουργίας τους και των χαρακτηριστικών ασφαλείας τους.
- Χρησιμοποιεί κρυπτογραφικά εργαλεία λογισμικού (Openssl, PGP, Sage (BooleanFunctions βιβλιοθήκη), υλοποίηση αλγορίθμου Berlekamp-Massey για κρυπτανάλυση, Cryptool).
- Γνωρίζει ειδικά θέματα κρυπτογραφίας, όπως τις έννοιες ομομορφικής κρυπτογράφησης, και πρωτοκόλλων μηδενικής γνώσης
- Αναγνωρίζει τη σπουδαιότητα της κρυπτογραφίας ως προς την αντιμετώπιση ζητημάτων που απορρέουν από νομικές απαιτήσεις αναφορικά με την προστασία προσωπικών δεδομένων και ιδιωτικότητας
- Γνωρίζει τα χαρακτηριστικά των τεχνολογιών blockchain.
- Γνωρίζει τα σύγχρονα ανοιχτά ερευνητικά προβλήματα και τις νέες τάσεις στην κρυπτογραφία.

Προ-απαιτούμενες Θεματικές Ενότητες	
-	**-**

Συν-απαιτούμενες Θεματικές Ενότητες	
-	**-**

Σύνθεση Βαθμολογίας			
Τρόπος Αξιολόγησης	***Βαρύτητα στον τελικό βαθμό***	***Φόρτος εργασίας***	
		Ώρες	***ECTS***
Εβδομαδιαίες Διαδραστικές Δραστηριότητες	*20* **%**	*175-210*	*7*
Εργασία 1	*15* **%**	*25-30*	*1*
Εργασία 2	*15* **%**	*25-30*	*1*
Τελική/Επαναληπτική Εξέταση	*50* **%**	*25-30*	*1*
Σύνολο	**100%**	***250-300***	***10***

Κανονισμοί Βαθμολογίας και Τρόποι Αξιολόγησης

- Ένας/Μια φοιτητής/-τρια βαθμολογείται με 9, εάν συγκεντρώσει το 90% της πιθανής βαθμολόγησης, δηλαδή, 90%*10=9, και ούτω καθεξής.
- Βαθμός επιτυχίας (Passing rate)
  - 50% στις Γραπτές Εργασίες
  - 50% στις Διαδραστικές Δραστηριότητες
  - Δικαίωμα συμμετοχής στις τελικές εξετάσεις μιας Θ.Ε. έχουν οι φοιτητές/-τριες που κατοχύρωσαν τον ελάχιστο απαιτούμενο βαθμό (≥ 50%) τόσο στις Γραπτές Εργασίες όσο και στις Διαδραστικές Δραστηριότητες
  - 50% στην Τελική εξέταση

Αν ένας/μια φοιτητής/-τρια συγκεντρώσει βαθμολογία με δεκαδικό ψηφίο, τότε αυτό στρογγυλοποιείται στην πλησιέστερη μισή μονάδα.