# Cryptographic Engineering

**ON-LINE CLASS by Microsoft TEAMS**

**May 31 - June 11, 2021**

<table>
<thead>
<tr>
<th>WEEK 1</th>
<th>MAY 31 - JUNE 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Modules (1:30hr each), 2 Modules per day</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WEEK 2</th>
<th>JUNE 7-11</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 Modules (1:30hr each), 2 Modules per day, except on Friday 1 module</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DAILY</th>
<th>Central European Time</th>
<th>Eastern Standard Time</th>
<th>Pacific Standard Time</th>
<th>India Standard Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CET (Lausanne)</td>
<td>EST (New York)</td>
<td>PST (California)</td>
<td>IST (India)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module 1</th>
<th>3:00-4:30 pm</th>
<th>9:00-10:30 am</th>
<th>6:00-7:30 am</th>
<th>7:30-9:00 pm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 2</td>
<td>5:00-6:30 pm</td>
<td>11:00 am -12:30 pm</td>
<td>8:00-9:30 am</td>
<td>9:30-11:00 pm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WEEK 1</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday, May 31</td>
<td>1 Introduction to Block Ciphers; DES and AES</td>
</tr>
<tr>
<td></td>
<td>2 Lightweight Block Ciphers for RFIDs</td>
</tr>
<tr>
<td>Tuesday, June 1</td>
<td>1 Specialized Hardware for Secret-Key Algorithms</td>
</tr>
<tr>
<td></td>
<td>2 Introduction to PUFs (Physically Unclonable Functions)</td>
</tr>
<tr>
<td>Wednesday, June 2</td>
<td>1 Integer Arithmetic Algorithms and Architectures</td>
</tr>
<tr>
<td></td>
<td>2 Finite Field Arithmetic Algorithms and Architectures</td>
</tr>
<tr>
<td>Thursday, June 3</td>
<td>1 Public-Key Cryptography: Algorithms and Protocols</td>
</tr>
<tr>
<td></td>
<td>2 Public-Key Cryptographic Hardware and Embedded Systems</td>
</tr>
<tr>
<td>Friday, June 4</td>
<td>1 Trusted Computing Architectures, SSL and IPSec</td>
</tr>
<tr>
<td></td>
<td>2 Introduction to Side-Channel Analysis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WEEK 2</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday, June 7</td>
<td>1 RSA - Side Channel Attacks &amp; Countermeasures</td>
</tr>
<tr>
<td></td>
<td>2 Electromagnetic Attacks, Countermeasures &amp; Advanced Analysis Techniques</td>
</tr>
<tr>
<td>Tuesday, June 8</td>
<td>1 ECC - Side Channel Attacks &amp; Countermeasures</td>
</tr>
<tr>
<td></td>
<td>2 Implementations of Fully Homomorphic Encryption Methods</td>
</tr>
<tr>
<td>Wednesday, June 9</td>
<td>1 Side Channel Attacks to Block Ciphers: DES &amp; AES</td>
</tr>
<tr>
<td></td>
<td>2 Countermeasures for Block Ciphers</td>
</tr>
<tr>
<td>Thursday, June 10</td>
<td>1 Random Number Generators for Cryptographic Applications</td>
</tr>
<tr>
<td></td>
<td>2 Evaluation Criteria Non-Deterministic Random Number Generators</td>
</tr>
<tr>
<td>Friday, June 11</td>
<td>1 Random Number Generator Design Constraints and Challenges</td>
</tr>
<tr>
<td></td>
<td>0.5 Course Evaluation</td>
</tr>
</tbody>
</table>

| Course Evaluation | Vlado Valence, All |

<table>
<thead>
<tr>
<th>Friday, June 11</th>
<th>Cryptographic Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON-LINE CLASS by Microsoft TEAMS</td>
<td></td>
</tr>
</tbody>
</table>

**May 31 - June 11, 2021**