Shahid Beheshti University

رمزنگاری

هادی سلیمانی

پژوهشکده فضای مجازی دانشگاه شهید بهشتی

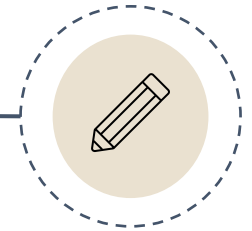
مجوز استفاده و نشر

- 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/

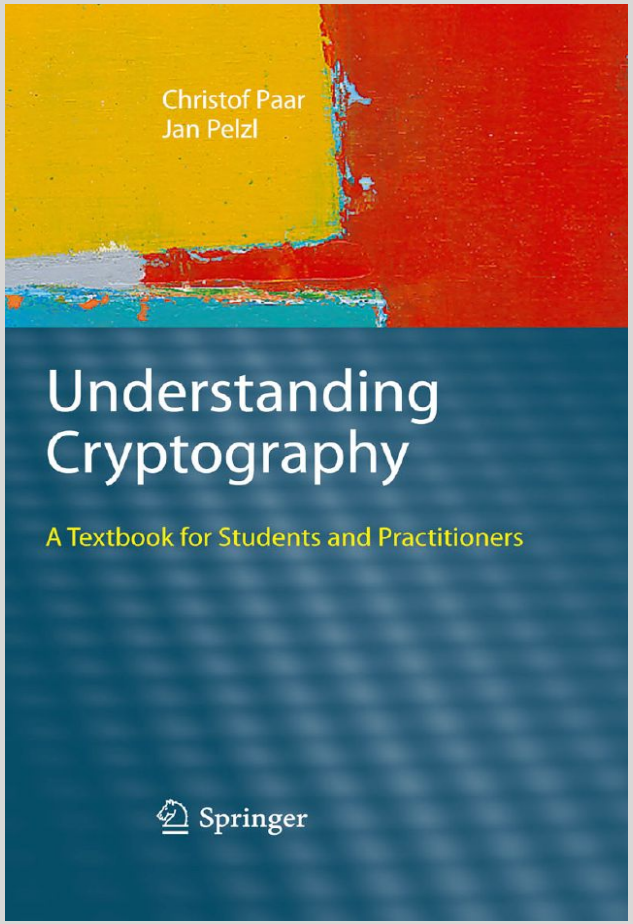
درس پانزدهم



کد احراز اصالت پیام

معرفی مـرجع

کد احراز اصالت پیام



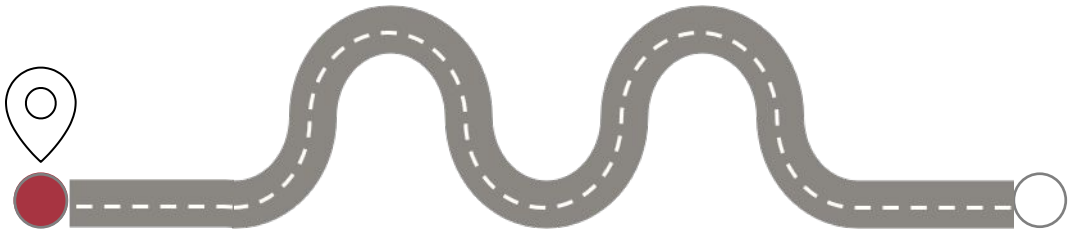
Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

مثال‌ها و تصاویر این بخش از درس از کتاب مرجع است (در غیر این صورت مرجع شکل ذکر شده است).

فهرست عناوین درس

کد احراز اصالت پیام

- مقدمه
- استفاده از تابع چکیده‌ساز برای ساخت MAC
- استفاده از رمز قالبی برای ساخت MAC
- رمزنگاری احراز اصالت شده
- جمع‌بندی مطالب



مقدمه

احراز اصالت پیام در رمزنگاری متقارن

- برای احراز اصالت و جامعیت پیام، می‌توان از امضای دیجیتال استفاده کرد.
- امضاهای دیجیتال مبتنی بر سیستم‌های رمزنگاری کلید عمومی هستند.
- اگر بین فرستنده و گیرنده، کلیدی به اشتراک گذاشته شده باشد، می‌توان از سیستم‌های رمزنگاری متقارن نیز استفاده کرد.
- اما چه لزومی دارد که به جای امضا، برای احراز اصالت و جامعیت پیام از رمزنگاری متقارن استفاده کرد؟
- **پاسخ:** سیستم‌های کلید عمومی به‌مراتب کندتر از رمزهای متقارن هستند.

کد احراز اصالت پیام

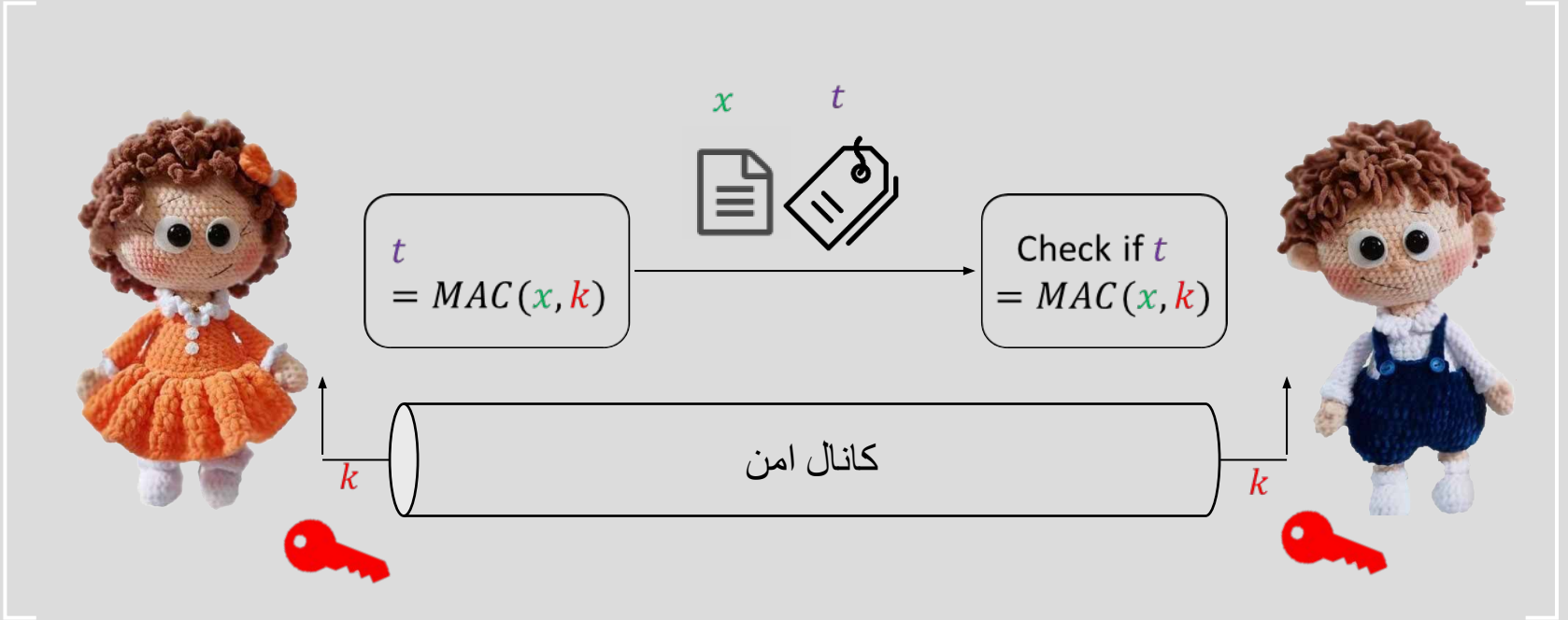
Message Authentication Code (MAC)

- کد احراز اصالت پیام (MAC)، تابعی است که به مقدار کلید (که از قبل به اشتراک گذاشته شده) و مقدار پیام وابسته است.
- ویژگی‌های کد احراز اصالت پیام:

1. متن ورودی آن می‌تواند طول دلخواه داشته باشد.
2. طول خروجی ثابت است (معمولا خروجی MAC را برچسب (Tag) می‌نامند).
3. با استفاده از کلید و مقدار MAC می‌توان اصالت و همچنین جامعیت پیام را احراز کرد.

نحوه‌ی استفاده از MAC

- فرض می‌کنیم که یک کلید مخفی از طریقی بین آلیس و باب به اشتراک گذاشته شده است.
- آلیس MAC پیام و کلید را محاسبه کرده، سپس پیام و برچسب را برای باب ارسال می‌کند.
- باب با دریافت پیام، MAC پیام و کلید را محاسبه کرده و خروجی آن را با برچسب دریافتی مقایسه می‌کند.
- ویژگی مورد نیاز برای احراز اصالت پیام: محاسبه‌ی یک زوج معتبر پیام و برچسب بدون دانستن و در اختیار داشتن کلید (به لحاظ عملی) امکان‌پذیر نباشد.



مقایسه امضا و MAC

مزایای MAC نسبت به امضا

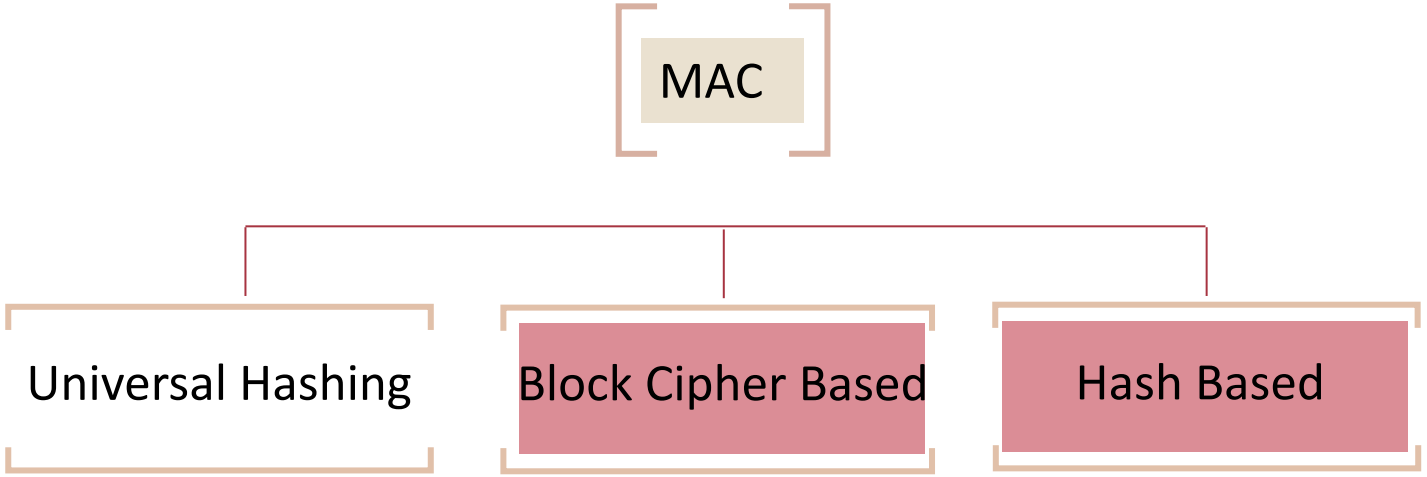
- سرعت (بسیار) بیشتر
- عدم نیاز به گواهی کلید عمومی (درس 16ام)

معایب MAC نسبت به امضا

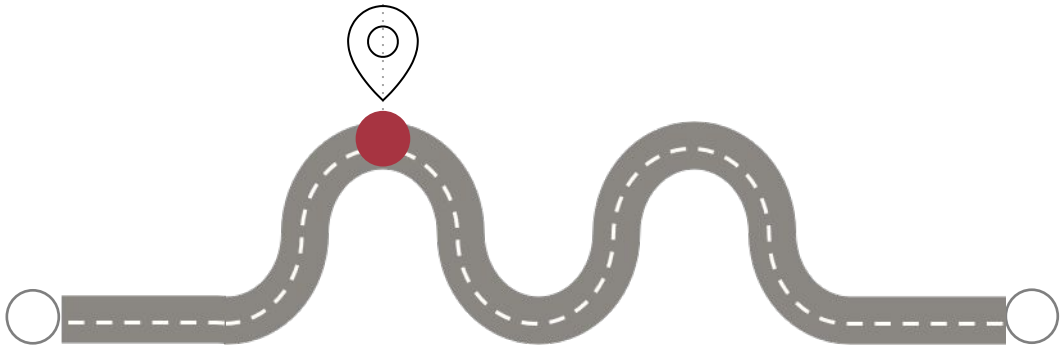
- به کلید مشترک ازپیش‌توزیع‌شده نیاز دارد.
- MAC ذاتا نمی‌تواند ویژگی انکارناپذیری را داشته باشد، چراکه هر دو طرف می‌توانند یک زوج معتبر را تولید کنند.

ساخت MAC

- به تعبیری، کد احراز اصالت پیام یک تابع چکیده‌ساز کلیددار است.
- برای ساخت MAC راهکارهای متفاوتی وجود دارد که عموما مبتنی بر سایر اولیه‌های رمزنگاری هستند.
- دو رویکرد متداول استفاده از تابع چکیده‌ساز و یا رمز قالبی است.



استفاده از تابع چکیده‌ساز برای ساخت MAC



مقدمه

راهکارهای ساده

- چگونه می‌توان یک تابع چکیده‌ساز کلیددار ساخت؟
- یکی از رویکردها، استفاده از یک تابع چکیده‌ساز امن (مانند H) با ورودی‌های پیام و کلید است.
- راهکار ساده‌ی اول (Secret Prefix):

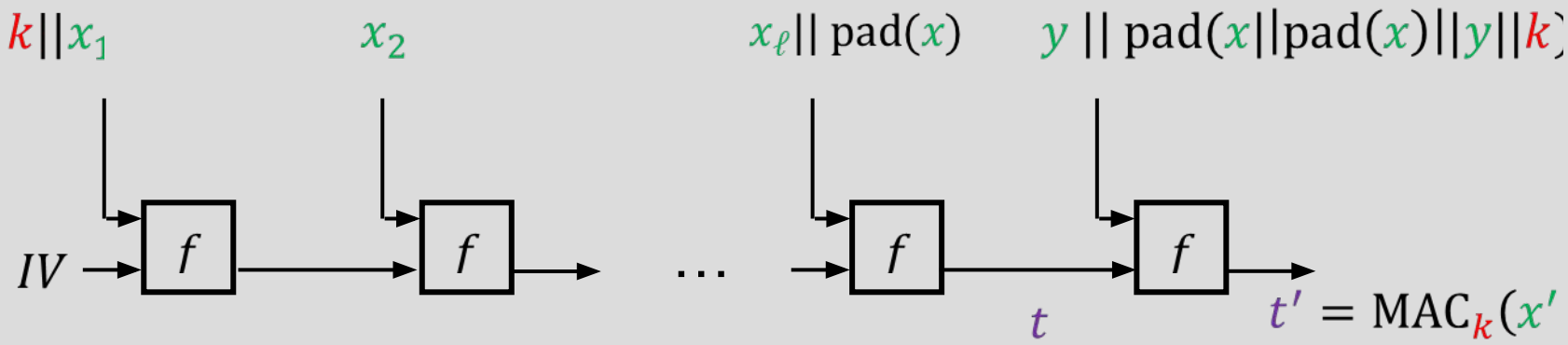
$$MAC(k, x) = H(k||x)$$

- راهکار ساده‌ی دوم (Secret Suffix):

$$MAC(k, x) = H(x||k)$$

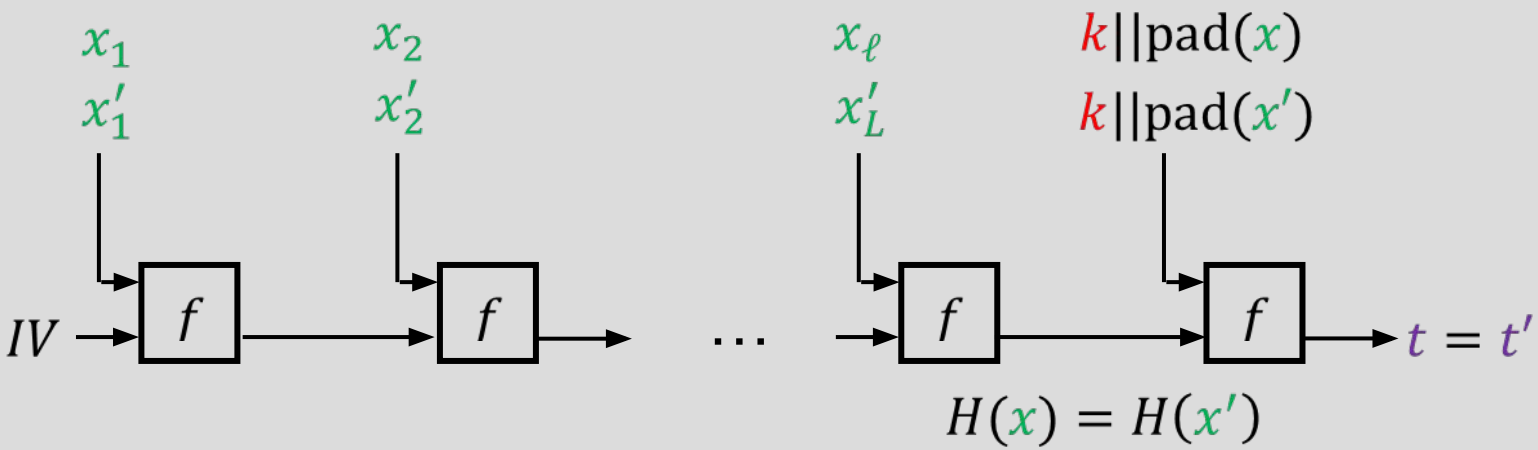
چالش راه‌کار اول

- فرض کنید که تابع چکیده‌ساز ساختار تکرارشونده داشته باشد، و مهاجم به زوج معتبر (x,t) دسترسی دارد.
- مهاجم می‌داند که $t = H(k||x||\text{pad}(x||k))$ است.
- اگر روش پدینگ مستقل از اندازه‌ی پیام باشد، مهاجم می‌تواند بدون دانستن کلید، به‌سادگی مقدار برچسب مربوط به پیام $x' = x||\text{pad}(x)||y$ را برای y محاسبه کند.
- ریشه‌ی مشکل: کلید تنها در محاسبه‌ی اولین تابع فشرده‌ساز است که به‌صورت مستقیم نقش دارد.



چالش راه‌کار دوم

- فرض کنید مهاجم بتواند دو مقدار x و x' با طول برابر را به‌نحوی پیدا کند که چکیده‌ی آن‌ها با هم برابر باشند.
- در این صورت برچسب معتبر برای هر دو پیام برابر می‌شود.
- پیدا کردن تصادم در عمل کار سختی است، اما اگر انجام شود به تمامی کاربران قابل‌اعمال خواهد بود (چون حمله مستقل از کلید است).
- ریشه‌ی مشکل: کلید صرفا در محاسبه‌ی آخرین تابع فشرده‌ساز نقش دارد.



راهکار سوم

- برای فائق آمدن به چالش‌های گفته شده، می‌توان از یک ساختار کلی به‌صورت زیر استفاده کرد:

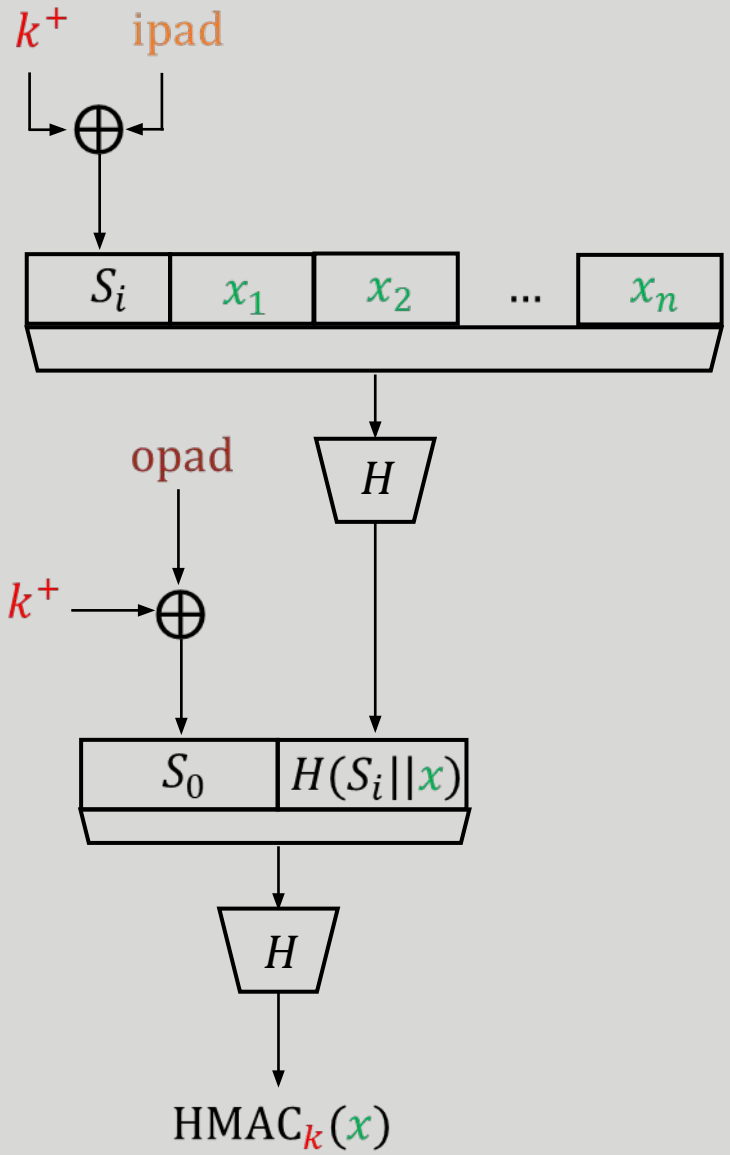
$$H[k||H(k||x)]$$

- امنیت این ساختار به مراتب از ساختارهای قبلی بیشتر است و هیچ‌کدام از ضعف‌های گفته شده را ندارد.
- از طرفی، به لحاظ کارایی، هزینه‌ی سربار زیادی ندارد؛ چون طول خروجی تابع چکیده‌ساز اول ثابت است و تقریبا می‌توان گفت که پیام یک بار پردازش می‌شود.
- بنابراین هرچند تابع چکیده‌ساز دو بار فراخوانی می‌شود، اما پیچیدگی محاسباتی تقریبا برابر با یک بار اجرای این تابع است.
- اصلاح‌شده‌ی این ساختار در کد احراز اصالت استاندارد HMAC، که یکی از پرکاربردترین کدهای احراز اصالت پیام است، استفاده شده است.

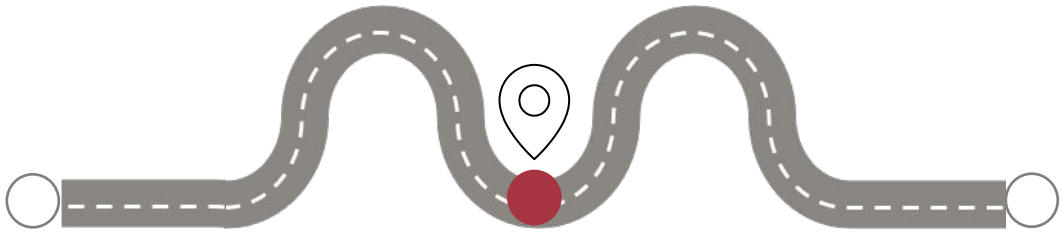
توصیف دقیق HMAC

- کد احراز اصالت HMAC به شکل زیر تعریف می شود:

1. ابتدا کلید با اضافه کردن تعدادی بیت 0 به سمت چپ آن بسط داده می‌شود (k^+)، به‌گونه‌ای‌که طول آن به اندازه‌ی طول قالب ورودی تابع فشرده‌ساز شود.
2. مقدار $H(k^+ \oplus \text{ipad}||x)$ محاسبه می‌شود که در آن ipad یک مقدار ثابت است.
3. مقدار چکیده‌ی $k^+ \oplus \text{opad}$ و خروجی مرحله‌ی دوم محاسبه می‌شود که opad نیز یک مقدار ثابت است.



استفاده از تابع
چکیده‌ساز برای
ساخت MAC

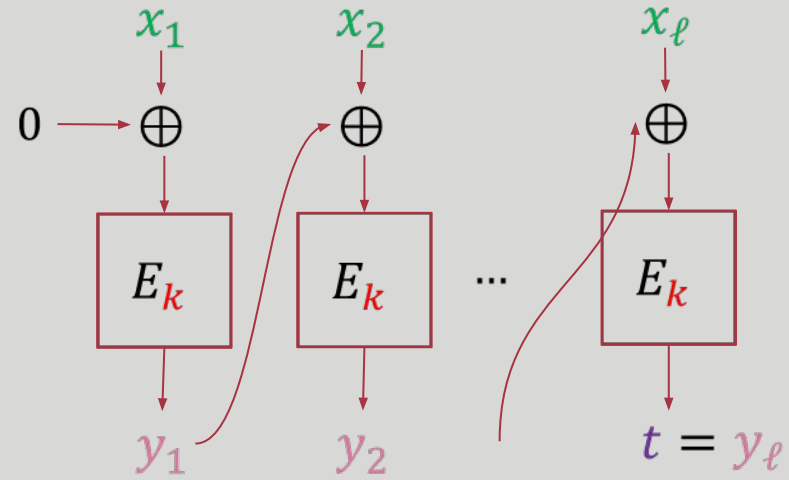


مقدمه

**استفاده از رمز
قالبی برای
ساخت MAC**

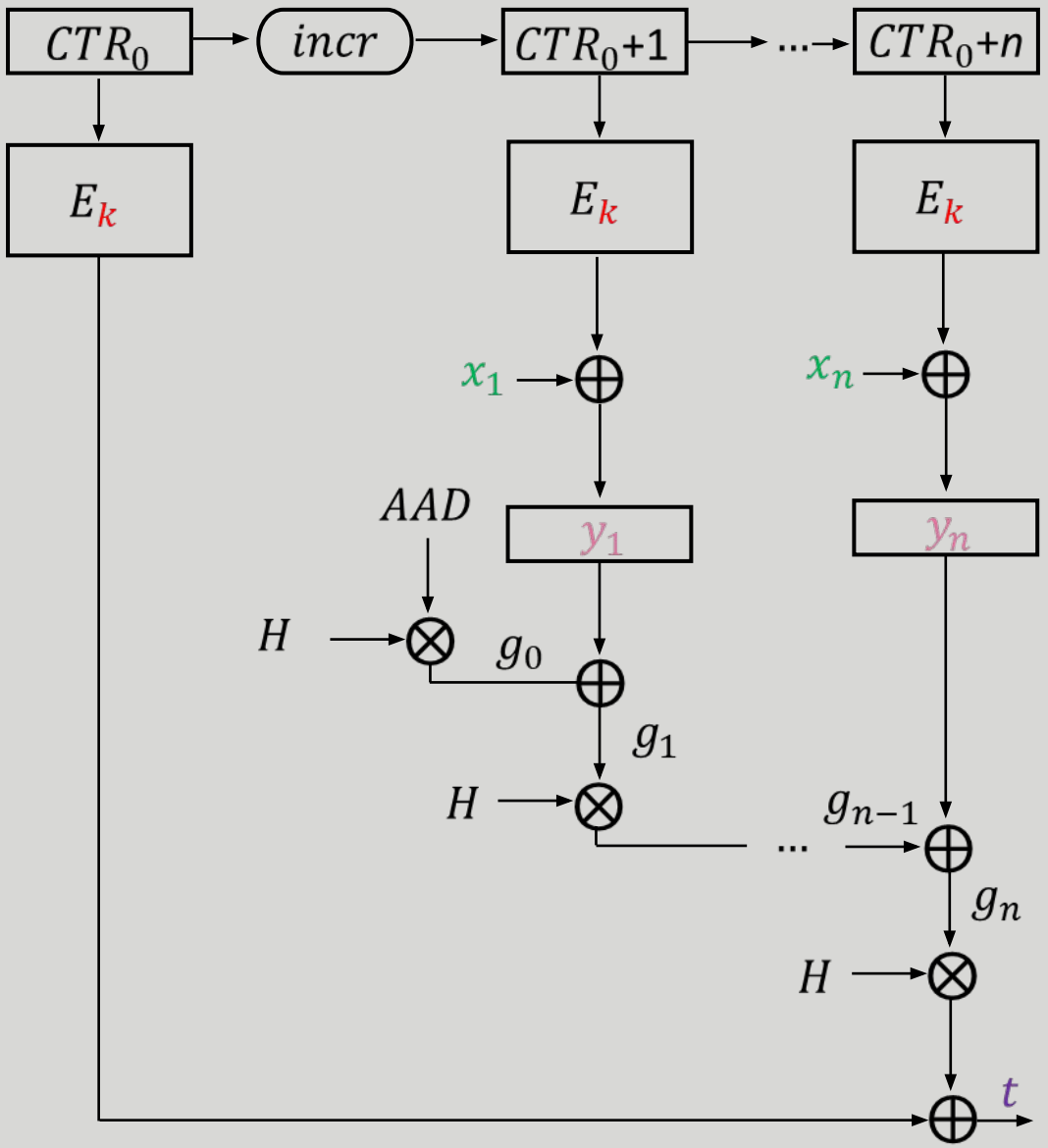
CBC-MAC

- ابتدا پیام بسط داده می‌شود تا ضریبی از طول قالب شود.
- قالب اول بدون تغییر رمز می‌شود (تحت کلید مخفی k).
- سایر قالب‌ها در مد CBC رمز می‌شوند.
- خروجی آخرین قالب به عنوان برچسب پیام در نظر گرفته می‌شود.



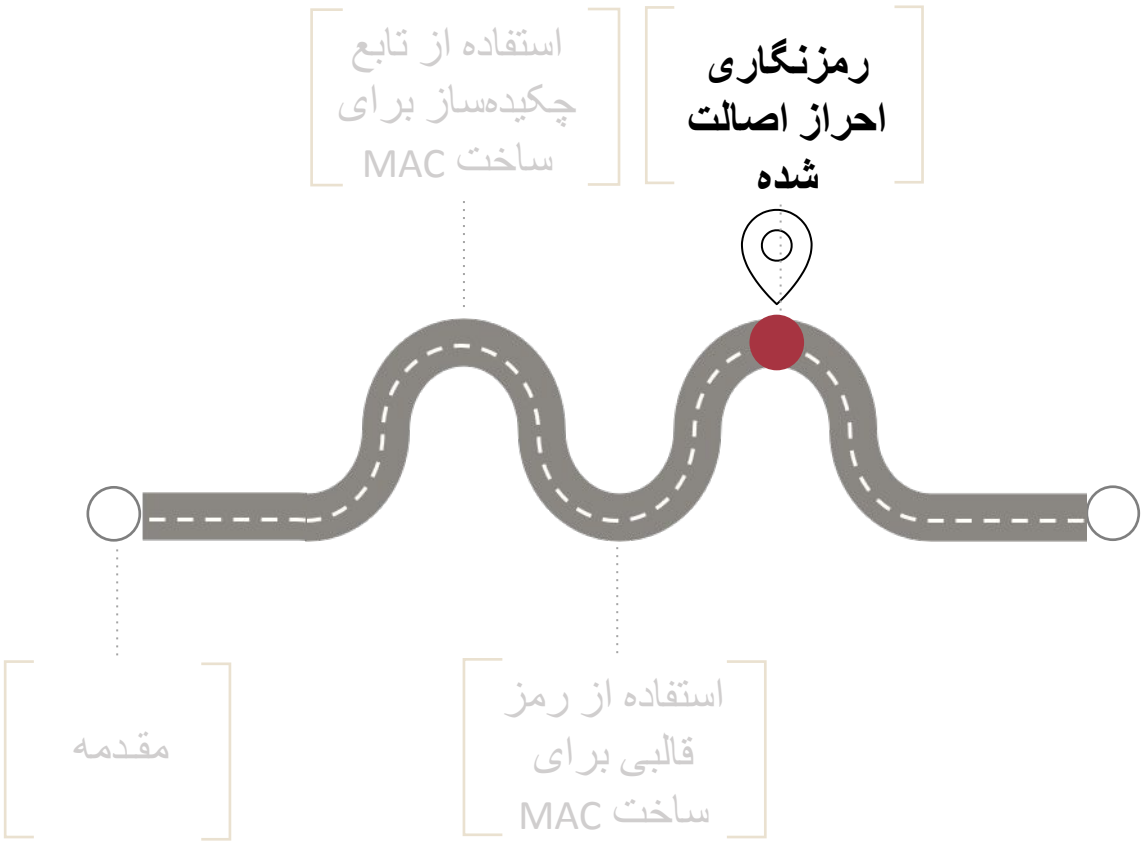
Galois Counter Mode

(GCM)



- GCM در استانداردهای متعددی مورد استفاده قرار گرفته است.
- در ساختار آن:
  - قالب‌های پیام با استفاده از مد Counter رمز می‌شوند.
  - از عملیات ضرب در میدان گالوا با مقدار H (که مقداری وابسته به کلید است) استفاده می‌شود.
  - میدان استفاده شده $GF(2^{128})$ است:

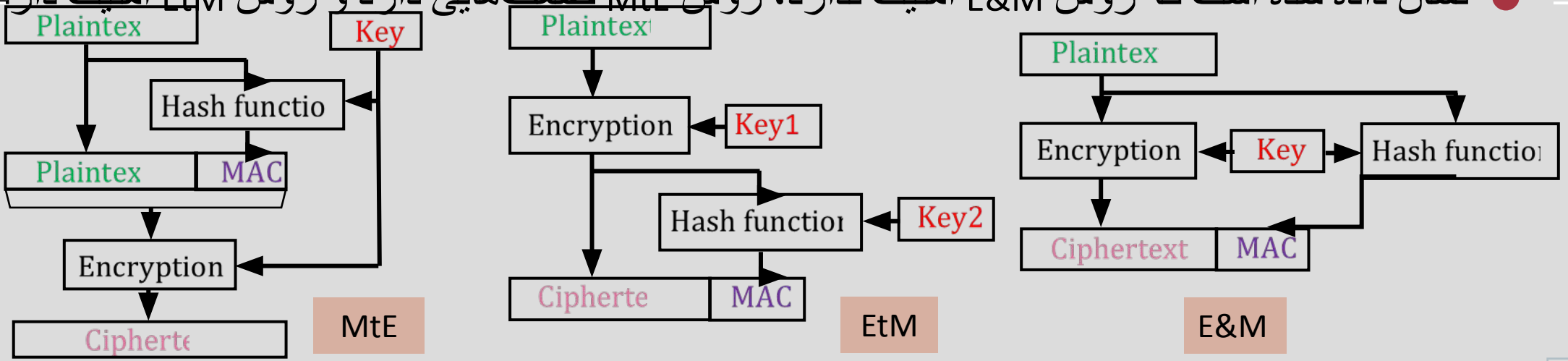
$$GF(2^{128}): GF(2)/\langle x^{128} + x^7 + x^2 + x + 1 \rangle$$


رمزنگاری احراز اصالت شده
استفاده از تابع چکیده‌ساز برای ساخت MAC
مقدمه
استفاده از رمز قالبی برای ساخت MAC

رمزنگاری احراز اصالت شده

(Authenticated Encryption)

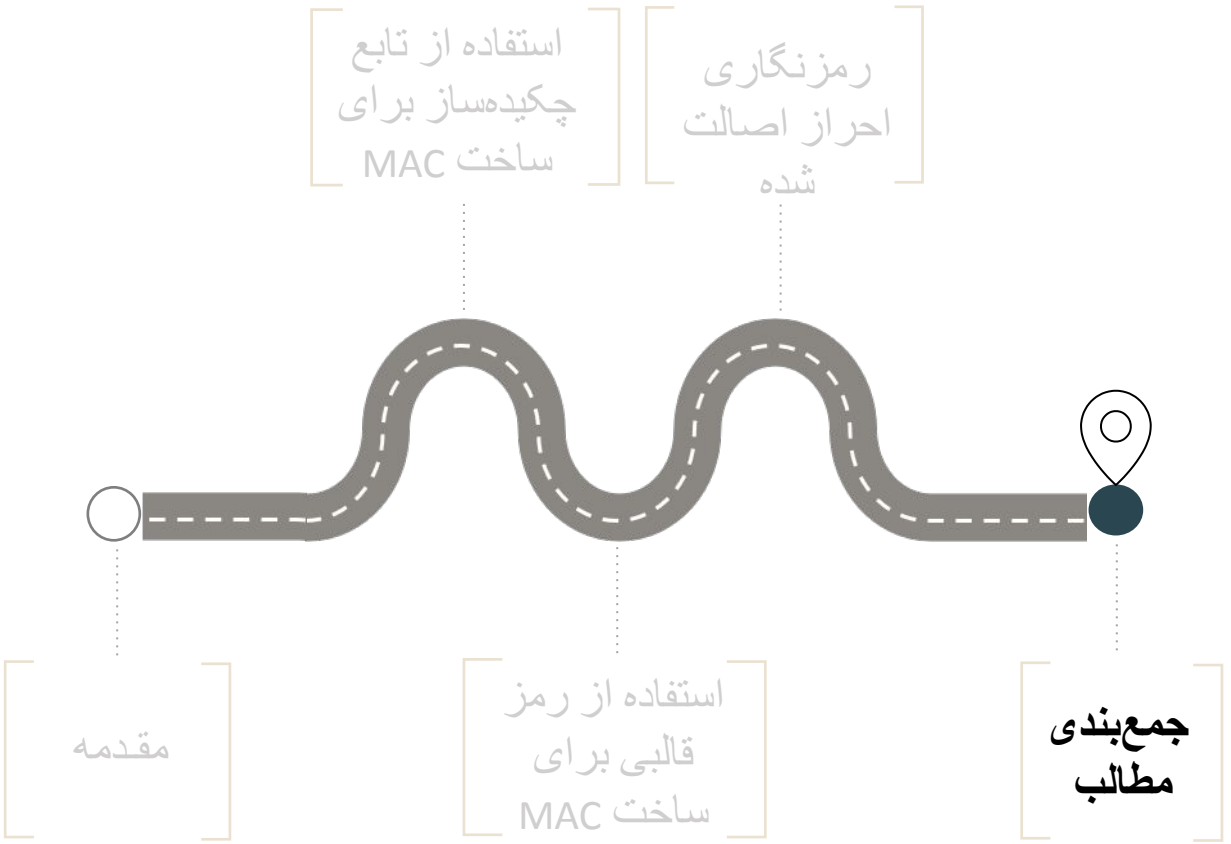
- طرح‌های رمزنگاری احراز اصالت شده، طرح‌هایی هستند که هم احراز اصالت و جامعیت پیام و هم محرمانگی آن را فراهم می‌کنند.
- یک رویکرد برای برآوردن این هدف می‌تواند استفاده‌ی توامان از یک الگوریتم رمزنگاری و همچنین یک MAC باشد.
- برای این استفاده‌ی توامان از رمزنگاری و MAC، سه روش کلی وجود دارد.
- نشان داده شده است که روش E&M امنیت ندارد، روش MtE ضعف‌هایی دارد و روش EtM امنیت دارد.



Figures source: Wikipedia

Authenticated Encryption with Associated Data (AEAD)

- در کاربردهای عملی، متن‌هایی که ارسال می‌شوند بعضا دو دسته هستند:
- پیام اصلی که باید از دید دیگران مخفی باشد.
  - هم به احراز اصالت و هم به محرمانگی نیاز دارد.
- پیام سربار که شامل اطلاعات عمومی است (Associated Data).
  - تنها به احراز اصالت نیاز دارد.
- هم‌اکنون مسابقه‌ای توسط NIST برای انتخاب یک AEAD سبک وزن در جریان است.


مقدمه
استفاده از رمز قالبی برای ساخت MAC
جمع‌بندی مطالب
رمزنگاری احراز اصالت شده
استفاده از تابع چکیده‌ساز برای ساخت MAC

جمع‌بندی مطالب

- یکی دیگر از روش‌های احراز اصالت و جامعیت پیام، استفاده از کدهای احراز اصالت است که نسبت به امضاهای دیجیتال سرعت بالاتری دارند.
- برای استفاده از کدهای احراز اصالت وجود یک کلید مشترک بین طرفین تبادل پیام ضروری است.
- دو رویکرد متداول برای ساخت کدهای احراز اصالت استفاده از توابع چکیده‌ساز امن و یا رمزهای قالبی است.
- هر یک از دو روش فوق مزایا و معایب مخصوص به خود را دارند.
- یکی دیگر از کاربردهای مهم کدهای احراز اصالت استفاده از آن‌ها در ساخت طرح‌های رمزنگاری احراز اصالت شده است.