CREDITS AND CONTACT HOURS: Credit Hours: 3, Contact Hours: 45

COORDINATOR:
Dr. Mahalingam Ramkumar


SPECIFIC COURSE INFORMATION:
Catalog Description: Three hours lecture. Basic and advanced concepts in cryptography and
network security: symmetric and asymmetric cryptography, key management, wired and
wireless network Internet security protocols, network systems security.
   a. Prerequisites: CSE 4153/6153
   a. Required/Elective:
      Computer Science – Elective
      Software Engineering – Selected Elective
      Computer Engineering - Elective

SPECIFIC GOALS OF THE COURSE:
a. Specific Outcomes of Instruction:
   1. To develop students' ability to understand the need for cryptographic
      primitives and cryptographic protocols.
   2. To develop students' ability understand the need and strategies for key
      distribution.
   3. To develop students' ability to understand a variety of Internet security issues
      in various Internet layers, and feasible strategies and existing protocols to
      address security issues.
   b. Criterion 3 Outcomes:
      Note: Parenthesized list indicates the ABET EAC and CAC outcomes addressed by
      each performance criteria.
      1. Gain understanding of fundamental concepts behind Symmetric and
         Asymmetric Ciphers, Hash functions, Keyed Message Authentication Codes
         (HMAC) and Digital signatures. (CAC: a,c,j); (EAC: a,c)
      2. Apply knowledge of mathematics to understand and analyze cryptographic
         techniques (CAC: a,b,j), (EAC: a,b)
      3. Understand issues and techniques related to key distribution. (CAC: b,c,g,i,k),
         (EAC: b,c,e,h,j)
      4. Comprehend security issues in networking infrastructure (CAC: a,c,e,g),
         (EAC: a,c,f,h)
      5. Develop understanding of security issues in networked applications
         (CAC:a,c,e,g,k), (EAC: a,c,f,h,k)
6. Gain understanding of various security protocols (employed at different network layers) (CAC: a,e,h), (EAC:a,f,i)

<table>
<thead>
<tr>
<th>TOPICS COVERED</th>
<th>(Number of class hrs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction:</td>
<td>2</td>
</tr>
<tr>
<td>2. Classical Cryptography</td>
<td>2</td>
</tr>
<tr>
<td>3. Symmetric Cryptography</td>
<td>6</td>
</tr>
<tr>
<td>4. Asymmetric Cryptography</td>
<td>6</td>
</tr>
<tr>
<td>5. Key management</td>
<td>6</td>
</tr>
<tr>
<td>7. System Security</td>
<td>4</td>
</tr>
<tr>
<td>8. Exams</td>
<td>5</td>
</tr>
</tbody>
</table>