به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری ۲ آذر ۱۳۹۱

جلسه‌ی ۱۵: مدهای عمل‌کرد رمزهای قالبی

مدرس: دکتر شهرام خزائی *نگارنده: مهدی مردی*

در این جلسه شیوه استفاده از *رمزهای قالبی*[۱] *را مورد بررسی قرار می‌دهیم و چهار مورد از* مدهای عملکرد[۲] را معرفی و در مورد امنیت آنها بحث می‌کنیم. در ابتدا توجه می‌کنیم که اگر $E : \{۰,۱\}^n \times \{۰,۱\}^n \longrightarrow \{۰,۱\}^n$ یک جایگشت شبه تصادفی (PRP) باشد آنگاه هر رشته n-بیتی را یک قالب می‌گوئیم. با این اصطلاح می بینیم که رمز قالبی فقط روی یک تک قالب عمل می‌کند و این سوال بوجود می‌آید که چگونه پیام‌های با طول دلخواه را رمز کنیم.

نکته ۱ *پیام‌های با طول دلخواه را می‌توان با اضافه کردن یک عدد* ۱ *و به تعداد کافی* ۰ *در انتهای آن، به طول مضربی از اندازه قالب مطلوب تبدیل کرد. این عمل پدینگ*[۳] *نامیده‌شود. به طور دقیق‌تر، اگر* $M \in \{۰,۱\}^*$ *یک رشته دلخواه باشد، رشته پد شده به صورت* $M۱۰^t$ *می‌باشد که* $۰ \le t \le n-۱$ *کوچکترین عددی است که به ازای آن* $|M۱۰^t|$ *مضرب* n *است که ما آن را به صورت زیر نشان می‌دهیم:*

$$M۱۰^t = m_۱ m_۲ \dots m_b \quad , \quad |m_i| = n \qquad for \ ۱ \le i \le b\,.$$

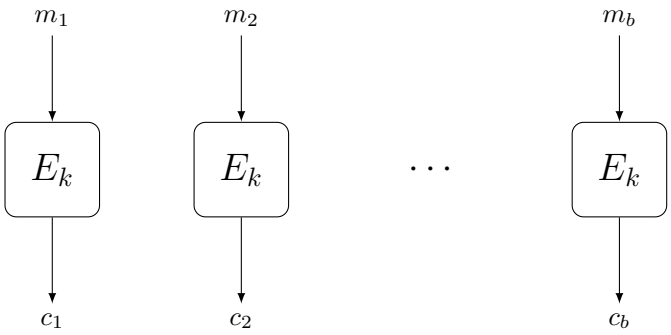
۱ مد کتاب الکترونیک

مد کتاب الکترونیک، ECB[۴]، یکی از ساده‌ترین مدهای ممکن است که رمز کردن به طور مستقیم با اعمال جایگشت شبه‌تصادفی روی هر قالب متن اصلی به طور جداگانه انجام می‌شود. به عبارت دقیق‌تر مد کتاب الکترونیک، متن اصلی پد شده $M۱۰^t = m_۱ m_۲ \cdots m_b$ را به متن رمزی

$$c = \langle E_k(m_۱), E_k(m_۲), \dots, E_k(m_b) \rangle$$

تبدیل می‌کند (شکل ۱).
بازگشایی رمز نیز به صورت واضحی با استفاده از این حقیقت که $E_k^{-۱}$ به صورت موثری قابل محاسبه است به دست می‌آید. البته باید توجه شود که رمزگشایی فقط درصورتی با موفقیت انجام می‌شود که رشته ورودی یک متن رمزشده معتبر باشد (یعنی، رمزشده یک متن اصلی باشد). به طور دقیق‌تر، برای رمزگشایی رشته $c \in \{۰,۱\}^*$

[۱] block ciphers
[۲] modes of operation
[۳] padding
[۴] Electronic Code Book (ECB) mode



شکل ۱: مد کتاب الکترونیک (ECB)

الگوریتم رمزگشایی ابتدا بررسی می‌کند که $|c|$ مضربی از n باشد. اگر نباشد $\perp$ برمی‌گرداند؛ در غیر این صورت، محاسبات زیر انجام می‌شود که $c = c_1 \dots c_b$ و $|c_i| = n$:

$$m_i = E_k^{-1}(c_i) \quad \texttt{for } 1 \le i \le b\,.$$

سپس، اگر m_b یک بلوک تمام‌صفر باشد، الگوریتم رمزگشایی باز هم $\perp$ برمی‌گرداند؛ در غیر این‌صورت، با حذف پدینگ متن M برگردانده می‌شود که $M10^t = m_1 m_2 \cdots m_b$ و $0 \le t \le n-1$.

فرآیند رمزنگاری در این مورد قطعی[۵] (غیراحتمالی) می‌باشد، بنابراین این روش عملکرد نمی‌تواند امنیت چندپیامی داشته باشد. در واقع با توجه به اینکه، قالب‌های برابر به قالب‌های یکسان نگاشته می‌شوند، این روش حتی امنیت تک‌پیامی هم ندارد. از این رو امکان تشخیص نمونه‌های متن اصلی در متن رمزشده وجود دارد. با استفاده از این مشاهده می‌توان یک مهاجم امنیت تک‌پیامی ارائه کرد. کافیست مهاجم پیام‌های $M_0 = 0^n 0^n$ و $M_1 = 0^n 1^n$ را (که دارای طول یکسان می‌باشند) به چالش‌گر فرستاده و پس از دریافت متن رمزی $c = \langle c_0, c_1, c_2 \rangle$ (که رمز شده‌ی یکی از پیام‌های M_0 یا M_1 می‌باشد و با توجه به انتخاب مهاجم طول آن حتماً $3n$ است)، بیت $\hat{b}$ را به صورت زیر تولید کند:

$$\hat{b} = \begin{cases} 1 & \texttt{if} \quad c_0 \neq c_1 \\ 0 & \texttt{if} \quad c_0 = c_1 \end{cases}$$

بنابراین همواره $b = \hat{b}$ و لذا احتمال موفقیت مهاجم در آزمایش برابر یک می‌باشد:

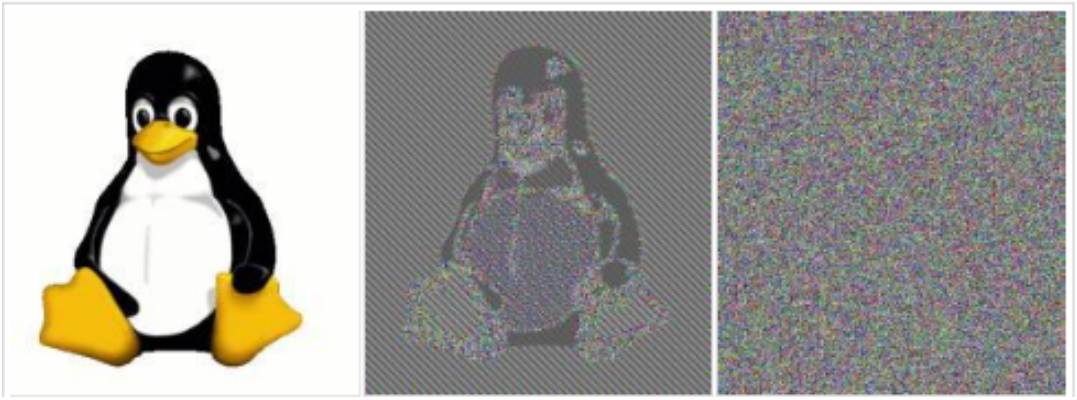
$$\Pr\{\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1\} = 1\,.$$

قابل توجه است که حمله فوق علیه مد کتاب الکترونیک، ECB، یک مسئله نظری نیست و اطلاعات زیادی را می‌توان با مشاهده متون رمز شده به دست آورد که توسط این روش تولید شده‌اند. بنابراین روش ECB نباید استفاده شود و معرفی این روش صرفاً به خاطر اهمیت تاریخی آن است.

یک مثال قابل توجه از اینکه ECB مقداری از اطلاعات متن اصلی را در متن رمزی فاش می‌کند، در حالتی است که برای رمزنگاری یک تصویر بیت‌مپ[۶] استفاده شود. در این حالت مناطق وسیعی از رنگ‌های یکنواخت به صورت مشابه رمز شده و رنگ‌های پیکسل‌های تکی نیز به صورت جداگانه رمز شده، یعنی همانگونه که گفته شد قالب‌های

[۵] deterministic
[۶] bitmap image

یکسان به قالب‌های مشابه رمز می‌شوند. این باعث می‌شود همان تفاوت‌های رنگ در متن اصلی در متن رمز شده نیز قابل دیدن باشد (شکل ۲).

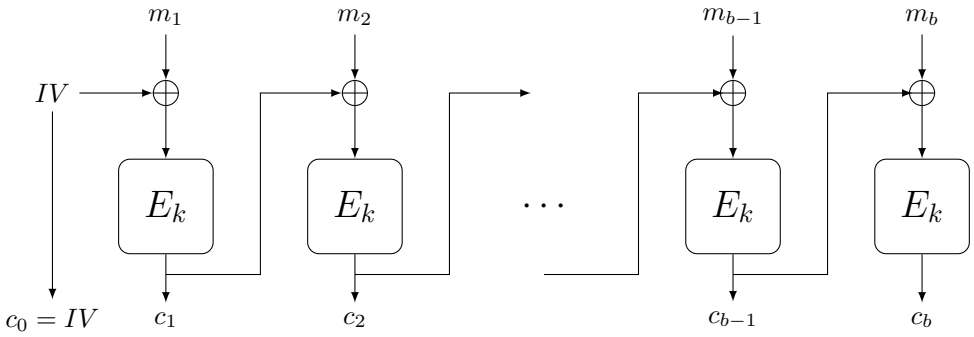


شکل ۲: [برگرفته از ویکی‌پدیا] یک تصویر بیت‌مپ و رمز شده آن با مد کتاب الکترونیک (شکل وسط) و یک مد امن (شکل سمت راست).

۲ مد زنجیری قالب رمز

در مد زنجیری قالب رمز، CBC[۷]، ابتدا یک بردار اولیه تصادفی IV به طول n انتخاب می‌شود که بخشی از متن رمز شده خواهد بود. سپس به طریق زیر متن رمزی حاصل می‌شود.

$$c_0 = IV \quad , \quad c_i = E_k(c_{i-1} \oplus m_i) \quad , \quad 1 \le i \le b$$



شکل ۳: روش زنجیری قالب رمز (رمزنگاری)

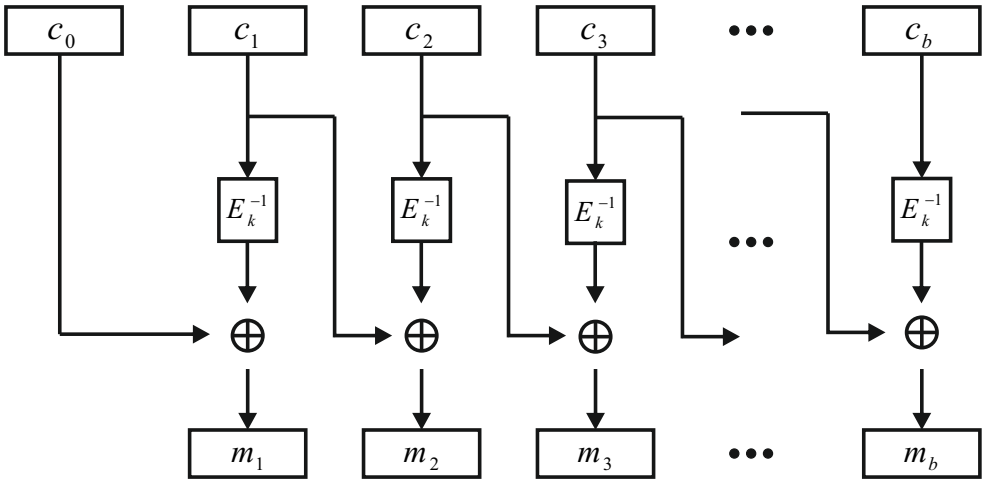
متن رمز نهایی به صورت $c = \langle IV, c_1, c_2, \ldots, c_b \rangle$ می‌باشد (شکل ۳).

[۷] Cipher Block Chaining (CBC) mode

برای باز نمودن این رمز کافی است m_i ها را به صورت زیر محاسبه (شکل ۴)

$$m_i = E_k^{-1}(c_i) \oplus c_{i-1}$$

و سپس پدینگ را حذف کنیم. در صورتی که پدینگ معتبر نباشد $\perp$ برگردانده می‌شود.



شکل ۴: روش زنجیری قالب رمز (رمزگشایی)

روش رمزنگاری به روش CBC احتمالاتی است و می‌توان ثابت کرد که اگر E یک جایگشت شبه‌تصادفی باشد آنگاه روش CBC دارای امنیت در مقابل حمله متن اصلی انتخابی[۸] است.

قضیه ۱ *اگر E یک جایگشت شبه‌تصادفی باشد، آنگاه روش CBC دارای امنیت متن اصلی انتخابی است.*

مهمترین اشکال این روش این است که رمزنگاری باید به طور متوالی انجام شود و قابلیت پردازش موازی ندارد. زیرا به ترتیب برای رمز کردن قالب متن اصلی m_j به قالب متن رمزی c_{j-1} نیاز است، و نیز به همین علت قالب های یکسان در زمینه های مختلف به شکل متفاوتی رمز می‌شوند. روش رمزنگاری CBC دارای امنیت حمله متن رمزی انتخابی[۹] نمی‌باشد. مهاجم را به این صورت طراحی می‌کنیم. در آزمایش حمله متن رمزی انتخابی مهاجم دو پیام به صورت $M_0 = 0^n$ و $M_1 = 1^n$ به چالش‌گر می‌دهد. سپس چالش‌گر متن رمز شده یکی از آنها را به صورت $c = \langle c_0, c_1, c_2 \rangle$ به مهاجم برمی‌گرداند. به یاد آورید که مهاجم دسترسی اوراکلی به الگوریتم رمزنگاری و رمزگشایی دارد ولی مجاز به درخواست رمزگشایی متن رمزی چالشی c نمی‌باشد. به همین علت مهاجم با تغییر اندکی در آن، متن رمزی درخواستی $c' = \langle c_0 \oplus 1^n, c_1, c_2 \rangle$ را به اوراکل رمزگشا می‌فرستد و پس از دریافت پیام متناظر آن، M'، بیت $\hat{b}$ را به صورت زیر تولید می‌کند:

$$\hat{b} = \begin{cases} 1 & \texttt{if} \quad M' = M_0 \\ 0 & \texttt{if} \quad M' = M_1 \end{cases}.$$

[۸] Chosen-Plaintext Attack
[۹] Chosen-Ciphertext Attack

بنابراین همواره $b = \hat{b}$ و لذا احتمال موفقیت مهاجم در آزمایش متن رمزی انتخابی برابر یک می‌باشد:

$$\Pr\{\mathsf{PrivK}^{\mathrm{cca}}_{\mathcal{A},\Pi} = ۱\} = ۱ .$$

۳ روش تغذیه خروجی

در اصل مد بازخورد خروجی، OFB[۱۰]، روشی برای تولید یک رشته شبه‌تصادفی با استفاده از رمزهای قالبی می‌باشد که مانند یک رمز دنباله‌ای عمل می‌کند. بدین صورت که ابتدا بردار تصادفی n-بیتی IV انتخاب می‌شود و دنباله $z_۰, z_۱, \cdot, c_b$ با شروع از $z_۰ = IV$ با استفاده از رابطه بازگشتی

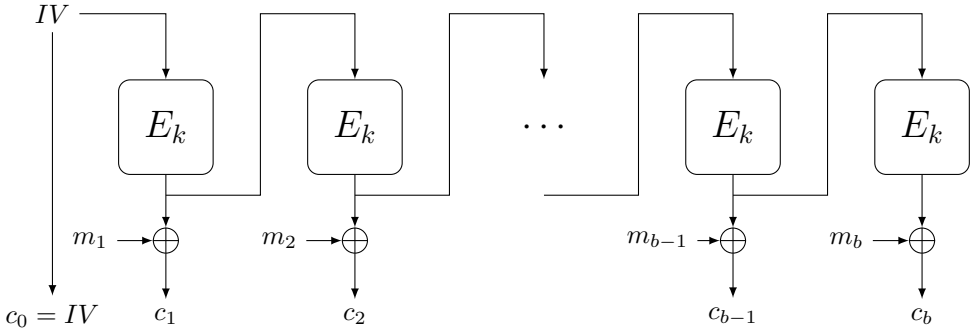
$$z_i = E(z_{i-۱}),\ i = ۱, ۲, \cdots, b$$

تولید می‌شود. در نهایت هر قالب از متن اصلی با قالب متناظر از دنباله برای تولید متن رمز شده به صورت زیر XOR می‌شود (شکل ۵):

$$c_i = m_i \oplus z_i,\ i = ۱, ۲, \cdots, b .$$

و سرانجام متن رمزی به صورت نهای زیر حاصل می‌شود:

$$c = \langle IV, c_۱, \cdots, c_b \rangle .$$



شکل ۵: رمزنگاری روش تغذیه خروجی (رمزنگاری)

رمزگشایی نیز به روش مشابه انجام می‌گیرد. در این روش نیز همانند روش CBC بردار آغازین IV قسمتی از متن رمزی می‌باشد. در مقایسه با روش CBC در اینجا لزومی ندارد که E وارون پذیر باشد و از یک تابع شبه‌تصادفی نیز به جای یک یگشت شبه‌تصادفی می‌توان استفاده کرد. در این روش نیز هر دو الگوریتم رمزنگاری و رمزگشایی باید به صورت متوالی انجام شوند، در نتیجه این مد نیز قابلیت پردازش موازی را ندارد. در نهایت قضیه زیر را بدون اثبات بیان می‌کنیم.

قضیه ۲ *اگر E یک تابع شبه‌تصادفی باشد، آنگاه روش OFB دارای امنیت متن اصلی انتخابی است.*

[۱۰] Output Feedback (OFB) mode

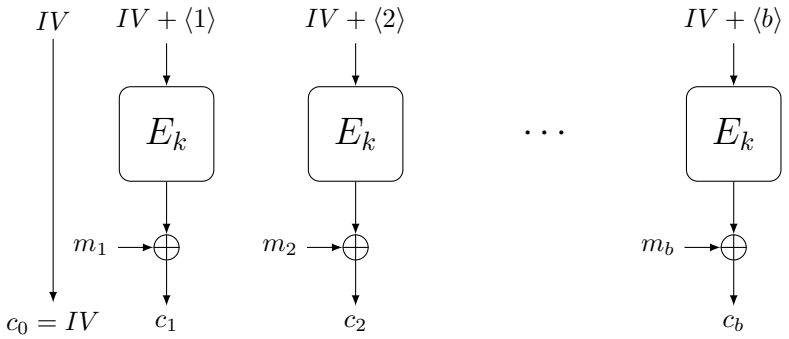
نکته ۲ *در مد OFB نیازی به پد کردن پیام نیست، زیرا می‌توان به تعداد لازم از بیت‌های آخرین قالب دنباله شبه‌تصادفی بُرید*[۱۱] *و برای رمز کردن آخرین بیت‌های پیام که تشکیل یک قالب کامل نمی‌دهند استفاده کرد.*

۴ روش شمارگر

روشی را که می‌خواهیم ارائه دهیم نسبت به روش CBC کمتر عمومیت دارد اما تعدادی مزیت نسبت به آن دارا می‌باشد. مد شمارگر، CTR[۱۲]، را همانند روش OFB می‌توان به صورت یک تولید کننده‌ی رشته تصادفی از یک رمز قالب در نظر گرفت. ابتدا یک بردار آغازین IV به صورت تصادف از $\{۰,۱\}^n$ انتخاب می‌شود و سپس محاسبات زیر صورت می‌گیرد:

$$c_i = m_i \oplus E(IV + \langle i \rangle),\ i = ۱, ۲, \cdots, b\,.$$

که $\langle i \rangle$ نمایش دودویی (مبنای دو) عدد i توسط یک رشته n-بیتی و $IV + \langle i \rangle$ جمع پیمانه‌ای به هنگ ۲^n می‌باشد که رشته‌های n بیتی به صورت عددی بین ۰ و $۲^n - ۱$ تفسیر می‌شوند.
متن رمز نهایی به صورت $c = \langle IV, c_۱, c_۲, \ldots, c_b \rangle$ می‌باشد (شکل ۶):



شکل ۶: رمزنگاری روش شمارگر

از مزیت های روش CTR می توان امنیت در مقابل حمله متن اصلی انتخابی، کاملاً موازی انجام شدن الگوریتم‌های رمزنگاری و رمزگشایی، و عدم نیاز به پدینگ متن اصلی را نام برد. همچنین این امکان را دارد که می تواند iامین قالب از متن رمزی را بدون رمزگشایی قالب‌های دیگر رمزگشایی کند. این ویژگی را دسترسی تصادفی می‌نامند.

قضیه ۳ *اگر E یک تابع شبه‌تصادفی باشد آنگاه روش شمارگر تصادفی، دارای امنیت متن اصلی انتخابی است.*

[۱۱] truncate
[۱۲] Counter (CTR) mode