



دانشکده علوم ریاضی و آمار



مدرس: دکتر مجتبی رفیعی

نیمسال دوم ۱۴۰۰-۱۴۰۱

رمزنگاری

اهداف درس

هدف از ارائه این درس آشنایی دانشجویان مقطع کارشناسی با مفاهیم اولیه امنیت داده و شبکه در حوزه سایبری است. به طور دقیق تر، دانشجویان در این درس با انواع تهدیدهای امنیتی، نیازمندیهای امنیتی، خدمات امنیتی، پروتکل های امنیتی و مکانیزم های امنیتی با تکیه بر ابزارهای رمزنگاری آشنا خواهند شد.

سر فصل مطالب

- مفاهیم و تعاریف اولیه،
- مکانیزم های تامین امنیت،
- مفاهیم رمزنگاری و رمزنگاری سنتی،
- رمزنگاری متقارن،
- رمزنگاری نامتقارن،
- کدهای تصدیق اصالت پیام و توابع چکیده ساز،
- امضای رقمی و زیرساخت کلید عمومی،
- طراحی پروتکل های رمزنگاری،
- متناسب با زمان باقی مانده تا پایان ترم: پروتکل کربروس، PGP، IPSec، SSL/TLS، دیوار آتش، سیستم تشخیص نفوذ، کنترل دسترسی.

منابع درس

- W. Stallings, Cryptography and network security principles and practices, 6th edition, 2011.
- Matt. Bishop, Introduction to computer security, 2005.

لازم به ذکر است که دانشجویان عزیز می توانند جزییات تدریس شده هر یک از جلسات در طول ترم را از طریق پیوند زیر دنبال کنند.

<https://mojtaba-rafiee.github.io/Teaching/DNS/>

شیوه گذراندن موفق درس

جهت فهم کامل محتوای این درس علاوه بر شرکت در کلاس و مطالعه یادداشت‌های کلاسی، توصیه می‌شود مراجع اصلی درس نیز مطالعه شود. ضمن آنکه حل کامل تمرین‌ها می‌تواند کمک قابل توجهی در درک کامل مطالب این درس داشته باشد. به طور متوسط این درس در هفته نیاز به ۴ ساعت مطالعه و صرف وقت جهت انجام تمرین‌ها و مرور مفاهیم تدریس شده دارد.

شیوه ارزیابی درس

هدف از اخذ این درس کسب دانش و نه کسب نمره است. نمره تنها ملاکی نه چندان کامل از میزان یادگیری شماست. ارزیابی دانشجویان این درس بر اساس موارد است.

- امتحان میان‌ترم (۶ نمره)
- امتحان پایان ترم (۸ نمره)
- تکالیف (۴ نمره)
- فعالیت‌های کلاسی و گزارش‌نویسی (۲ نمره)

نمرات ممکن است در انتهای ترم، بسته به کیفیت محتوایی هریک از موارد فوق، اندکی تغییر کند. لازم به ذکر است که به بخش مربوط به فعالیت‌های کلاسی و گزارش‌نویسی ممکن است آیت‌های بیشتری در طول ترم اضافه شود.

برخی نکات مهم

- انجام تکالیف به صورت انفرادی است. حل گروهی تکالیف، نسخه‌برداری از پاسخ‌های دیگران و استفاده از مطالب موجود در اینترنت منجر به اعمال نمره منفی معادل نمره کل تمرین (برای سری مربوطه) خواهد شد.
- از آنجاییکه هدف از تکالیف تعیین شده یادگیری و مدیریت زمان توسط شما دانشجویان عزیز است، لذا رعایت مهلت‌های زمانی اعلام شده برای تحویل تمرین‌ها الزامی است.
- حداقل دو سری از تمرین‌ها می‌بایست توسط \LaTeX نوشته شود. دیگر تمرینات را در صورت تمایل می‌توانید با لاتک تهیه کنید و تا ۱۰٪ نمره‌ی اضافه کسب نمایید. در غیر این صورت، تمرین‌هایی که دستی نوشته می‌شوند باید با کیفیتی مطلوب و حجمی پایین، اسکن و ارسال شوند.
- نامگذاری فایل تمرین باید به صورت "studentno_HWX.pdf" باشد، جاییکه studentno شماره دانشجویی شما و X شماره سری تمرین است.

انتقادات/پیشنهادهات

به منظور بالا بردن کیفیت درس و رضایت حداکثری، دانشجویان عزیز می‌توانند به طور پیوسته از اولین جلسه کلاس تا بعد از ثبت نهایی نمرات پایان ترم از طریق پیوند زیر، انتقادات و پیشنهادات خود را با استاد درس مطرح کنند. لازم به ذکر است که ثبت بازخوردهای شما دانشجویان عزیز به صورت کاملاً گمنام صورت گرفته و از این منظر با آسودگی خاطر اقدام به ثبت نظرات خود نمایید.

<https://forms.gle/vZAUvGERdSvuDm66>

دستیارهای آموزشی و نحوه رفع اشکال

اسامی دستیارهای آموزشی این درس به همراه رایانامه آنها در زیر آمده است. جهت ارتباط با دستیارهای آموزشی می‌توانید از طریق رایانامه اقدام نمایید.

– دستیار شماره ۱، mail1@mail.com

– دستیار شماره ۲، mail2@mail.com

– دستیار شماره ۳، mail3@mail.com

– دستیار شماره ۴، mail4@mail.com

جهت رفع هرگونه اشکال در خصوص محتویات درس نیز می‌توانید به دستیارهای آموزشی و یا مستقیماً با بنده از طرق رایانامه زیر مطرح نمایید. لازم به ذکر است که در صورت مکاتبه با دستیارهای آموزشی، رونوشت آن را به استاد درس نیز ارسال نمایید (یعنی در رایانامه ارسالی بنده را سی‌سی (CC) کنید).

ui.cs.dns.rafaee@gmail.com

نکات مهم ارسال رایانامه

- رایانامه‌های خود را صرفاً با نام رسمی خود به اینجانب بفرستید؛ برای این‌کار در تنظیمات ایمیل خود نام و نام خانوادگی خود را به انگلیسی وارد کنید. علاوه بر این حتماً در انتهای رایانامه‌تان، نام خود را به فارسی بنویسید.
- عنوان رایانامه خود را به صورت “عنوان مناسب” [“DNS:: Request”](#) یا “DNS:: Request for meeting” می‌توانند عنوان رایانامه شما باشد.
- رایانامه‌های خود را صرفاً به فارسی (با الفبای عربی) یا به انگلیسی بفرستید. از ارسال ایمیل به فارسی با الفبای لاتین (فینگلیش) جداً خودداری نمایید.

بازهای زمانی امتحانات و تمرین‌ها

- امتحان پایان‌ترم: ۲۶ خرداد ماه ۱۴۰۱ ساعت ۰۸:۰۰ برگزار می‌شود.
- امتحان میان‌ترم: در جلسات ابتدایی تعیین خواهد شد.

رعایت اصول اخلاقی

- یکی از اهداف تمرین نگارشی، یاد گرفتن \LaTeX می‌باشد. بنابراین فایل \LaTeX را باید خودتان تهیه کنید و آماده کردن آن توسط دیگران، هرچند نگارش آن از خودتان باشد، به هیچ‌وجه مجاز نیست.
- مشورت و بحث در مورد تمرینات و پروژه‌ها آزاد است؛ ولی دانشجویان باید آنها را شخصاً بنویسند. پیدا کردن پاسخ‌ها از اینترنت یا متن کتاب (به جز کتاب حل‌المسائل)، در صورتی که خود به تنهایی آن را یافته باشید، مانعی ندارد، هر چند توصیه نمی‌شود؛ مگر اینکه پس از چند روز فکر کردن بر روی سوال به نتیجه نرسیده باشید. در هر صورت، بازنویسی از روی پاسخ‌هایی که در مراجع دیگر می‌یابید، حداقل سه روز پس از دیدن راه‌حل و بدون مراجعه مجدد به آن باید انجام شود. پیاده‌سازی تمامی کدها (اعم از زبان‌های برنامه‌نویسی، نرم‌افزارهای محاسباتی و لاتک) و نوشتن گزارش آن‌ها باید توسط دانشجو به صورت انفرادی و بدون مراجعه به اینترنت انجام شود. همچنین نوشتن تمرین به صورت گروهی مجاز نیست و مصداق تقلب محسوب می‌شود. به خاطر داشته باشید هرگونه به اشتراک‌گذاری کدها و تمرینات با سایر دانشجویان، و یا ارسال آن‌ها در اینترنت و شبکه‌های اجتماعی نقض صریح اصول اخلاقی این درس محسوب می‌شود. در صورت مشاهده و یا اطلاع از هر یک از موارد ذکر شده، نمره شخص خاطی ۰/۲۵ لحاظ خواهد شد.