<table>
<tr><td>Τίτλος Μαθήματος</td><td colspan="5">Ασφάλεια Υπολογιστικών Συστημάτων και Δικτύων</td></tr>
<tr><td>Κωδικός Μαθήματος</td><td colspan="5">ΗΜΥ 457</td></tr>
<tr><td>Τύπος μαθήματος</td><td colspan="5">Επιλογής</td></tr>
<tr><td>Επίπεδο</td><td colspan="5">Προπτυχιακό</td></tr>
<tr><td>Έτος / Εξάμηνο φοίτησης</td><td colspan="5">4ο Έτος / 1ο ή 2ο Εξάμηνο</td></tr>
<tr><td>Όνομα Διδάσκοντα</td><td colspan="5">Γεώργιος Έλληνας</td></tr>
<tr><td>ECTS</td><td>6</td><td>Διαλέξεις / εβδομάδα</td><td>2 x 1.5 ώρες (διαλέξεις) + 1 ώρα (φροντ.) ανά εβδομάδα</td><td>Εργαστήρια / εβδομάδα</td><td></td></tr>
<tr><td>Στόχοι Μαθήματος</td><td colspan="5">• Παροχή γνώσης και κατανόησης των θεμελιωδών ζητημάτων και των λύσεων για την επίτευξη ασφαλών επικοινωνιών.
• Κάλυψη ενός μεγάλου συνόλου θεμάτων που σχετίζονται με την ασφάλεια των πληροφοριών και του δικτύου.
• Κάλυψη πτυχών της ασφάλειας από τη θεωρία στην πράξη</td></tr>
<tr><td>Μαθησιακά Αποτελέσματα</td><td colspan="5">• Κατάδειξη γνώσης και κατανόησης ζητημάτων ασφάλειας.
• Δυνατότητα να προσδιοριστούν απειλές ασφάλειας υπολογιστών και δικτύων, ταξινόμηση των απειλών και ανάπτυξη ενός πρότυπο ασφάλειας που αποτρέπει, που ανιχνεύει και που ανακτεί από τις επιθέσεις.
• Κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων χρησιμοποιώντας τμήματα ciphers, υπογραφή και έλεγχος των μηνυμάτων χρησιμοποιώντας τους γνωστούς αλγορίθμους παραγωγής και επαλήθευσης υπογραφών.
• Ανάλυση υπάρχουσας επικύρωσης και των βασικών πρωτοκόλλων συμφωνίας, προσδιορισμός των αδυναμιών αυτών των πρωτοκόλλων.</td></tr>
<tr><td>Προαπαιτούμενα</td><td colspan="2">ΗΜΥ 360</td><td>Συναπαιτούμενα</td><td colspan="2"></td></tr>
<tr><td>Περιεχόμενο Μαθήματος</td><td colspan="5">Επισκόπηση απειλών και προβλημάτων ασφάλειας Εισαγωγή στην Ασφάλεια: ιδιότητες ασφαλείας, επιθέσεις και κατηγορίες απειλών, σχεδιασμός ασφάλειας σε διάφορα επίπεδα δικτύου. Ασφαλείς επικοινωνίες: κρυπτογράφηση και αποκρυπτογράφηση. Κρυπτολογική ανάλυση και υπολογιστική πολυπλοκότητα. Κρυπτογραφήματα αντικατάσταση, μετατόπισης, και γινομένων. Πρότυπα κρυπτογράφησης στοιχείων (DES). Αρθρωτή αριθμητική. Κρυπτογράφηση με δημόσιο κλειδί: μέθοδοι RSA, σακιδίου (knapsack) και παραγοντοποίησης. Μέθοδοι απόδειξης ταυτότητας και κρυπτογραφικά πρωτόκολλα. Ψηφιακή υπογραφή.</td></tr>
</table>

Μεθοδολογία Διδασκαλίας	• Διαλέξεις • Κατ' οίκον εργασίες
Βιβλιογραφία	• W. Stallings, *Network Security Essentials: Applications and Standards*, Prentice Hall, 3rd Ed., 2007. • W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, 2013. • M. Bishop, *Introduction to Computer and Network Security*, Pearson, 2005.
Αξιολόγηση	• Κατ' οίκον εργασίες • Ενδιάμεση εξέταση • Τελική εξέταση
Γλώσσα	Ελληνική