



Shahid Beheshti  
University

# رمزنگاری پیشرفته

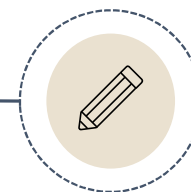
هادی سلیمانی

پژوهشکده فضای مجازی دانشگاه شهید بهشتی

- 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/advanced-cryptography-course/](http://facultymembers.sbu.ac.ir/h_soleimany/advanced-cryptography-course/)

درس صفرم



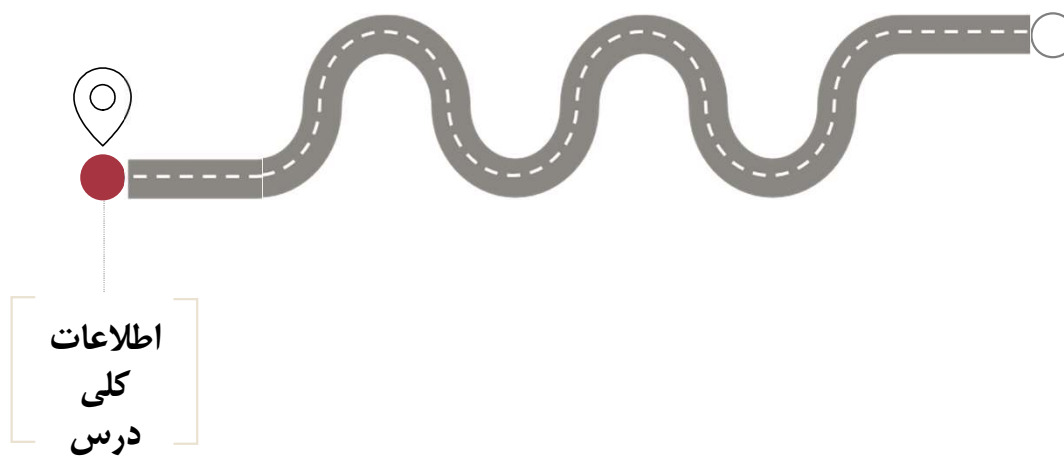
## مقدمه‌ای بر درس رمزنگاری پیشرفته

## ■ فهرست عناوین درس

### مقدمه‌ای بر درس رمزنگاری پیشرفته

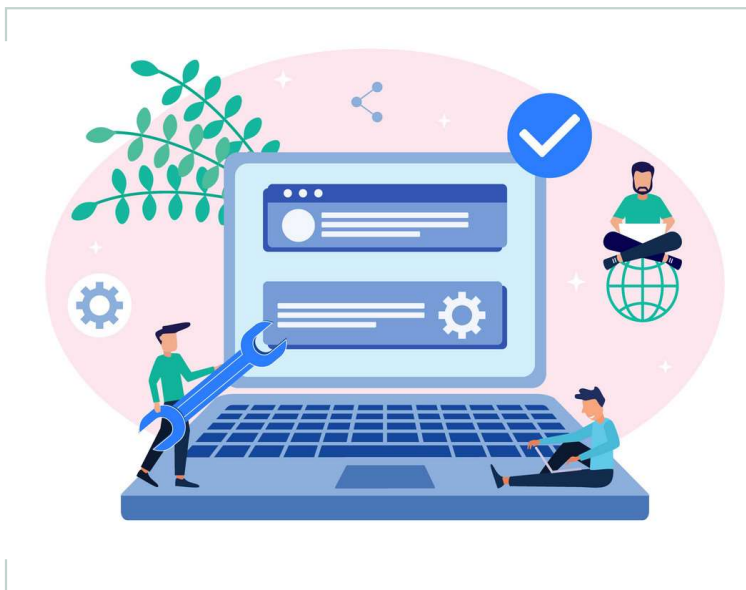
- اطلاعات کلی درس
- آشنایی با مدل‌های امنیتی
- مقایسه‌ی حملات با یکدیگر
- اهداف و سرفصل‌های درس
- معرفی مراجع
- تریبون آزاد دانشجویی (:





## ■ پیش نیازهای درس

1. آشنایی با مفاهیم ابتدایی رمزنگاری
  - گذراندن درس اصول رمزنگاری.
2. آشنایی مقدماتی با برنامه نویسی!



## ■ شیوه‌ی ارزیابی (تقریبی)

1. کار عملی (۳ پروژه برای درس در نظر گرفته شده است): ۶ نمره
  2. میان‌ترم (شامل تحلیل‌های مدل جعبه سیاه): ۶ نمره و به‌صورت حذفی
  3. پایان‌ترم (شامل حملات مدل جعبه خاکستری): ۸ نمره
- زمان: براساس اعلام دانشگاه (سیستم گلستان)



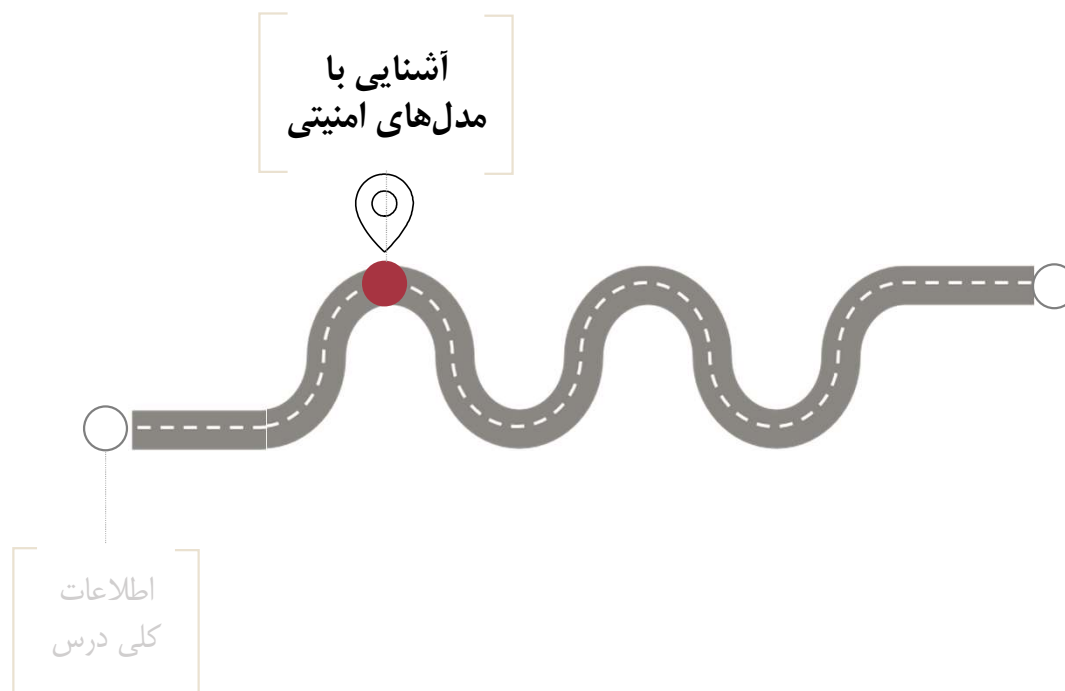
## ■ ساعت‌های مراجعه‌ی دانشجویان

• از طریق هماهنگی قبلی:




hadi.soleimany@gmail.com







## ■ دسته‌بندی حملات از منظر دسترسی مهاجم

مدل جعبه سفید	مدل جعبه خاکستری	مدل جعبه سیاه
مهاجم درون سیستم است و به مقادیر میانی و ... دسترسی دارد!	مهاجم به ابزاری که رمزنگاری را انجام می‌دهد دسترسی (بعضا فیزیکی) دارد.	مهاجم به مجموعه‌ای از <b>متون اصلی</b> و <b>معادل رمزشده‌ی</b> آن‌ها دسترسی دارد.
		

- ممکن است الگوریتمی در مدل جعبه سیاه امن باشد اما در مدل‌های جعبه خاکستری یا سفید امن نباشد!



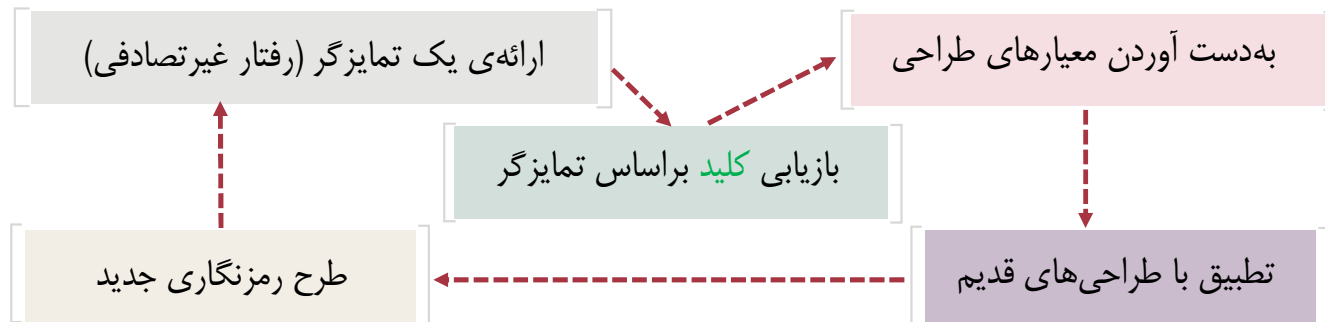
تمرکز ما در این درس بر روی حملات مدل‌های جعبه سیاه و جعبه خاکستری است.

## ■ اهداف تحلیل‌های مدل جعبه سیاه

- بازیابی کلید (Key Recovery):
  - حملاتی که منجر به پیدا کردن کلید می‌شوند.
- استنتاج کلی (Global Deduction):
  - بدون به دست آوردن کلید، رابطه‌ای ارائه می‌شود که می‌توان به کمک آن با داشتن متن رمز شده، متن اصلی معادل را پیدا کرد.
- استنتاج نمونه‌ای (Instance Deduction):
  - بدون به دست آوردن کلید، رابطه‌ای ارائه می‌شود که می‌توان به کمک آن با داشتن بخشی از متن رمز شده، بخشی از متن اصلی معادل را پیدا کرد.
- تمایزگر (Distinguisher):
  - حملاتی که به پیدا کردن کلید منجر نمی‌شوند، اما یک ویژگی غیرتصادفی 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.

## ■ تحلیل‌های مدل جعبه‌سیاه: تحلیل‌های آماری - ساختاری

- تحلیل‌های مدل جعبه‌سیاه معمولاً از مشخصات آماری و یا ساختاری الگوریتم‌های رمزنگاری استفاده می‌کنند.
- روند ارائه‌ی این حملات معمولاً بدین گونه است:
- ابتدا تلاش می‌شود برای الگوریتم‌های رمزنگاری هدف، یک تمایزگر ارائه شود که براساس آن، بتوان الگوریتم را از جایگشت ایده‌آل (Random Permutation) تشخیص داد.
- سپس تلاش می‌شود که براساس مشخصه‌ی غیرتصادفی، اطلاعاتی درباره‌ی **کلید** به دست آید.
- براساس همان مشخصه‌ی غیرتصادفی، راه‌کارهایی نیز به منظور جلوگیری از حملات ارائه می‌شود.
- الگوریتم‌های جدید براساس معیارهای کشف‌شده به‌روزرسانی و بازطراحی می‌شوند.
- بنابراین، الگوریتم‌ها معمولاً در مقابل حملات شناخته‌شده امن هستند، اما نمی‌توان ادعا کرد که در مقابل تمامی مهاجم‌ها امنیت قابل اثبات دارند!



## ■ طبقه‌بندی حملات جعبه‌خاکستری

### • منظر ۱:

- **حملات فعال (Active):** مهاجم با تغییر عواملی نظیر دما، کلاک، ولتاژ، تابش لیزر و ...، شرایط کاری سیستم را تغییر می‌دهد.

- **حملات غیرفعال (Passive):** مهاجم صرفاً از اطلاعات نشت یافته توسط سیستم استفاده می‌کند.

### • منظر ۲:

- **حملات تهاجمی (Invasive):**

- مهاجم به اجزای داخلی سیستم دسترسی دارد؛ مثلاً از طریق لایه‌برداری یا ایجاد حفره در لایه‌ی محافظ!
- پیچیده، هزینه‌ی بالا و زمان‌بر.

- **حملات نیمه‌تهاجمی (Semi-invasive):**

- مهاجم بدون آسیب رساندن به اجزای داخلی سیستم دسترسی دارد.

- **حملات غیرتهاجمی (Non-invasive):**

- مهاجم به ابزار دسترسی دارد ولی تنها رفتار کلی سیستم را (از نزدیک) بررسی می‌کند.
- مزایا: حضور مهاجم را کسی متوجه نمی‌شود! ارزان و قابل تکرار هستند.

## ■ طبقه‌بندی حملات جعبه‌خاکستری

... ادامه

گران‌تر و موثرتر

	فعال	غیرفعال
تهاجمی	Permanent Faults	Probing
نیمه تهاجمی	Radiation Attack	Optical Inspection
غیرتهاجمی	Fault Attacks	Side-channel Attacks

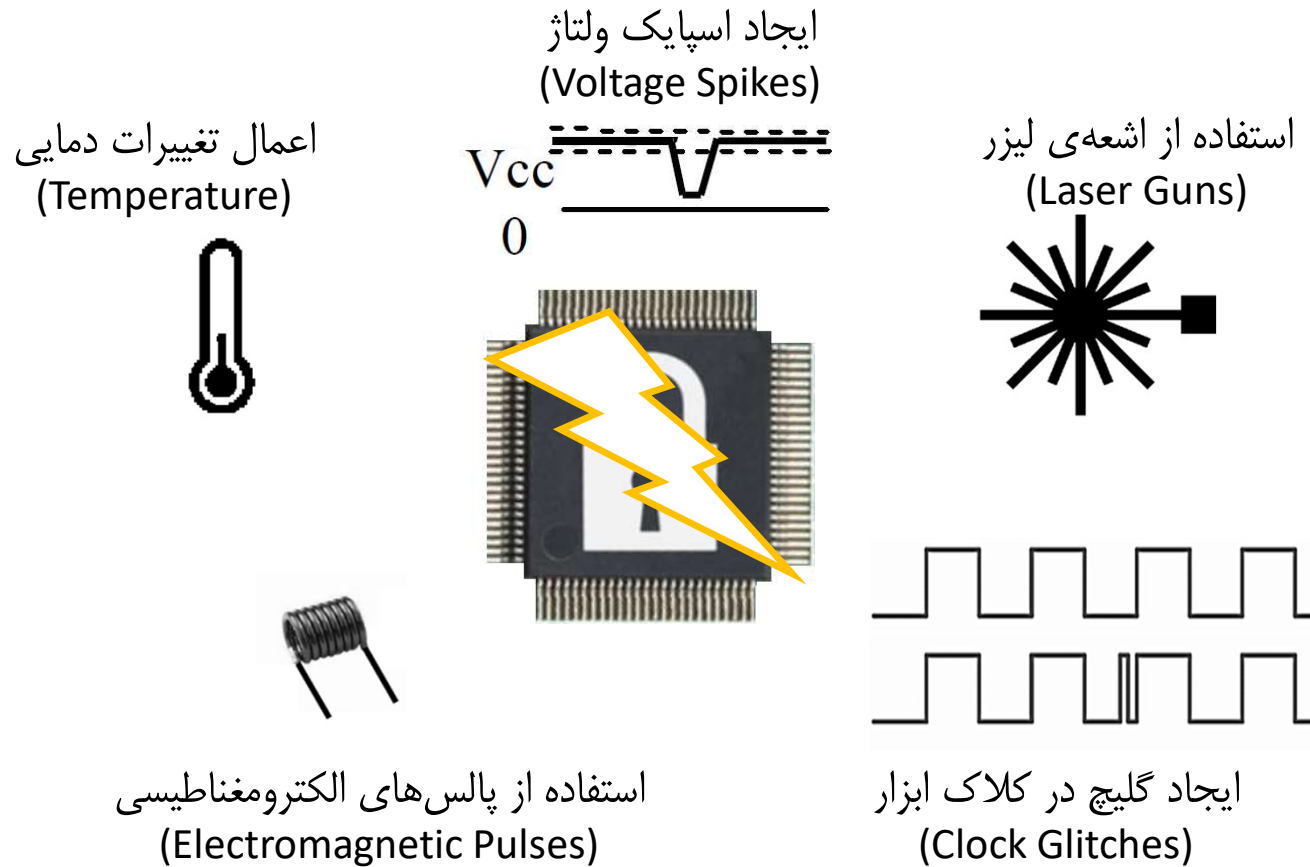
ارزان‌تر، قابلیت اجرا در کاربردهای بیشتر

تفاوت تعریف در برخی از متون دیده می‌شود:

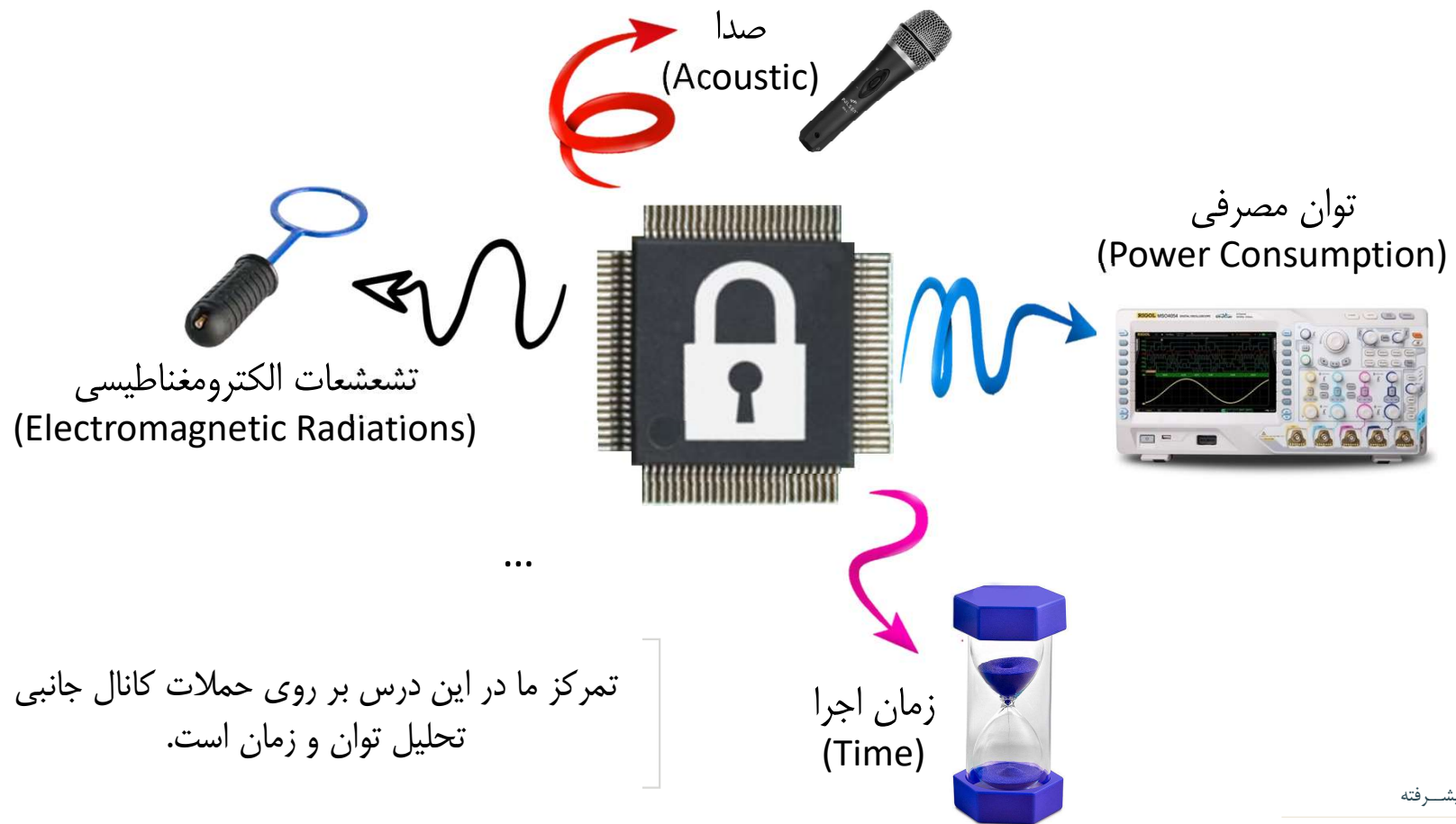
- در مواردی، حملات فعال را به صورت کلی حملات القاء خطا نام‌گذاری می‌کنند (فلسفه: حملات فعال معمولاً منجر به اعمال خطا می‌شوند).

تمرکز ما در این درس بر روی حملات غیرتهاجمی است.

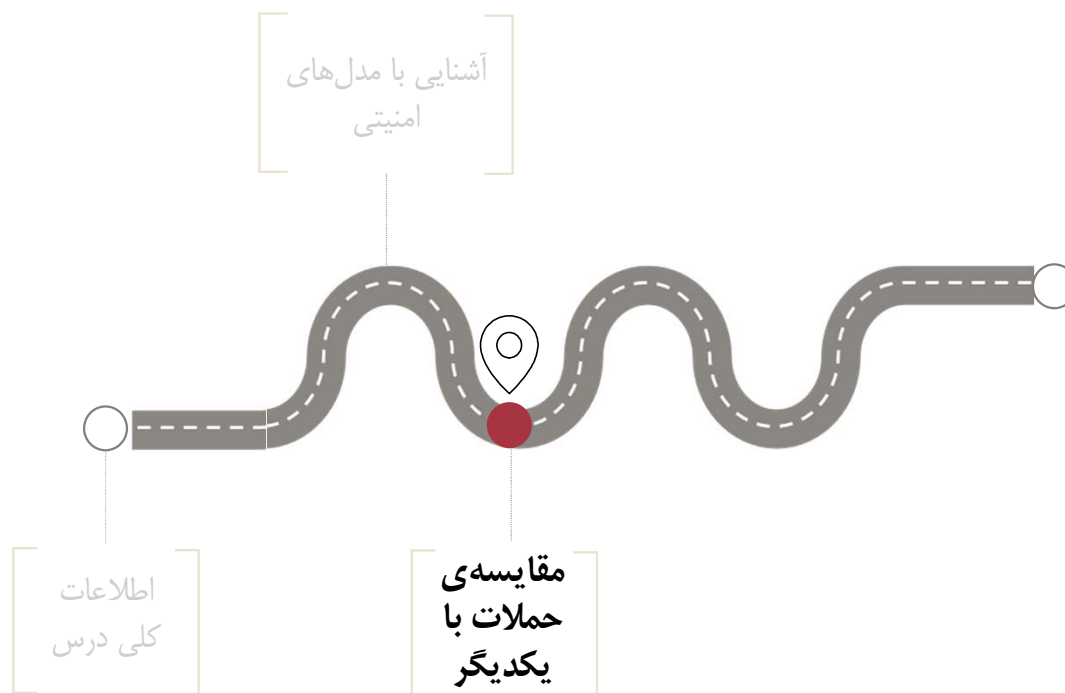
## ■ برخی از انواع مهم روش‌های القاء خطا



## ■ برخی از انواع مهم کانال‌های جانبی







## ■ 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
- سناریوهای مختلف حمله
- معیارهای سنجش موفقیت؟

## ■ سناریوهای مختلف حمله به الگوریتم های رمزنگاری

### 1. حمله ی متن رمز تنها (Ciphertext-only Attack):

- تحلیل گر تنها متن رمز شده را در اختیار دارد.

### 2. حمله ی متن اصلی معلوم (Known-plaintext Attack):

- تعدادی متن رمز شده و متن اصلی معادل آن ها در اختیار تحلیل گر است، اما در انتخاب آن ها اختیاری برای تحلیل گر وجود ندارد.

### 3. حمله ی متن اصلی منتخب (Chosen-plaintext Attack):

- متن رمز شده ی متناظر با هر متن اصلی دلخواهی برای تحلیل گر در دسترس است. به عنوان مثال، یک دستگاه رمز کننده با کلیدی نامعلوم در اختیار تحلیل گر است و هدف به دست آوردن کلید است.

### 4. حمله ی متن رمز شده منتخب (Chosen-ciphertext Attack):

- تحلیل گر قادر است متن اصلی متناظر با هر متن رمز شده ی دلخواهی را به دست آورد.
- به عنوان مثال، یک دستگاه رمز گشایی با کلیدی نامعلومی در اختیار تحلیل گر است و هدف به دست آوردن کلید است.

### 5. حمله ی متن اصلی منتخب و فقی (Adaptive Chosen-plaintext Attack):

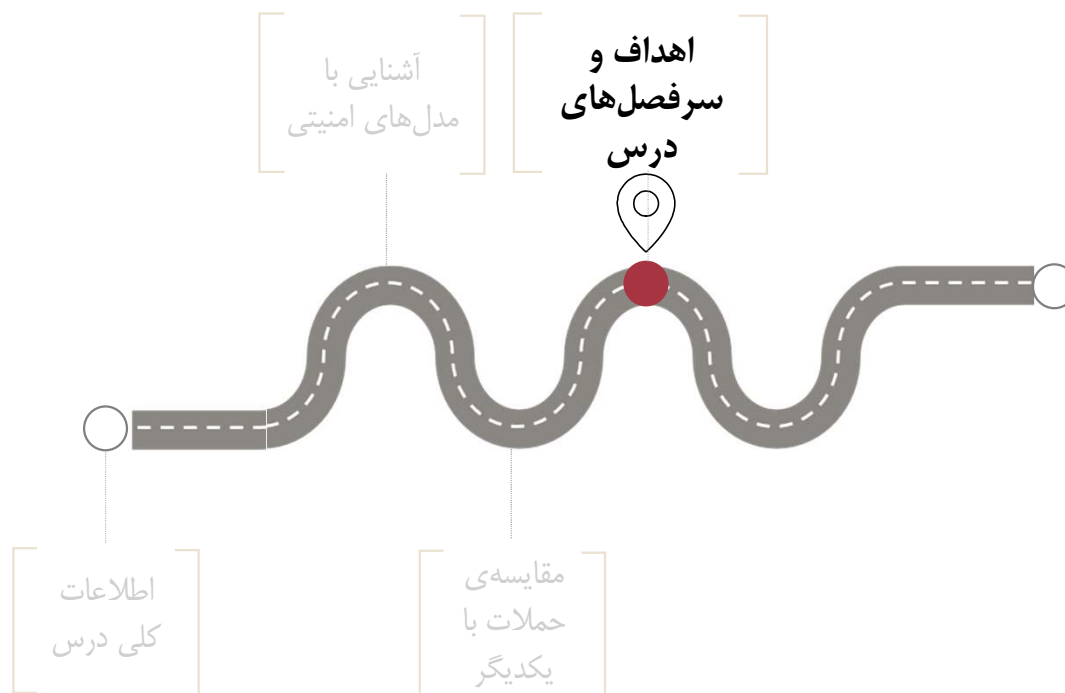
- مهاجم در زمان اجرای حمله درخواست می کند که معادل متن اصلی برخی متون را در اختیار او قرار دهند.

رمزنگاری پیشرفته

پاییز سال ۱۴۰۰

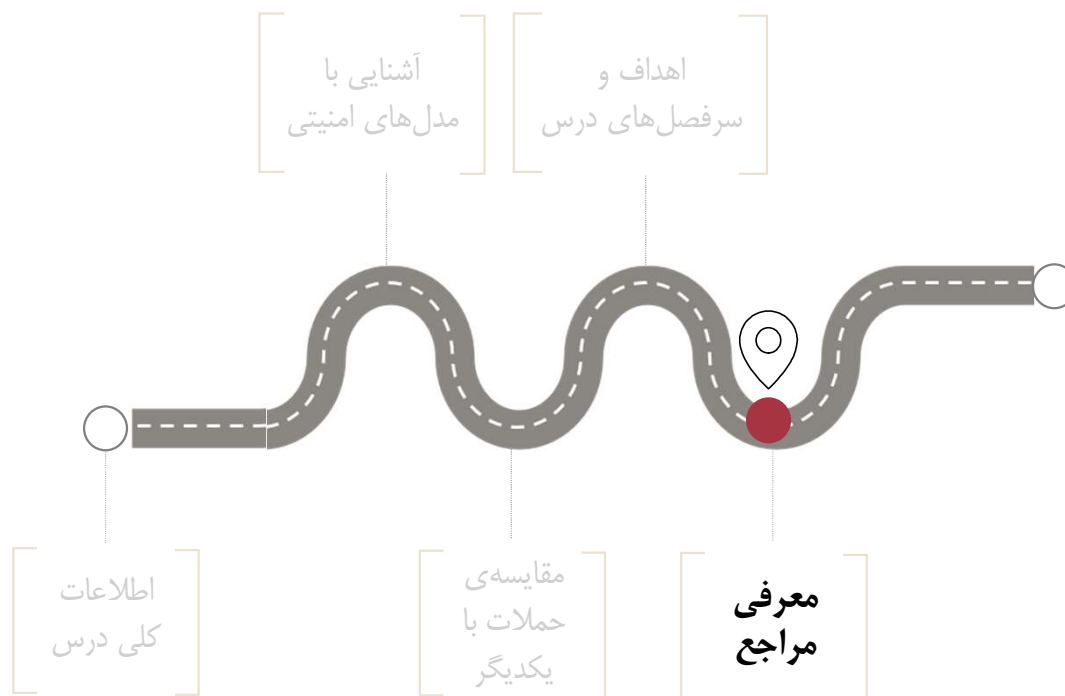
## ■ معیارهای سنجش موفقیت حملات مختلف

1. **نوع داده‌ی مورد نیاز:** هر قدر مفروضات یک حمله ضعیف‌تر باشند، در کاربردهای بیشتری امکان اجرا دارد!
  2. **پیچیدگی داده (data complexity):** تعداد **متن اصلی** یا **متن رمز شده‌ی** مورد نیاز برای اجرای یک حمله.
  3. **پیچیدگی حافظه (memory complexity):** میزان حافظه‌ی مورد نیاز برای نگهداری داده در طول یک حمله.
  4. **پیچیدگی زمانی (time complexity):** مدت زمان لازم برای اجرای یک حمله؛ که معمولاً از طریق شمارش تعداد عملیات‌های رمزنگاری و رمزگشایی الگوریتم مورد نظر برای اجرای حمله صورت می‌گیرد.
  5. **احتمال موفقیت (success rate):** احتمال موفقیت یک حمله از نظر آماری.
- اکثر حملات انجام شده به سیستم‌های رمز حملات احتمالاتی هستند. به همین دلیل، احتمال اجرای موفق یک حمله از معیارهای مهم اندازه‌گیری کارایی و میزان عملی بودن یک حمله است.



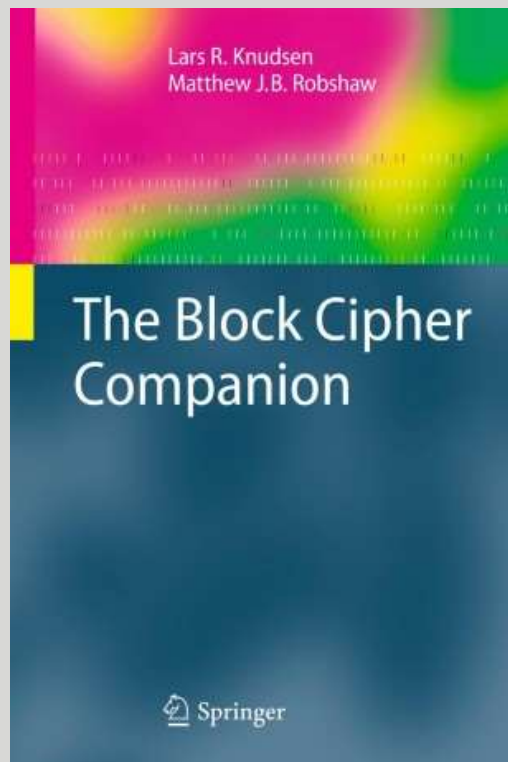
## ■ اهداف و سرفصل‌های درس

- هدف ما بررسی تحلیل‌ها و حملاتی است که نقشی پایه‌ای و مهم در فهم و اجرای سایر تحلیل‌ها و حملات دارند.
- **سرفصل‌های درس در مدل امنیتی جعبه‌سیاه:**
  - تحلیل تفاضلی به رمزهای قالبی (درس ۱).
  - تحلیل خطی به رمزهای قالبی (درس ۲).
  - تحلیل همبستگی (سریع) به رمزهای جریانی (درس ۳).
- **سرفصل‌های درس در مدل امنیتی جعبه‌خاکستری:**
  - حملات القاء خطا (درس ۴).
  - حملات کانال جانبی:
  - حملات تحلیل توان (درس‌های ۵، ۶، ۷ و ۸).
  - حملات زمانی یا ریزمعماری (درس ۹).



## ■ معرفی مراجع (اصلی) درس

### بخش حملات جعبه سیاه



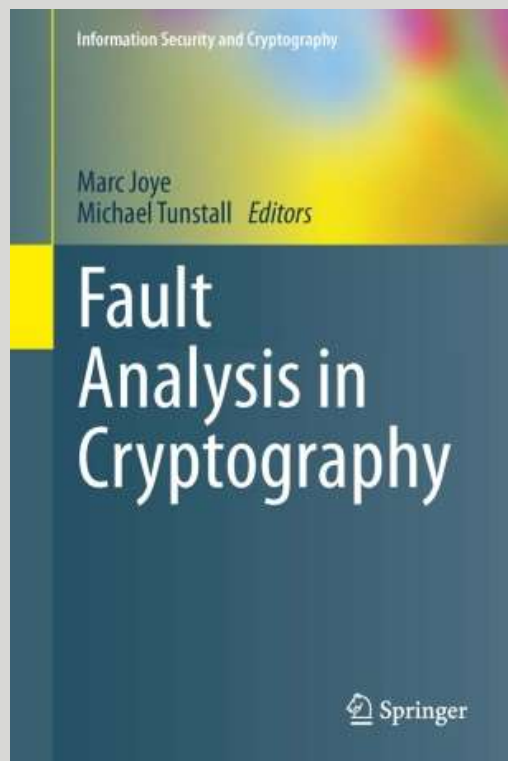
1. Knudsen, L. R., & Robshaw, M. (2011). The block cipher companion. Springer Science & Business Media.
2. Heys, H. M. (2002). A tutorial on linear and differential cryptanalysis. Cryptologia, 26(3), 189-221.
3. T. Siegenthaler. "Decrypting a class of stream ciphers using ciphertext only". IEEE Trans. Comput., 34:81–85, 1985.
4. W. Meier and O. Staffelbach, "Fast Correlation Attacks on Certain Stream Ciphers". J. Cryptology, vol 1, number 3, pages 159-176, 1989.

فصل‌های ششم و هفتم به ترتیب برای تحلیل تفاضلی و تحلیل خطی



## ■ معرفی مراجع (اصلی) درس

### بخش حملات جعبه خاکستری – حملات القاء خطا

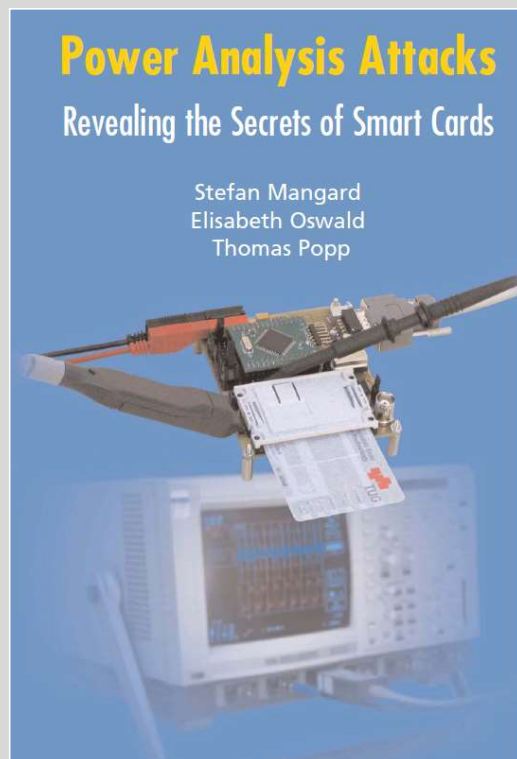


Joye, M., & Tunstall, M. (Eds.). (2012). Fault analysis in cryptography (Vol. 147). Heidelberg: Springer.

- تمرکز ما در بخش حملات القاء خطا بر روی رمزهای متقارن است.
- فصل‌های دوم تا ششم این کتاب (با فرض فهم مباحث ارائه شده در بخش تحلیل تفاضلی).

## ■ معرفی مراجع (اصلی) درس

### بخش حملات جعبه خاکستری – حملات تحلیل توان

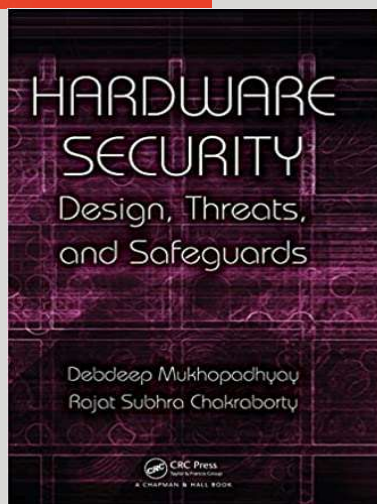
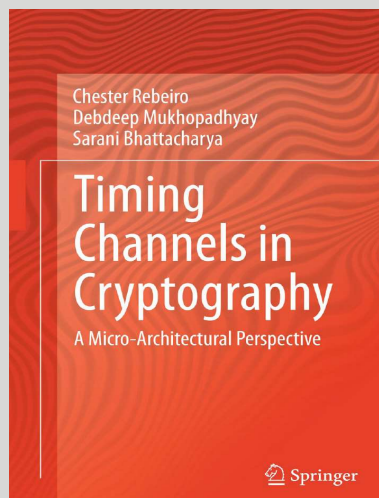


Mangard, S., Oswald, E., & Popp, T. (2008). Power analysis attacks: Revealing the secrets of smart cards (Vol. 31). Springer Science & Business Media.

- فصل‌های دوم تا ششم به صورت تقریباً کامل (مفاهیم پایه، تحلیل توان ساده و تحلیل توان تفاضلی).
- مقدمه‌ای کوتاه از فصل‌های هفتم (مخفی‌سازی) و نهم (نقاب‌گذاری).
- خواندن این کتاب به طور جدی توصیه می‌شود!

## ■ معرفی مراجع (اصلی) درس

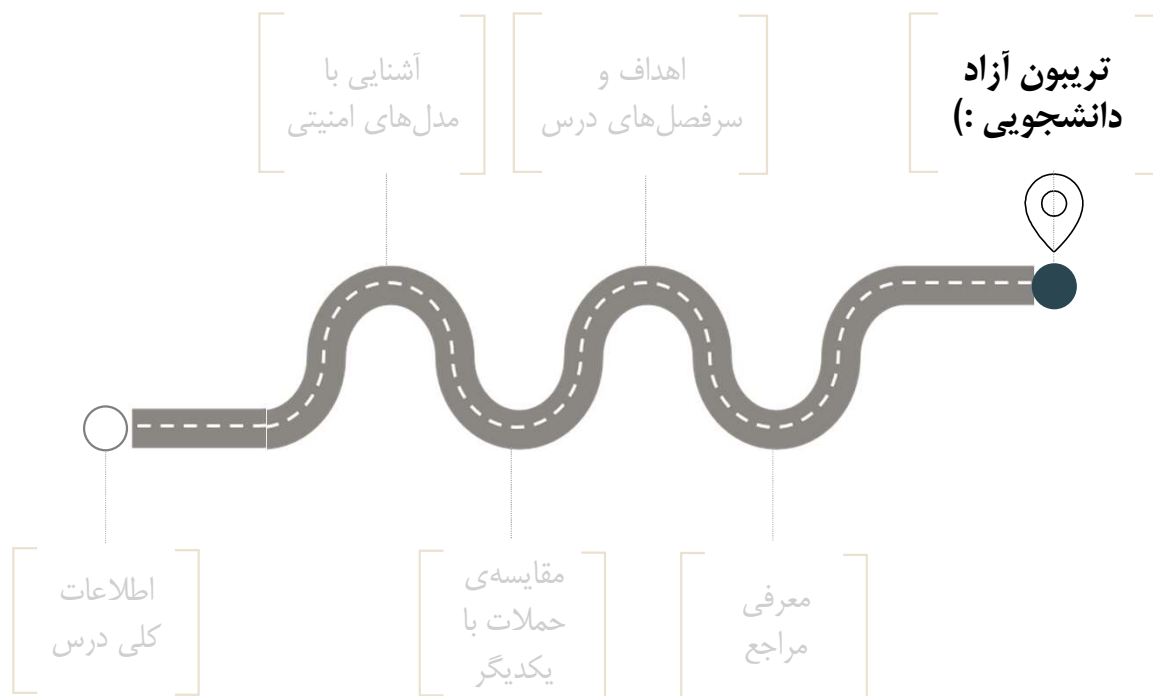
### بخش حملات جعبه خاکستری – حملات زمانی



1. Rebeiro, C., Mukhopadhyay, D., & Bhattacharya, S. (2014). Timing channels in cryptography: a micro-architectural perspective. Springer.
2. Mukhopadhyay, D., & Chakraborty, R. S. (2014). Hardware security: design, threats, and safeguards. CRC Press.

مرجع اول: فصل‌های سوم، چهارم، هفتم و هشتم

مرجع دوم: فصل نهم



## ■ نوبت شماست!

- به چه موضوعاتی در حوزه‌ی رمزنگاری علاقه‌مند هستید؟
- برای موضوع پایان‌نامه تصمیم گرفته‌اید؟
- از این درس چه انتظاراتی دارید؟

