دانشکده علوم ریاضی و آمار

مدرس: **دکتر مجتبی رفیعی** نیمسال دوم ۱۴۰۰-۱۴۰۱

مبانی نظری رمزنگاری

اهدف درس

این درس برای دانشجویان کارشناسی ارشد و به منظور آشنایی با مفاهیم رمزنگاری مدرن در نظر گرفته شده است. دانشجویان با گذراندن این درس توانمندی لازم برای تبدیل یک سناریو مدل واقعی از یک فرآیند امنیتی را به یک مجموعه از مفاهیم حاوی تعاریف رسمی نحوی و امنیتی فرا می‌گیرند و مهارت‌های لازم برای ارائه اولیه‌های رمزنگاری با امنیت اثبات‌پذیر را کسب می‌کنند.

سر فصل مطالب

- **مقدمات:** رمزنگاری کلاسیک و مدرن، امنیت کامل و محدودیت‌های آن، امنیت محاسباتی، تمایزناپذیری محاسباتی.
- **رمزنگاری کلید خصوصی (متقارن):** نحو سیستم رمز متقارن، تعاریف امنیتی مختلف برای رمز متقارن (تک‌پیامی، چندپیامی، متن اصلی انتخابی، متن رمزی انتخابی)، مولدهای شبه‌تصادفی، توابع شبه‌تصادفی، جایگشت‌های شبه تصادفی.
- **کد اصالت‌سنجی پیام:** تفاوت محرمانگی و اصالت پیام، نحو کد اصالت سنجی پیام، تعاریف امنیتی (جعل‌ناپذیری ضعیف و قوی)، ساختارهای اصالت سنجی پیام (برای پیامهای با طول ثابت و متغیر)، رمزنگاری احراز اصالت شده.
- **توابع چکیده‌ساز و کاربردها:** نحو و تعاریف امنیتی تابع چکیده‌ساز، ساخت کد اصالت سنجی پیام با استفاده از تابع چکیده‌ساز، حملات عام، مدل سروش تصادفی، کاربردها (پروتکلهای تعهد، درخت مرکل و ...).
- **رمزنگاری کلید عمومی (نامتقارن):** مرور کلی (تاریخچه، سناریوی استفاده، نحو و ...)، ناممکن بودن امنیت کامل، تعاریف امنیتی (متن اصلی انتخابی، متن رمزی انتخابی)، فرض‌های سختی (مساله لگاریتم گسسته، مساله‌های دیفی-هلمن محاسباتی و تصمیمی، مساله‌های تجزیه و محاسبه ریشه در هنگ اعداد مرکب)، سیستم‌های رمز نامتقارن الجمال و RSA، رمزنگاری ترکیبی و پارادایم KEM-DEM.
- **امضای دیجیتال:** نحو و تعاریف امنیتی امضای دیجیتال، پارادایم hash-and-sign، امضای RSA و امضاهای مبتنی بر لگاریتم گسسته (DSA و اشنور).

منابع درس

- Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography, Second Edition, CRC Press 2014.
- Dan Boneh and Victor Shoup: A graduate course in applied cryptography. Preprint version 0.5, Jan. 2020.

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

https://mojtaba-rafiee.github.io/Teaching/CRYPTO/

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 ۵ تا ۷ 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 آیتم‌های 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/پیشنهادات

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 کاملا گمنام صورت گرفته و از این منظر با آسودگی خاطر اقدام به ثبت نظرات خود نمایید.

https://forms.gle/DYVN۴nnowUaVScvFA

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، *mail۱@mail.com*
- دستیار شماره ۲، *mail۲@mail.com*
- دستیار شماره ۳، *mail۳@mail.com*
- دستیار شماره ۴، *mail۴@mail.com*

جهت رفع هر گونه اشکال در خصوص محتویات درس نیز می‌توانید به دستیارهای آموزشی و یا مستقیما 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.crypto.rafiee@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 ::CRYPTO" انتخاب کنید. مثلاً "درخواست ملاقات ::CRYPTO" یا "::CRYPTO Request for meeting" می‌توانند عنوان رایانامه شما باشد.
- رایانامه‌های خود را صرفا 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:** ۲۹ خرداد ماه ۱۴۰۱ ساعت ۰۸:۰۰ برگزار می‌شود.
- **امتحان میان‌ترم:** در جلسات ابتدایی تعیین خواهد شد.

رعایت اصول اخلاقی

- یکی از اهداف تمرین نگارشی، یادگرفتن 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 دانشجو باید آنها را شخصا بنویسد. 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 شبکه های 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.