دانشکده علوم ریاضی و آمار

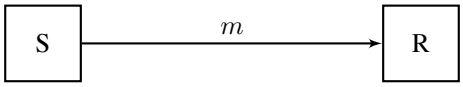
رمزنگاری

مجتبی رفیعی کرکوندی

# جلسه ۱۷: کد اصالت‌سنجی پیام

## ۱ مقدمه

تا به حال تمرکز ما معطوف به رمزنگاری پیام فرستنده به سوی گیرنده بوده است:




در این راستا امنیت رمز استفاده شده را در برابر حمله‌های شنود[1] (تک پیامی و چند پیامی) و سناریوهای قوی‌تر (متن اصلی انتخابی[2] و متن اصلی رمزی[3]) بررسی کردیم. نکته‌ای که در این میان وجود دارد آن است که این حمله‌ها از نوع حمله‌ی منفعل[4] هستند.

***تعریف ۱ (حمله منفعل)*** *حمله‌ای منفعل است که در آن مهاجم نتواند تغییری در پیام ارسالی از فرستنده به گیرنده ایجاد کند و صرفا تلاش می‌کند تا اطلاعاتی در مورد پیام بدست آورد.*

*حمله کننده فعال[5] با دست‌کاری در پیام‌های ارسالی سعی در خراب‌کاری دارد. یک حمله‌ی فعال تحت سناریوی متن رمزی انتخابی علیه یک سیستم رمز را در نظر بگیرید. اگر سیستم رمز دارای امنیت متن رمزی انتخابی باشد، حمله کننده قادر نیست متن رمزی را طوری تغییر دهد که تبدیل به متن رمز شده‌ی متناظر با پیام دلخواهش شود. درواقع چنین سیستم رمزی، دارای امنیت قوی‌تری است: مهاجم قادر نیست متن رمز شده را طوری تغییر دهد، به طوری‌که بتواند در مورد متن اصلی متناظر آن اطلاعاتی کسب کند. با این وجود ممکن است مهاجم بتواند متن رمزی بسازد که معتبر باشد و گیرنده بتواند آنرا رمزگشایی کند. چنین ویژگی در بعضی کاربردها می‌تواند خطرناک باشد.*

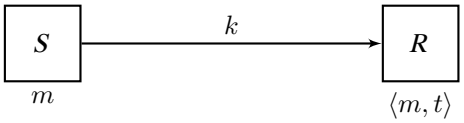
$$\begin{array}{ccc} m & \xrightarrow{\mathsf{Enc}} & c \\ \wr & & \wr \\ m' & & c' \end{array}$$

[1] eavesdropping
[2] chosen-plaintext attack
[3] chosen-ciphertext attack
[4] passive
[5] active

**سوال.** *سوالی که پیش می‌آید آن است که چه کار می‌توان کرد تا گیرنده از اصالت پیام دریافتی مطمئن شود.*
**پاسخ.** *اولین چیزی که به ذهن می‌رسد آن است که فرستنده باید ویژگی خاصی از پیام اصلی بدست آورده و یا مقداری را از روی آن حساب کند و بجای پیام، مجموعه‌ی پیام و مقدار محاسبه شده را برای ارسال در نظر بگیرد تا اعتبار پیام از روی این مقدار بررسی شود:*

$$\langle m, f(m)\rangle$$

*در عمل، تابع $f$ می‌تواند یک $parity$ روی بیت‌های $m$ و یا $checksum$ پیام اصلی باشد. اما در این حالات این تابع عمومی[6] است و مهاجم با اطلاع از تابع $f$ قادر است، حمله مناسبی طراحی کند. برای حل این مشکل در اینجا نیز از یک کلید مشترک بین فرستنده و گیرنده استفاده می‌کنیم. یعنی در پایان پیام یک برچسب[7] چون $t$ به پیام اضافه می‌کنیم که این برچسب تابعی از پیام اصلی و کلید است:*




*در نهایت گیرنده با دریافت $t$ بررسی می‌کند که آیا $t$ تابعی معلوم از پیام و کلید است یا خیر و به این ترتیب صحت و اصالت پیام را ملاحظه می‌کند.*

## ۲ کد اصالت‌سنجی پیام

**تعریف ۲** *یک سیستم کد اصالت‌سنجی پیام[8] ($MAC$) به صورت $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ از الگوریتم‌های چندجمله‌ای تصادفی روی فضای $\mathcal{M}$ است که در آن:*

- Gen: *الگوریتم تولید کلید احتمالاتی است که از روی پارامتر امنیت $n$ کلید $k$ را تولید می‌کند. $\mathcal{K}$ را فضای کلید، یعنی مجموعه همه خروجی‌های الگوریتم تولید کلید در نظر می‌گیریم.*
- Mac: *الگوریتم تولید برچسب است و پیام $m \in \mathcal{M}$ و کلید $k \in \mathcal{K}$ را به برچسب $t \leftarrow \mathsf{Mac}_k(m)$ می‌نگارد.*
- Vrfy: *الگوریتم تایید برچسب است و پیام $m \in \mathcal{M}$، کلید $k \in \mathcal{K}$ و برچسب $t$ را می‌گیرد و خروجی یک (به معنی معتبر) یا صفر (به معنی نامعتبر) بر می‌گرداند.*

**شرط صحت.** *برای هر پیام $m$ و هر کلید $k$ داریم:*

$$\Pr[k \leftarrow \mathsf{Gen}(1^n)\,; t \leftarrow \mathsf{Mac}_k(m) : \mathsf{Vrfy}_k(\langle m, t\rangle) = 1] = 1\ .$$

**نکته.** *الگوریتم تولید برچسب می‌تواند قطعی یا تصادفی باشد. اما الگوریتم تایید برچسب همواره قطعی است.*

**چگونه می‌توان یک کد اصالت‌سنجی ساخت؟** *برای پاسخ به این سوال ابتدا فرض می‌کنیم که پیام‌های ما طول ثابتی دارند؛ مثلاً $\mathcal{M} = \{0,1\}^n$. ایده‌ی ابتدایی این است که مشابه رمزنگاری از $OTP$[9] برای کد اصالت‌سنجی پیام استفاده کنیم، داریم:*

- $\mathsf{Gen}(1^n) : k \leftarrow \{0,1\}^n$
- $t = \mathsf{Mac}_k(m) : t \leftarrow m \oplus k$
- $\mathsf{Vrfy}_k(\langle m, t\rangle) = \begin{cases} 1 & if\ (t = m \oplus k) \\ 0 & o.w. \end{cases}$

[6] public
[7] tag
[8] Message Authentication Code
[9] One Time Pad

**آیا این روش برای ساخت برچسب امن است؟** *برای پاسخ به این پرسش ابتدا نیاز داریم که تعریفی دقیقی از امنیت کد اصالت‌سنجی پیام ارائه کنیم که قابلیت‌های حمله‌کننده‌های فعال را در دنیای واقعی مدل می‌کند.*

## ۳ امنیت سیستم کد اصالت‌سنجی پیام

*حمله به یک سیستم کد اصالت‌سنجی با هدف جعل پیام صورت می‌گیرد. به عبارت دیگر مهاجم برای پیام مورد نظرش یک برچسب معتبر می‌سازد تا گیرنده به هنگام بررسی اصالت پیام، آن را معتبر تشخیص دهد. برای تعریف امنیت چنین سیستمی، ابتدا نیاز است تا آزمایش مناسبی طراحی کرد تا توان حمله‌ی مهاجم[۱۰] به این سیستم را مدل کند. طراحی این آزمایش به صورت یک بازی بین مهاجمی چون $\mathcal{A}$ و یک چالشگر[۱۱] فرضی اجرا می‌شود. در این آزمایش بررسی می‌شود که آیا مهاجم می‌تواند برای پیامی که قبلا برچسب آن را ندیده است، برچسب معتبری تولید کند یا خیر. این آزمایش که با $\mathsf{MacForge}_{\mathcal{A},\Pi}$ نشان داده می‌شود، به صورت زیر اجرا می‌شود:*

۱. *چالشگر یک کلید $k$ تولید می‌کند:*

$$k \leftarrow \mathsf{Gen}(1^n)$$

۲. *به مهاجم دسترسی اوراکلی به $\mathsf{Mac}_k(\cdot)$ داده می‌شود تا پیام‌های مختلف را بررسی کرده و در نهایت پس از پرسمان[۱۲]های لازم، یک زوج $\langle m, t\rangle$ خروجی دهد:*

$$\langle m, t\rangle \leftarrow \mathcal{A}^{\mathsf{Mac}_k(\cdot)}(1^n)$$

*مجموعه‌ی پرسمان‌های مهاجم به هنگام بررسی را $Q$ می‌نامیم. خروجی آزمایش که با متغیر تصادفی $\mathsf{MacForge}_{\mathcal{A},\Pi}(n)$ نشان داده می‌شود یک در نظر گرفته می‌شود اگر و فقط اگر مهاجم موفق به جعل یک برچسب معتبر برای پیامی که قبلاً پرسمان نکرده است شود. به طور دقیق‌تر:*

$$\mathsf{MacForge}_{\mathcal{A},\Pi}(n) = \begin{cases} 1 & \text{if}(m \notin Q \wedge \mathsf{Vrfy}_k(\langle m, t\rangle) = 1) \\ 0 & \text{o.w.} \end{cases}$$

***تعریف ۳*** *یک سیستم کد اصالت‌سنجی پیام دارای امنیت جعل‌ناپذیری[۱۳] است، هرگاه برای هر مهاجم تصادفی چون $\mathcal{A}$ که در زمان چندجمله‌ای اجرا می‌شود، یک تابع ناچیز چون $\varepsilon(n)$ یافت شود به طوری که داشته باشیم:*

$$\Pr[\mathsf{MacForge}_{\mathcal{A},\Pi}(n) = 1] \leqslant \varepsilon(n)$$

***نکته ۱*** *تعریف فوق حمله بازپخش[۱۴] را مدل نمی‌کند. به عبارت دیگر اگر زوج $\langle m, t\rangle$ توسط فرستنده مجاز برای گیرنده ارسال شود، مهاجم می‌تواند بعدا همین پیام را از طرف فرستنده برای گیرنده ارسال کند و گیرنده آنرا بپذیرد. این بدین معنی نیست که حمله بازپخش در عمل مهم نیست؛ برعکس، حمله بازپخش در عمل می‌تواند بسیار خطرناک باشد. اما برای مقابله با آن باید چاره‌های دیگری اندیشید (مانند استفاده از مهر زمانی[۱۵]) که از موضوع این درس خارج است.*

*اکنون باید واضح باشد که چرا پیشنهاد قسمت قبلی برای کد اصالت‌سنجی دارای امنیت لازم نیست. برای اثبات دقیق ادعا مهاجم $\mathcal{A}$ را به صورت زیر می‌سازیم که در آزمایش همواره برنده می‌شود (خروجی آزمایش با احتمال یک برابر 1 می‌شود). مهاجم ابتدا پرسمان داخواه $m_1$ را به اوراکل $\mathsf{Mac}_k(\cdot)$ ارسال می‌کند و برچسب $t_1$ را دریافت می‌کند. سپس زوج $\langle m, t\rangle = \langle m_1 \oplus 1^n, t_1 \oplus 1^n\rangle$ را به خروجی می‌دهد. به وضوح داریم:*

$$\Pr[\mathsf{MacForge}_{\mathcal{A},\Pi}(n) = 1] = 1 \ .$$

[10] adversary
[11] challenger
[12] query
[13] unforgeability
[14] replay attack
[15] timestamp

### ۱.۳ امنیت جعل‌ناپذیری قوی

*در آزمایش جعل‌ناپذیری، مجموعه‌ی همه زوج پرسمان‌های ارسالی و برچسب‌های دریافتی توسط مهاجم به هنگام بررسی را $Q'$ بنامید. یک خروجی دیگر که با متغیر تصادفی $\mathsf{SMacForge}_{\mathcal{A},\Pi}(n)$ نشان داده می‌شود برای آزمایش در نظر بگیرید که برابر یک در نظر گرفته می‌شود اگر و فقط اگر مهاجم موفق شود به یکی از دو هدف زیر دست یابد:*

- *جعل یک برچسب معتبر برای پیامی که قبلاً پرسمان نکرده است،*
- *جعل یک برچسب جدید برای پیامی که قبلاً پرسمان کرده است.*

*به طور دقیق‌تر:*

$$\mathsf{SMacForge}_{\mathcal{A},\Pi}(n) = \begin{cases} 1 & \text{if } (\langle m,t\rangle \notin Q' \wedge \mathsf{Vrfy}_k(\langle m,t\rangle) = 1) \\ 0 & \text{o.w.} \end{cases}$$

***تعریف ۴*** *یک سیستم کد اصالت‌سنجی پیام دارای امنیت جعل‌ناپذیری قوی[۱۶] است، هرگاه برای هر مهاجم تصادفی چون $\mathcal{A}$ که در زمان چندجمله‌ای اجرا می‌شود، یک تابع ناچیز چون $\varepsilon(n)$ یافت شود به طوری که داشته باشیم:*

$$\Pr[\mathsf{SMacForge}_{\mathcal{A},\Pi}(n) = 1] \leqslant \varepsilon(n)$$

***قضیه ۱*** *امنیت جعل‌ناپذیری قوی، امنیت جعل‌ناپذیری را نتیجه می‌دهد.*

***قضیه ۲*** *اگر الگوریتم تولید برچسب قطعی باشد، امنیت جعل‌ناپذیری قوی و امنیت جعل‌ناپذیری معادلند.*

## ۴ ساخت یک کد امن اصالت‌سنجی پیام

*در ابتدا بررسی می‌کنیم که چگونه می‌توان یک **MAC** مناسب برای رشته‌های با طول ثابت، مثلا مجموعه رشته‌های $n$-بیتی ساخت. فرض کنید مجموعه توابع $f_k : \{0,1\}^{|k|} \to \{0,1\}^{|k|}$ خانواده‌ای از توابع شبه‌تصادفی باشند. سیستم کد اصالت‌سنجی پیام $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ را روی $\mathcal{M} = \{0,1\}^n$ اینگونه تعریف می‌کنیم:*

- $\mathsf{Gen}(1^n) : k \leftarrow \{0,1\}^n$
- $\mathsf{Mac}_k(m) : \langle m, f_k(m)\rangle$
- $\mathsf{Vrfy}_k(\langle m,t\rangle) = \begin{cases} 1, & \textit{if } t = f_k(m) \wedge m,t \in \{0,1\}^n \\ 0, & \textit{otherwise} \end{cases}$

***قضیه ۳*** *سیستم کد اصالت‌سنجی فوق دارای امنیت جعل‌ناپذیری است.*

*برای اثبات قضیه فوق از برهان خلف کمک می‌گیریم. فرض کنید این سیستم جعل‌پذیر است. پس مهاجم می‌تواند برای پیامی چون $m$ که پرسمان نشده، مقدار تابع $f_k(m)$ را محاسبه کند، که این معادل شبه تصادفی نبودن تابع $f_k$ است.*

[16] strong unforgeability