** به نام خدا سال تحصیلی:**

|  |  |  |  |
| --- | --- | --- | --- |
| شماره تلفن:73225048 | شماره اتاق: 419 | نام مدرس: دکتر فتحیان | دانشکده : صنایع |
| نام درس : امنیت تجارت الکترونیکی |
| Email:fathian@iust.ac.ir | پیشنیاز:----- | تعدادواحد: **3** |
| **جایگاه درس در برنامه درسی دوره :****درس امنیت تجارت الکترونیکی به عنوان یکی از دروس اصلی در برنامه درسی رشته مهندسی تجارت الکترونیکی محسوب می شود.** |
| هدف کلی :**هدف از این درس آشنایی با اصول، مفاهیم و مکانیزم های تامین امنیت فناوری اطلاعات و تجارت الکترونیکی است**. |
| **اهداف عینی:**  اهداف مفهومی: **آشنایی با مفاهیم امنیت فناوری اطلاعات و به ویژه تجارت الکترونیکی**  اهداف مهارتی :**توانمندی درک، تحلیل،طراحی و بکارگیری مفاهیم و روش های تامین امنیت تجارت الکترونیکی** اهداف نگرشی :نگاه عمیق و مفهومی به امنیت فناوری اطلاعات و تاثیر آن بر تحقق ایمن تجارت الکترونیکی |
| **امکانات آموزشی: رایانه متصل به اینترنت و ویدئو پروژکتور همراه با امکانات اولیه موردنیاز برای تدریس**  |

**محتوای درس :**

|  |  |  |
| --- | --- | --- |
| **محتویات موضوع** | **موضوع** | هفته |
| **مفهوم امنیت فناوری اطلاعات - تهدیدات فعال و غیرفعال\_ سایر دسته بندی های تهدیدات امنیتی- روند مقابله با تهدیدات در فضای سایبر- چگونگی مدیریت خطرات و تدوین سیاستها، خدمات و مکانیز مهای امنیتی** | **آشنایی با مفهوم امنیت فناوری اطلاعات و تهدیدات امنیتی** | 1 |
| **چگونگی تحقق مکانیزم صحت داده-ویژگی ها و شرایط توابع درهم (HASH)-ساختار تابع SHA و MD4و MD5 – حملات نوع اول و دوم به توابع درهم- بررسی حمله روز تولد** | **مکانیزم صحت داده** | 2 |
| **مروری بر روش های رمز کلاسیک – روش های رمز تک الفبایی و چند الفبایی- قانون شانون و روش رمز کامل** | **مکانیزم رمزگذاری کلاسیک** | 3 |
| **شرایط و ویژگیهای روش رمز متقارن- ساختار و تحلیل عملکرد هر یک ازآلگوریتمهای DES, 2DES,3DES** | **مکانیزم های رمز گذاری مدرن - متقارن** | 4 |
| **شرایط و ویژگیهای روش رمز نامتقارن- ساختار و تحلیل عملکرد آلگوریتم RSA – بررسی و تحلیل عملکرد آلگوریتم منحني هاي بيضوي و مقایسه آن با سایر آلگوریتم ها** | **مکانیزم های رمز گذاری مدرن - نامتقارن** | 5 |
| **مکانیزمهای امضای دیجیتال- ساختار آلگوریتم DSS – ساختار آلگوریتم ECDSS- مروری بر مدل های کنترل دسترسی- مدلهای کنترل دسترسی اجباری و اختیاری(دیوار چین- بل لا پادولا و ...)** | **مکانیزم امضای دیجیتال و کنترل دستیابی** | 6 |
| **مفهوم و چگونگی تحقق مکانیزم تبادل احراز هویت- پروتکل بدون دانش ZK – پروتکل Guillou – Quisquater- کاربرد های این پروتکل** | **مکانیزم های تبادل احراز هویت** | 7 |
| **حمله تحلیل ترافیک و مکانیز مهای پوشش ترافیک-مکانیز مهای جلوگیری از حمله تکرار مجدد و حفظ تازگی پیام** | **مکانیزم های پوشش ترافیک و تازگی پیام** | 8 |
| **مفهوم مدیریت کلید- تولید و توزیع کلید- گواهي ها و پروتكلهاي تبادل و توافق كليد ( Diffe-Hellman، ....) –ساختار و استاندارد های ایجاد گواهی ها- زیر ساخت کلید عمومی -ساختار و وظایف مراکز CA** | **مدیریت کلید و گواهی ها** | 9 |
| **تهدیدات در رو شهای مختلف پرداخت الکترونیکی -انواع خدمات امنیت پرداخت الکترونیکی (گمنامی کاربر- عدم ردیابی مکان-گمنامی پرداخت کننده، عدم انکار، تازگی پیام و ....)** | **امنیت پرداخت الکترونیکی و دسته بندی خدمات امنیتی مرتبط** | 10 |
| **خدمات امنیتی پول الکترونیکی- مکانیزم امضای کور-خدمات امنیتی محافظت در مقابل دزدی، جعل، سرقت و استفاده مجدد سکه** | **امنیت پول الکترونیک** | 11 |
| **تهدیدات در چک الکترونیکی- مفهوم پراکسی-امنیت اجازه انتقال پرداخت -پروتکل کربروس** | **امنیت چک الکترونیک** | 12 |
| **تشریح عملکرد و ویژگیهای پروتکل های امنیتی شبیه SSL، iKp، SET و IPSEC** | **پروتکل های امنیت پرداخت** | 13 |
| **آشنایی با برخی از استاندارد های مدیریت امنیت پرداخت-استاندارد BS7799 و مراحل تحقق امنیت اطلاعات** | **مدیریت امنیت اطلاعات و استانداردهای ذیربط** | 14 |
| **مفاهیم و روش های آشکار سازی مزاحمت- آلگوریتم های مطرح IDS- مفاهیم و روش های تحقق فایروال – استفاده از فایروال در لایه های مختلف شبکه** | **سیستم های آشکار سازی مزاحمت و سیستم های فایروال** | 15 |
| **امنیت کارت هوشمند، امنیت عامل­های متحرک ،چالش ها و روش های تحقق حریم خصوصی، مکانیزم های تحقق گمنامی ، امنیت وب** | **سایر مباحث در حوزه امنیت وب و شبکه** | 16 |
| **منابع درس** |
| **1\_Vesna Hessler, Security fundamentals for E-commerce, Artech House,2000****2\_ David A. Montague, Essentials of Online payment Security and Fraud Prevention, John Wiley & Sons, 2010.****3-William Stallings, Network and Internetwork Security, Prentice Hall, 1995****3\_  Rolf Oppliger, Internet and Intranet Security, Second Edition, Artech House, 2002** |

**شیوه ارزیابی :**

|  |  |  |
| --- | --- | --- |
| **درصد نمره** | **عنوان** | **ردیف** |
| 10 | حضور فعال در کلاس | **1** |
| 20 | انجام تحقیقات موضوعی و ارائه نتایج در کلاس شامل:**ARTICLE REVIEW, CONCEPT REVIEW** | **2** |
| 70 | امتحان میان ترم و پایان ترم | **3** |

**وظایف دانشجویان :**

|  |  |
| --- | --- |
| **شرح وظایف** | **ردیف** |
| **حضور فعال در کلاس** | **1** |
| **مطالعه منابع درسی** | **2** |
| **انجام تحقیقات موضوعی و ارائه نتایج در کلاس** | **3** |
| شرکت در جلسات امتحان | **4** |