Shahid Beheshti University

رمزنگاری

هادی سلیمانی

پژوهشکده فضای مجازی دانشگاه شهید بهشتی

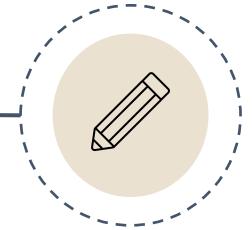
مجوز استفاده و نشر

- اجازه‌ی ایجاد نسخه‌های دیجیتالی جدید براساس بخشی یا تمام مطالب این اسلاید بدون پرداخت هزینه اعطا می‌شود، مشروط بر این‌که:
  - فقط به‌منظور و در راستای استفاده‌ی آموزشی (شخصی و یا کلاسی) ساخته شده باشند و برای کسب هرگونه سود و یا مزیت تجاری استفاده نشوند.
  - نسخه‌های جدید حاوی ارجاع مستقیم به نام تهیه‌کننده اسلاید (هادی سلیمانی) و محل کار وی (پژوهشکده فضای مجازی دانشگاه شهید بهشتی) باشند.
- مجموعه‌ی حاضر براساس نظرات ارزشمند دانشجویان (سابق) دانشگاه شهید بهشتی و همکاران محترم تهیه شده است که از تمام آن‌ها قدردانی می‌شود؛

  (به‌خصوص خانم‌ها **سارا زارعی** و **فاطمه عزیزی** نقش مهمی را در تهیه نسخه‌ی نهایی بر عهده داشته‌اند. خانم مهندس زارعی علاوه بر کمک در آماده‌سازی نسخه‌ی فعلی اسلایدها، در تصحیح اشتباهات نسخه‌ی قبلی و همچنین تکمیل و بازتعریف محتوای درس‌ها بسیار تاثیرگذار بوده‌اند).
- برای مشاهده‌ی اسلایدها و ویدئوهای تدریس این درس به آدرس زیر مراجعه فرمایید:

http://facultymembers.sbu.ac.ir/h_soleimany/cryptography-course/

درس صفرم

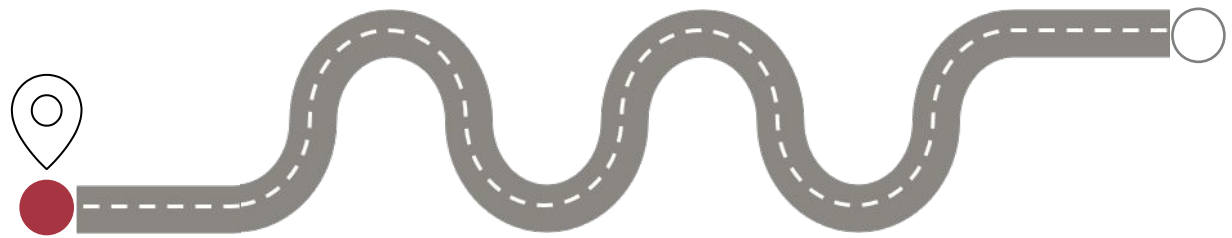


مقدمه‌ای بر درس رمزنگاری

فهرست عناوین درس

مقدمه‌ای بر درس رمزنگاری

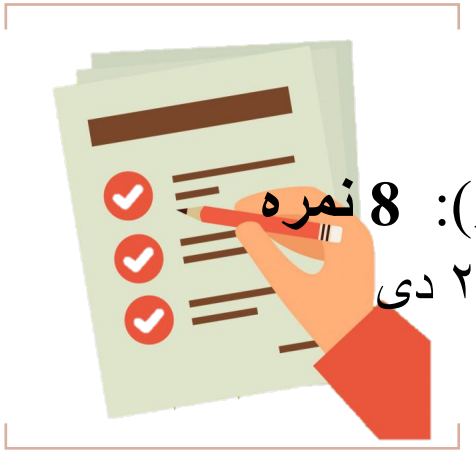
- اطلاعات کلی درس
- آشنایی با علم رمزنگاری
- آشنایی با حملات و مقایسه‌ی آن‌ها
- سرفصل‌های درس
- معرفی مراجع
- تریبون آزاد دانشجویی :)



اطلاعات
کلی درس

شیوه‌ی ارزیابی (تقریبی)

1. کار کلاسی (برای این درس 7 سری تمرین در نظر گرفته شده است): **۴ نمره**
   - کلاس حل تمرین: دوشنبه‌ها ساعت ۱۰-۱۱:۳۰
   - شرکت در کلاس حل تمرین اجباری است و در نمره‌ی شما تاثیر مستقیم دارد.
2. میان‌ترم (شامل مقدمات و رمزنگاری متقارن): **۸ نمره و به‌صورت حذفی**
   - زمان: چهارشنبه ۱۷ آذر (در ساعت کلاس)
3. پایان‌ترم (شامل رمزنگاری کلید عمومی و توابع درهم‌ساز): **8 نمره**
   - زمان: براساس اعلام دانشگاه (سیستم گلستان): چهارشنبه ۲۲ دی



ساعت‌های رفع اشکال یا مراجعه‌ی دانشجویان

- پس از اتمام کلاس و یا جلسه‌ی حل تمرین، می‌توانید برای رفع اشکال در کلاس بمانید.
- زمان‌های دیگر از طریق هماهنگی قبلی:

hadi.soleimany@gmail.com

درس‌افزار

- تمرین‌ها و اسلایدها در درس‌افزار قرار می‌گیرند:

https://courseware.sbu.ac.ir

آشنایی با علم
رمزنگاری

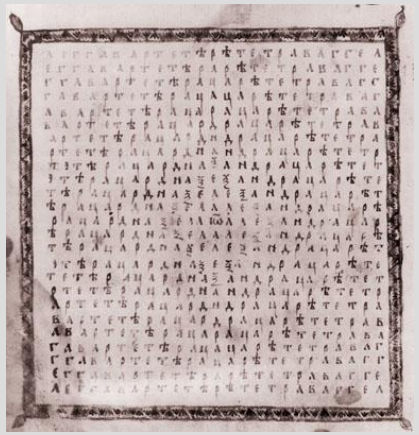
اطلاعات
کلی درس

تاریخ مختصری از علم رمزنگاری

- تا ابتدای قرن بیستم: استفاده از روش‌های ساده‌ی جانشانی و جابه‌جایی حروف که به صورت دستی انجام می‌شد!
- تا جنگ جهانی دوم: استفاده از ماشین‌های الکترومکانیکی به منظور به کارگیری روش‌های جانشانی و جابه‌جایی پیچیده‌تر.

سکیتال (یونان باستان)

ماشین Enigma (آلمان- جنگ جهانی دوم)

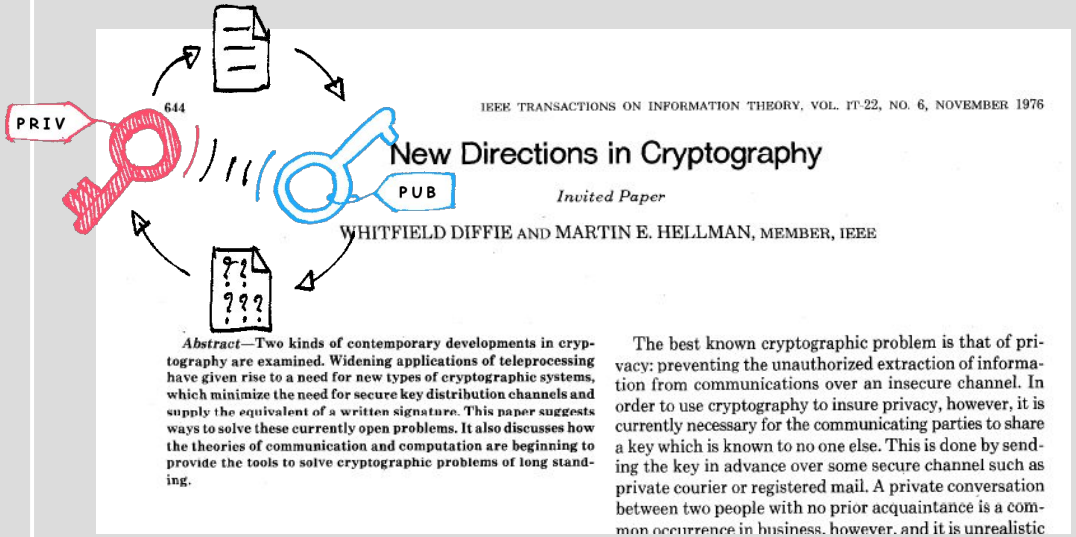


مربع جادویی حروف برای رمزنگاری و رمزگشایی انجیل

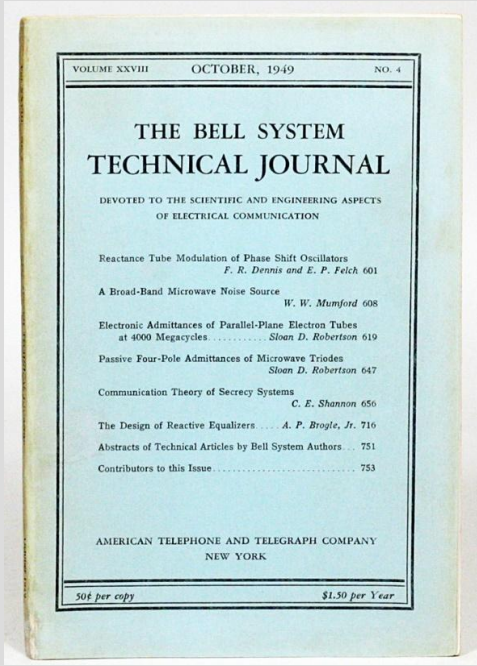
تاریخ مختصری از علم رمزنگاری

... ادامه

- سال 1949: انتشار مقاله‌ی شانون به همراه پیشرفت‌های الکترونیکی.
- سال 1976: ارائه‌ی رمزنگاری کلید عمومی توسط Diffie و Hellman که امکان به کارگیری گسترده‌ی رمزنگاری را در کاربردهای تجاری ایجاد کرد.



مقاله‌ی تاریخی دفی - هلمن



مقاله‌ی تاریخی شانون

تاریخ مختصری از علم رمزنگاری

... ادامه

- تجاری‌سازی رایانه‌های شخصی، گسترش روزافزون شبکه‌های کامپیوتری و پیشرفت‌های سریع در تکنولوژی مدارهای مجتمع: فراگیر شدن رمزنگاری در کاربردهای غیرنظامی.
- ما هر روز از رمزنگاری استفاده می‌کنیم: ایمیل، باز کردن درب خودرو، تلفن همراه، پرداخت‌های بانکی، ....
- امروزه رمزنگاری از یک هنر به یک علم تبدیل شده است.

رمزنگاری SSL/TLS

امضاهای دیجیتال

بانکداری آنلاین امن

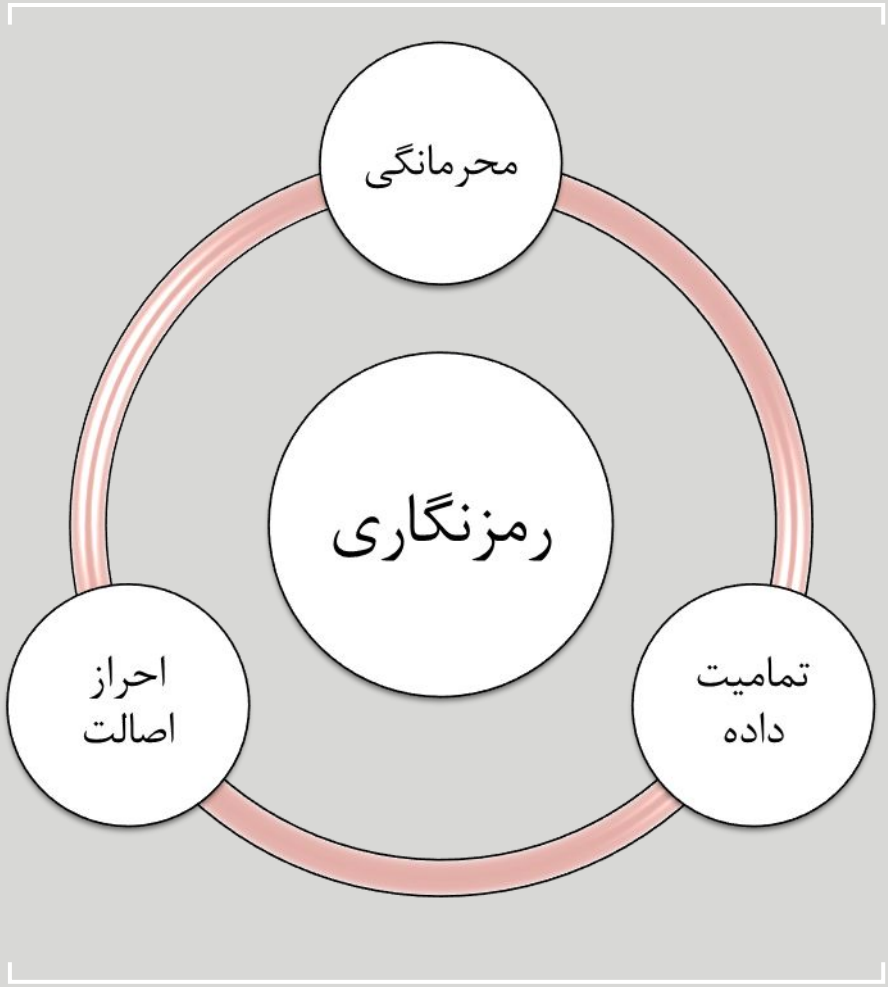
پیام‌رسان‌های امن

و ...

رمزنگاری ایمیل‌ها

رمزارزها

اهداف رمزنگاری



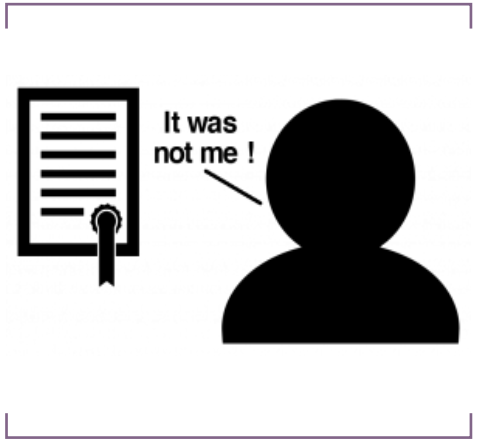
- سه هدف اصلی که می‌توانند در طراحی سیستم‌های رمزنگاری مدنظر قرار گیرند، عبارت‌اند از:

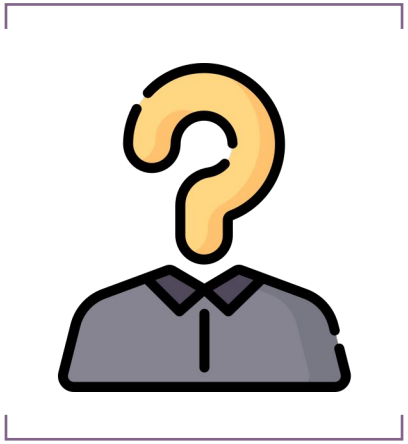
1. **محرمانگی (Confidentiality):**
   - افراد غیرمجاز نتوانند اطلاعات را مشاهده کنند.
2. **احراز اصالت (Authentication):**
   - تایید اینکه چیزی (نظیر هویت یک فرد یا منشا یک پیام) اصل و معتبر است.
3. **تمامیت داده (Data Integrity):**
   - این اطمینان را فراهم می‌کند که پیام دریافتی دقیقا همان پیامی است که توسط فرستنده ارسال شده است.

اهداف رمزنگاری

... ادامه

- سیستم‌های رمزنگاری ممکن است برای برآوردن اهداف دیگری نیز به کار روند:
  1. حفظ حریم خصوصی (Privacy Preserving)
  2. انکارناپذیری (Non-Repudiation)
  3. گمنامی (Anonymity)
  4. ...





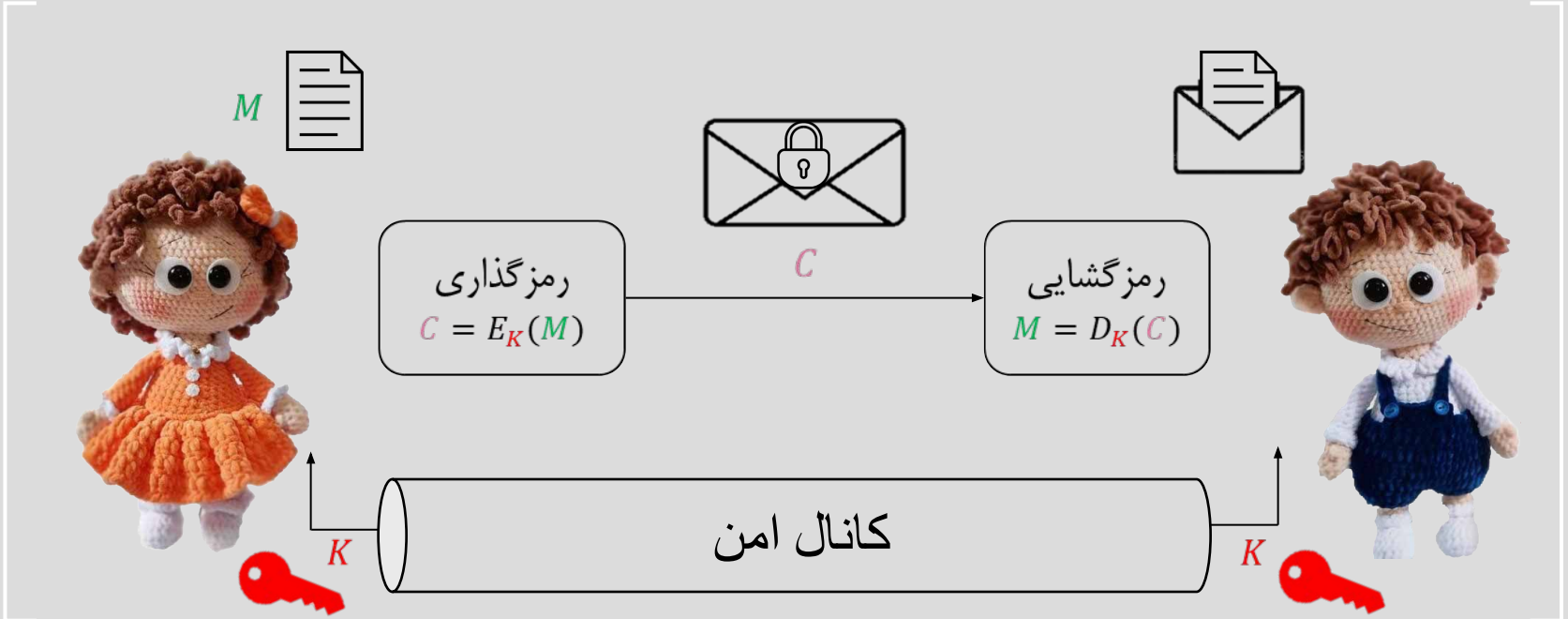
هدف اول: محرمانگی

- آلیس و باب می‌خواهند از طریق یک کانال ناامن (مثل اینترنت) که در معرض رصد مهاجم(ها) قرار دارد، یک ارتباط امن برقرار کنند.

رمزنگاری متقارن

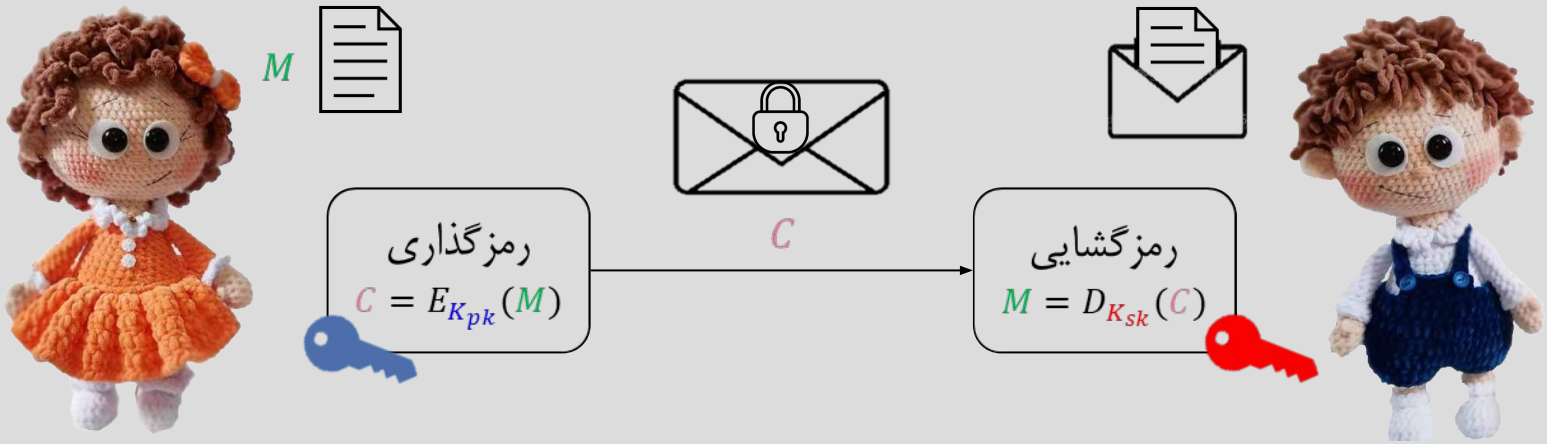
- راهکار اول:

  از طریق یک کانال دیگر که امن است، یک کلید مبادله کنند و سپس از رمزنگاری استفاده کنند.



رمزنگاری کلید عمومی (نامتقارن)

- راهکار دوم:
  - برای رمزگذاری و رمزگشایی از دو فرآیند متفاوت استفاده می‌شود.
  - یک کلید (عمومی) برای رمزگذاری از طریق کانال ناامن اعلام می‌شود تا هر فردی بتواند عملیات رمزگذاری را انجام دهد.
  - اما عمل رمزگشایی را تنها از طریق یک کلید مخفی می‌توان انجام داد.



مولفه‌های یک سیستم رمزنگاری

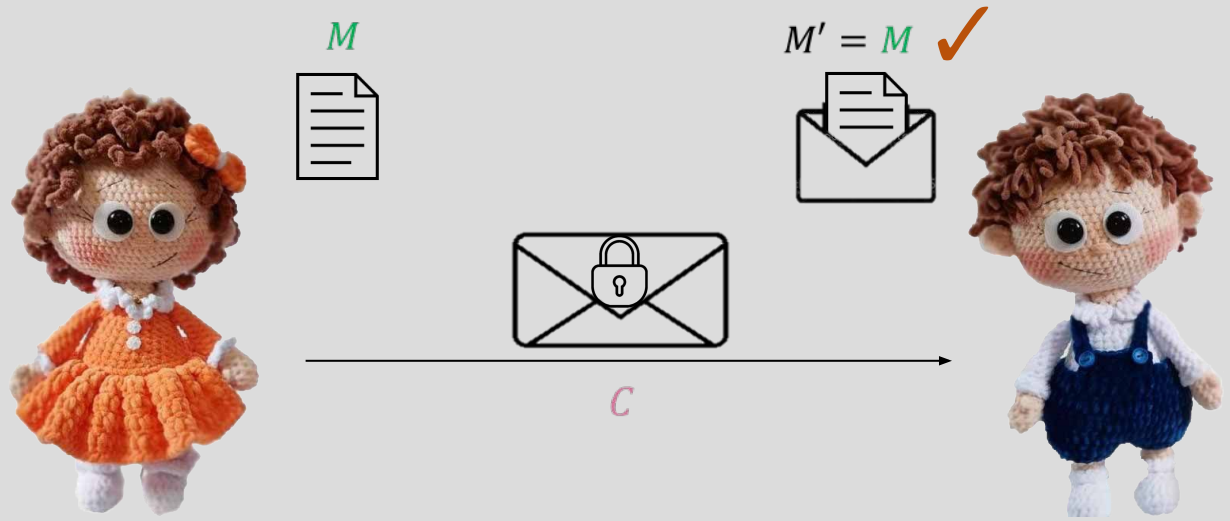
1) فضای پیام اصلی (Plaintext): $\mathcal{P}$
2) فضای متن رمز شده (Ciphertext): $\mathcal{C}$
3) فضای کلید (Key): $\mathcal{K}$
4) مجموعه تبدیل‌های رمزگذاری شده (Encryption): $\mathcal{E}$
5) مجموعه تبدیل‌های رمزگشایی (Decryption): $\mathcal{D}$

هدف دوم: احراز اصالت

- آلیس می‌خواهد به باب اثبات کند که آلیس است! و یا پیامی که برای باب ارسال شده است از طرف خود آلیس است.
- وقتی آلیس یک چک را امضا می‌کند، (احتمالا) محرمانگی پیام مهم نیست، بلکه تایید هویت آلیس توسط بانک مهم است.

هدف سوم: جامعیت پیام

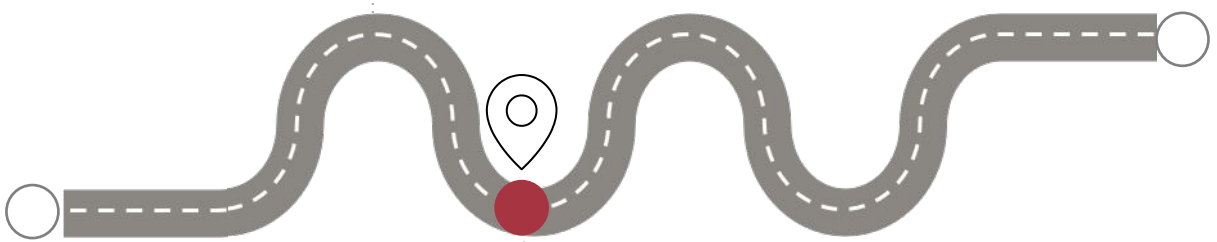
- آلیس می‌خواهد این اطمینان را فراهم کند که پیام دریافتی، دقیقا همان پیامی است که توسط او ارسال شده است.
- وقتی آلیس یک چک را امضا می‌کند، نه تنها تایید هویت آلیس توسط بانک مهم است، بلکه بانک باید مطمئن باشد که پیام تغییر نکرده است.



امنیت اولیه‌های رمزنگاری

- اصل کرشهف (Kerckhoff): مهاجم جزئیات الگوریتم‌های رمزنگاری را می‌داند و در نتیجه، امنیت یک الگوریتم باید تنها مبتنی بر ندانستن کلید باشد.
- این اصل برای کاربردهای تجاری (که موضوع درس ما است) صادق است.
  - برای داشتن سیستم‌های یکپارچه، عموما از الگوریتم‌های استاندارد استفاده می‌شود.
- در مواردی هم که الگوریتم از ابتدا مشخص نبوده است، پس از مدتی با روش‌های مهندسی معکوس و یا طرق دیگر مشخص شده است.

آشنایی با علم
رمزنگاری



اطلاعات
کلی درس

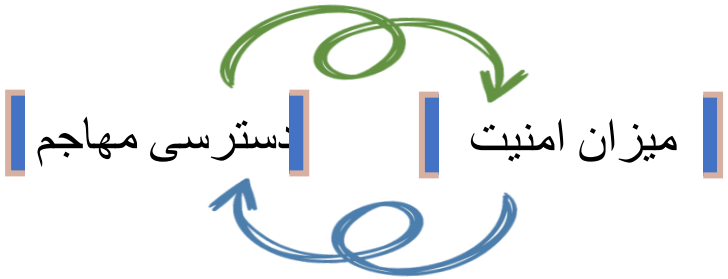
**آشنایی با
حملات و
مقایسه‌ی آن‌ها**

دسته‌بندی حملات از منظر دسترسی مهاجم

مدل جعبه‌سیاه	مدل جعبه‌خاکستری	مدل جعبه‌سفید
مهاجم به مجموعه‌ای از متون اصلی و معادل رمزشده‌ی آن‌ها دسترسی دارد.	مهاجم به ابزاری که رمزنگاری را انجام می‌دهد دسترسی (بعضا فیزیکی) دارد	مهاجم درون سیستم است و به مقادیر میانی و ... دسترسی دارد!



- ممکن است الگوریتمی در مدل جعبه‌سیاه امن باشد اما در مدل‌های جعبه‌خاکستری یا سفید امن نباشد!



اهداف تحلیل‌های مدل جعبه سیاه (خروجی حمله)

- **بازیابی کلید (Key Recovery):**
  حملاتی که منجر به پیدا کردن کلید می‌شوند.
- **استنتاج کلی (Global Deduction):**
  بدون به دست آوردن کلید بتوانیم رابطه‌ای ارائه دهیم که با استفاده از آن بتوان با داشتن متن رمزشده، متن اصلی معادل را پیدا کرد.
- **استنتاج نمونه‌ای (Instance Deduction):**
  مهاجم بدون به دست آوردن کلید بتواند رابطه‌ای ارائه دهد که با داشتن بخشی از متن رمزشده، بخشی از متن اصلی معادل پیدا شود.
- **تمایزگر (Distinguisher):**
  حملاتی که منجر به پیدا کردن کلید نمی‌شوند اما یک ویژگی غیر تصادفی را معرفی می‌کنند که با استفاده از آن و با پیچیدگی کمتر از پیچیدگی جست‌وجوی کامل، می‌توان الگوریتم رمز را از یک جایگشت تصادفی ایده‌آل تشخیص داد.

مقایسه‌ی حملات با یکدیگر

- دو دیدگاه متداولی که برای مقایسه‌ی حملات مختلف وجود دارد:
  1. از نظر نوع داده‌ای که مهاجم برای حمله در اختیار دارد
  2. از نظر میزان موفقیت هر حمله

سناریو های مختلف حمله

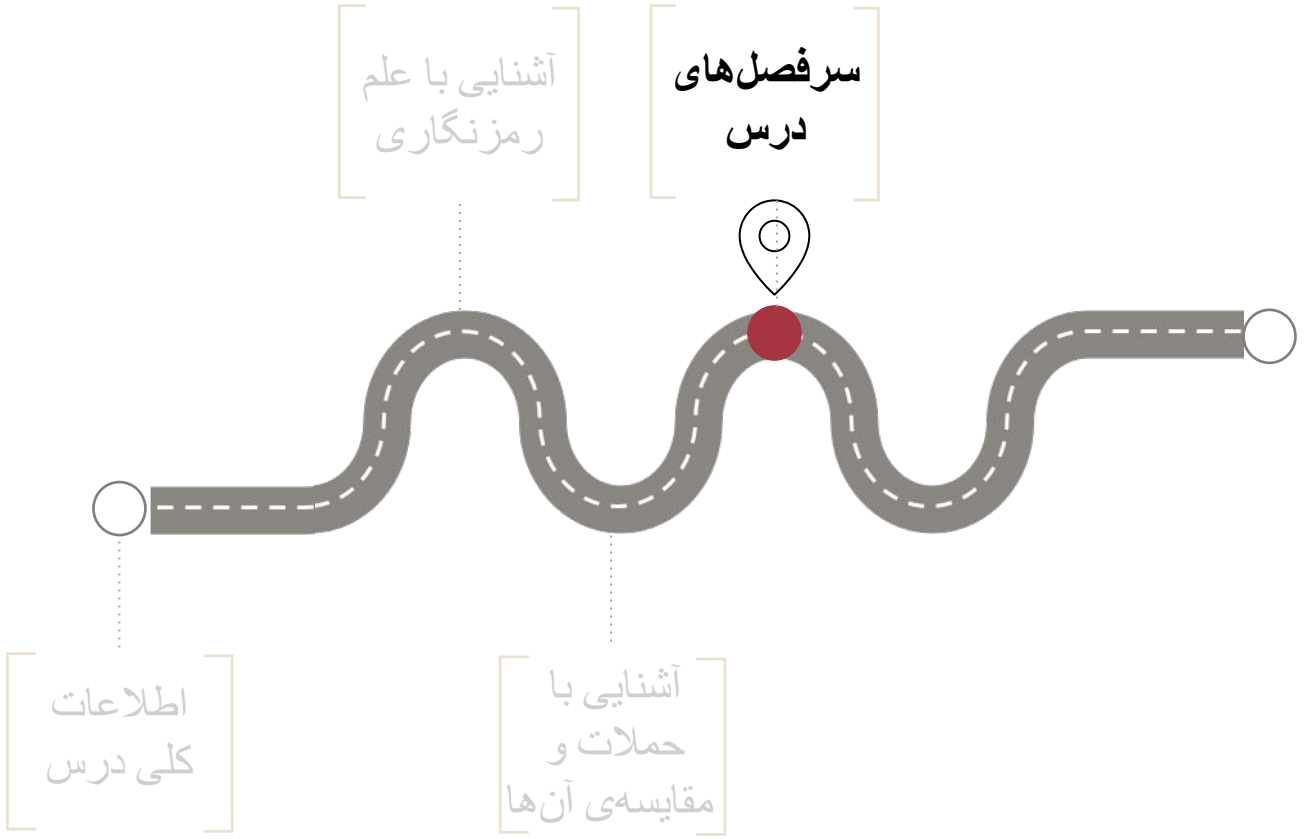
معیار های سنجش موفقیت؟

سناریوهای مختلف حمله به الگوریتم های رمزنگاری

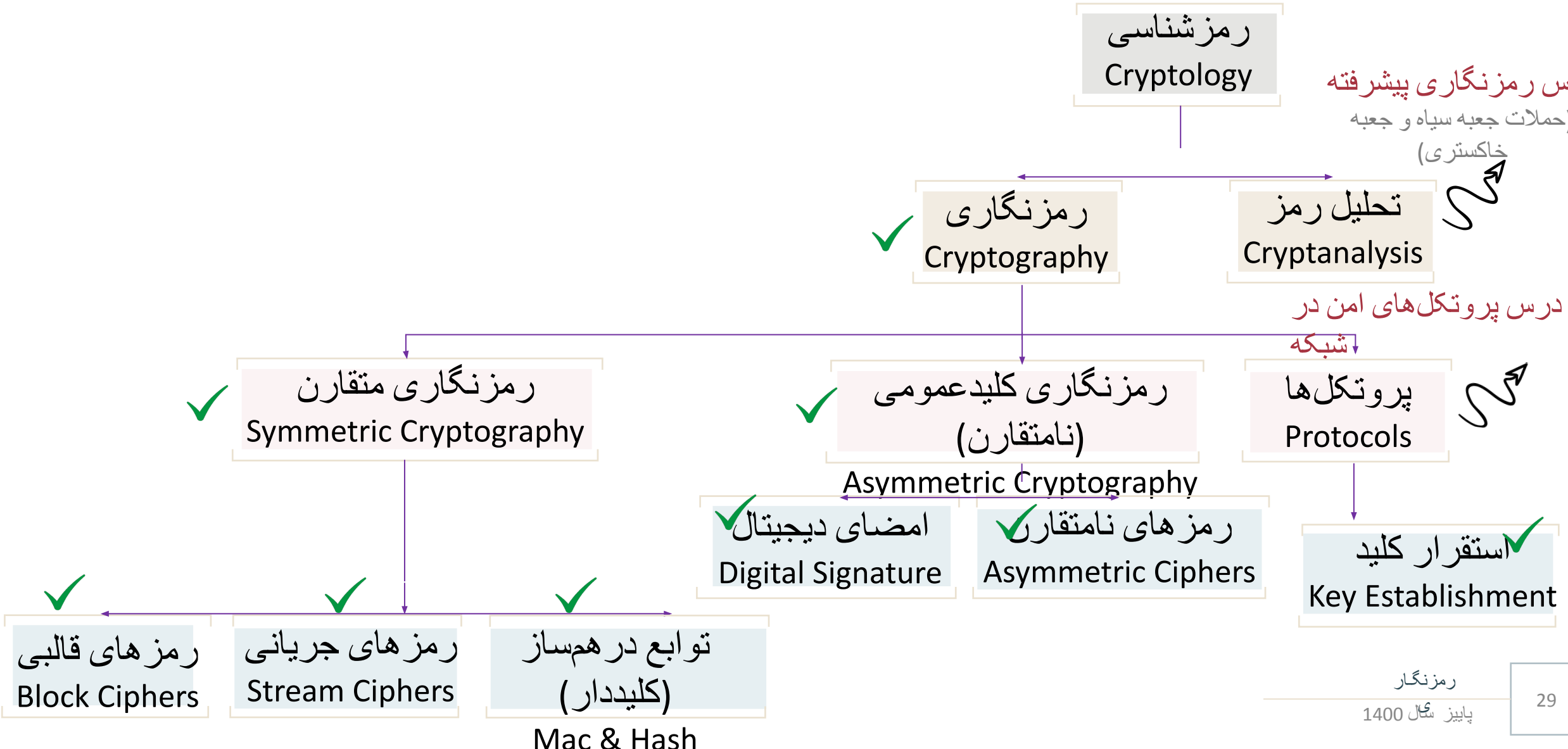
1. **حمله‌ی متن رمز تنها (Ciphertext-Only Attack):**
   - تحلیلگر تنها متن رمزشده را در اختیار دارد.
2. **حمله‌ی متن اصلي معلوم (Known-Plaintext Attack):**
   - تعدادي متن رمزشده و متن اصلي معادل آنها در اختیار تحلیلگر است، اما در انتخاب آن‌ها اختیاري براي تحلیلگر وجود ندارد.
3. **حمله‌ی متن اصلي منتخب (Chosen-Plaintext Attack):**
   - متن رمزشده‌ی متناظر با هر متن اصلي دلخواهی براي تحلیلگر دردسترس است. به عنوان مثال، یک دستگاه رمزکننده با کلیدی نامعلوم در اختیار تحلیلگر است و هدف به دست آوردن کلید است.
4. **حمله‌ی متن رمزشده منتخب (Chosen-Ciphertext Attack):**
   - تحلیلگر قادر است متن اصلي متناظر با هر متن رمزشده‌ی دلخواهی را به دست آورد.
   - به عنوان مثال، یک دستگاه رمزگشایي با کلیدی نامعلومي در اختیار تحلیلگر است و هدف به دست آوردن کلید است.
5. **حمله‌ی متن اصلی منتخب وفقی (Adaptive Chosen-Plaintext Attack):**
   - مهاجم در زمان اجرای حمله درخواست می کند که متن اصلی معادل برخی متون را در اختیار او قرار دهند.

معیارهای سنجش موفقیت حملات مختلف

1. **نوع داده‌ی مورد نیاز:** هرقدر مفروضات یک حمله ضعیف‌تر باشند، در کاربردهای بیشتری امکان اجرا دارد!
2. **پیچیدگي داده (Data Complexity):** تعداد متن اصلي یا متن رمزشده‌ی مورد نیاز براي اجراي یک حمله.
3. **پیچیدگي حافظه (Memory Complexity):** میزان حافظه‌ی مورد نیاز براي نگهداري داده در طول یک حمله.
4. **پیچیدگي زماني (Time Complexity):** مدت زمان لازم براي اجراي یک حمله؛ که معمولاً از طریق شمارش تعداد عملیات‌های رمزنگاري و رمزگشایي الگوریتم مورد نظر براي اجراي حمله صورت میگیرد.
5. **احتمال موفقیت (Success Rate):** احتمال موفقیت یک حمله از نظر آماری.
   - اکثر حملات انجام شده به سیستمهاي رمز حملات احتمالاتي هستند. به همین دلیل، احتمال اجراي موفق یک حمله از معیارهاي مهم اندازهگیري کارآیي و میزان عملي بودن یک حمله است.


سرفصل‌های درس
آشنایی با علم رمزنگاری
اطلاعات کلی درس
آشنایی با حملات و مقایسه‌ی آن‌ها

طبقه‌بندی اجمالی علم رمزشناسی (Cryptology)



معرفی سرفصل‌های درس

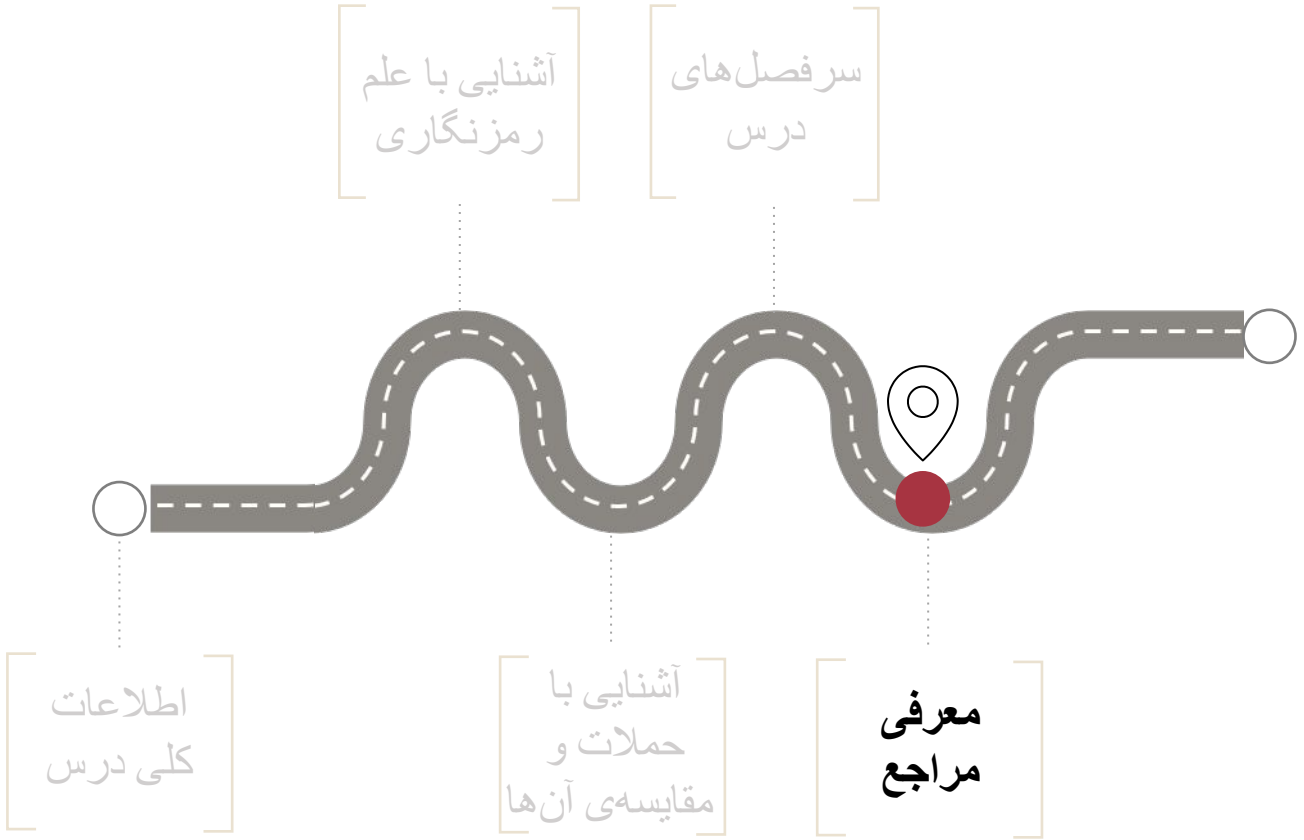
مباحث میان‌ترم (تقریبی)

- مقدمات و تعاریف اولیه (درس صفرم (همین درس))
- مبانی ریاضیات رمزنگاری: گروه، حلقه، میدان و انجام عملیات در آنها (درس یکم)
- نظریه‌ی اطلاعات (در حد آشنایی) و مقاله‌ی شانون (درس دوم)
- آشنایی اجمالی با سیستم‌های کلاسیک رمزنگاری (درس سوم)
- آشنایی با رمزهای جریانی (درس چهارم)
- آشنایی با رمزهای قالبی (درس پنجم)
- آشنایی با الگوریتم‌های AES، DES و مدهای رمزنگاری (درس‌های ششم، هفتم و هشتم)

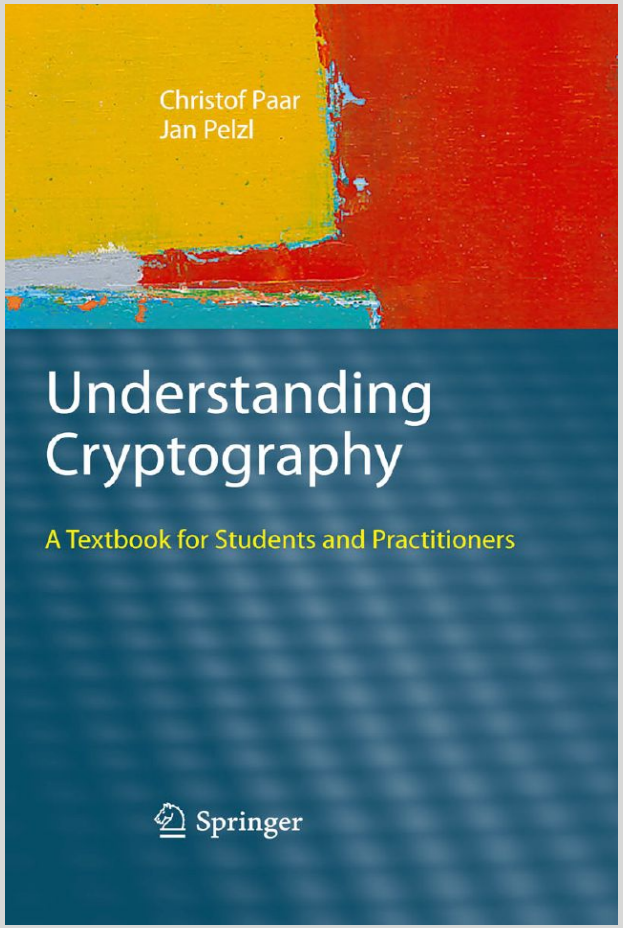
معرفی سرفصل‌های درس

مباحث پایان‌ترم (تقریبی)

- مقدمه‌ای بر سیستم‌های رمزنگاری کلید عمومی (درس نهم)
- رمزنگاری کلید عمومی مبتنی بر سختی تجزیه‌ی عدد (درس دهم)
- رمزنگاری کلید عمومی مبتنی بر لگاریتم گسسته (درس یازدهم)
- رمزنگاری کلید عمومی مبتنی بر لگاریتم گسسته روی خم‌های بیضوی (درس دوازدهم)
- امضای دیجیتال (درس سیزدهم)
- آشنایی با توابع درهم‌ساز و MAC (درس چهاردهم و پانزدهم)
- استقرار کلید (درس شانزدهم)


آشنایی با علم رمزنگاری
سرفصل‌های درس
اطلاعات کلی درس
آشنایی با حملات و مقایسه‌ی آن‌ها
معرفی مراجع

مرجع اصلی درس

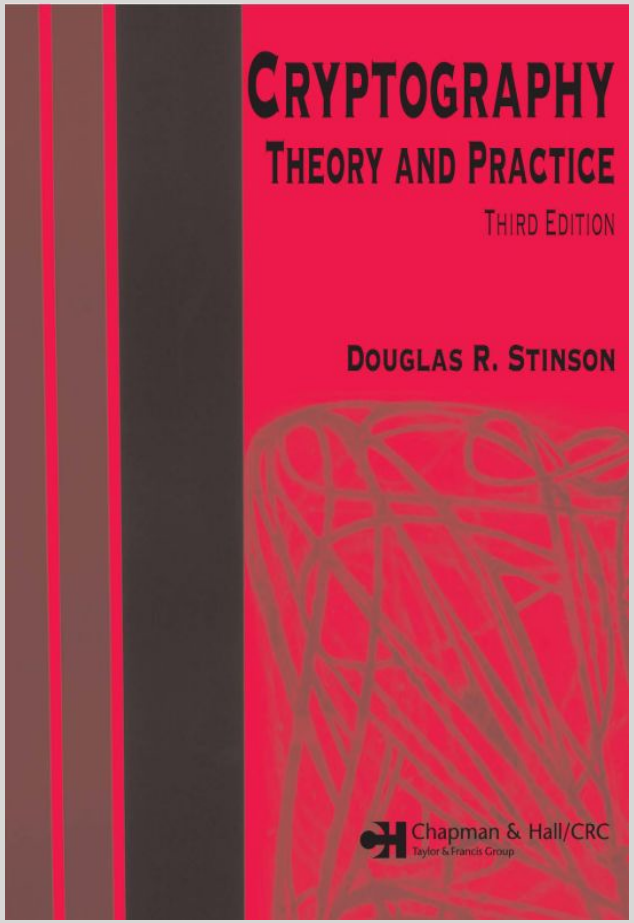


Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

- خواندن این کتاب **به‌طور جدی** توصیه می‌شود!
  (می‌توانید از کتابخانه‌ی پژوهشکده امانت بگیرید و یا از نسخه‌ی الکترونیکی استفاده کنید.)
- کانال یوتوب برای دانشجویان علاقه‌مند:

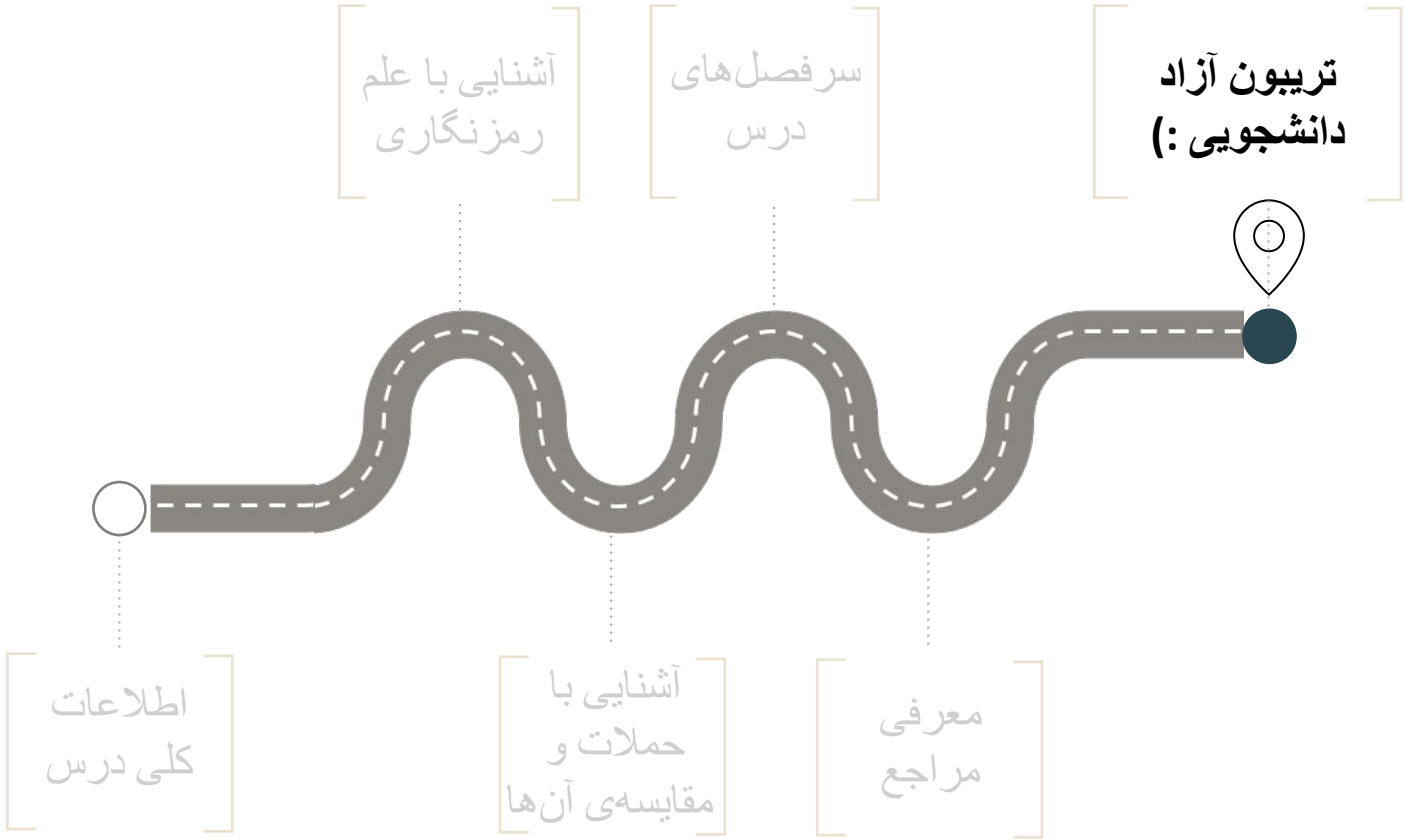
https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg

مرجع تکمیلی



Stinson, D. R. (2005). Cryptography: theory and practice. Chapman and Hall/CRC.

- در صورت علاقه به موضوعی خاص، می‌توانید با بنده برای معرفی مراجع تکمیلی تماس بگیرید.


تریبون آزاد
دانشجویی :)
سرفصل‌های درس
آشنایی با علم رمزنگاری
اطلاعات کلی درس
آشنایی با حملات و مقایسه‌ی آن‌ها
معرفی مراجع

نوبت شماست!

- خودتان را معرفی کنید.
- از رشته مخابرات امن و رمزنگاری چه می‌دانید؟
- از این درس چه انتظاری دارید؟