

## مدلهای محکم در روش مالبر

در این بخش، سیوہ استفاده از روش‌های مالبر بر پایه‌های ماملول صفتی را صورت می‌گیرد و بر اساس هرچهاری دو قسم، در این راسته، چهار صور را از مدل‌های محکم در (modes of operation) را معرفی و در رابطه با آنها که چه خواصیم گز.

**یادآوری ۱:** پیام‌های با طول رله‌فاه رای توان با افنافر کردن یک عدد  $\frac{t}{n}$  و به تعداد کافی در انواعی آن، آنرا به طول صفتی از اندازه مالب مطلوب تبدیل کرد که به این عمل اصطلاحاً دیبالرزین (Padding) اطلاق می‌شود.

به طور دقیق تر از  $m_{10}^t = m_1 m_2 \dots m_n$  که رکمه رله‌فاه باشد، رسته پرسده به صورت  $m_{10}^t$  می‌باشد، حاصله  $t-1$  باید که صفتی عددی است که باز آن  $m_{10}^t$  صفتی  $n$  باید صورت کرده باشند تا بصورت زیر نشان داده شود:

$$m_{10}^t = m_1 m_2 \dots m_n, |m_i| = n \quad \text{for } 1 \leq i \leq b.$$

**یادآوری ۲:** برای بررسی صفتی مالبر امنیت هر یک از عدهای معرفی شده، می‌بایست سلسله‌ای از صورت اسنایزر دفعی سده را برائیم. بر این مبنای متفکر به طور خلاصه این مفاهیم را در ادامه معرفی کنیم

که تعریف امنیت عده است بر اساس یک مدل که در محتوا ر تعریف شود. در هر مدل که در می‌بایست دو حاکم رزیر در تظریز فتنه سود را

**۱- داشتن معاجم:** در روابط هف از عده را مسُفَعْتَه لذو  
تی توان آن را درین رسته بنیانی ملی به صورت  
از در تظریز فتنه:

**۱- بدست آوردن ملی:**

۱-۲: بدهست آکوردن صن اهلی برای مریو طلب کی متن رضی

۳-۱: بدهست آکوردن تا سه تا زمان اهلی برای مریو طلب کی متن رضی

۴-۱: بدهست آکوردن یک سیت لازم متن اهلی

۵-۱: تکمیل کننده همچنان از متن اهلی بدهست نیا مور (حین حزین)

۶: اطلاعات و متأثیه در اختیار محاجم است در واقع برای قدرت محاجم راشان می تدوین شود

مملوکیت در ردیف زیر تقسیم نباید شود

۷-۱: عذر متن رفیعها (COA): در این چهار محاجم تنها از امور سهای رشته کاری به  
مراد یک (یا چند) متن رضی آمده است.

۷-۲: عذر متن اکثار متأثیه شده (KPA): در این عذر محاجم علاوه بر اطلاعات اعلمه  
COA، یک یا چند حفظ متن اکثار و متن رفیع  
فعال آن را هم می داند

۷-۳: عذر متن اکثار انتخابی (CPA): در این چهار محاجم علاوه بر امور سهی رشته کاری،  
متن افزایشی مذکور یا یا چند متن اکثار مور  
نظر رایی توانند باشند باشد به عبارت اسرار  
یک باز و زمانی متفق هم کنند و متن رضی کاری را  
به صورت اراله در اختیار نمایند.

۷-۴: عذر متن رفیع انتخابی (CCA): مسایله مذکور عذر CPA ایت هایی تقدیر کر  
جارد مذکور ای ای هم ماسن امزی کاری را مقدم  
ای اکثر ب ماسن رضی که ای در انتخاب محاجم  
غیر دارد

۷-۵: عذر انتخابی (CA): مسایله مذکور عذر می باشد که کمی هم ب ماسن امزی کاری  
در مذکور ای را در انتخاب قرار دارد

جامعة رفیقاری مهواره تفاصیل برآن است که همچشم همچو بورس اطلاعی از من اهلی (حدی خوبی) بودست نیاز و دلایل برآری که طرح رفیقاری معمولی کانزراپتیو را درینجا راستا به بخوازید بکار گیرند  
برآن امنیت هنایس (semantic security) می‌گویند:

۱- همچشم رویام  $m_1, m_2$  باشد  $|m_1| = |m_2|$  (طول تکیان) رانتخابی شوند

۲- آریک پیام بر اشاره انتخاب  $m_1$  و سپس بررسی را فیلم  $E_{K_1}(m_1)$  و سپس  $E_{K_2}(m_2)$

۳- همچشم نتوانند  $E_{K_1}(m_1) \oplus E_{K_2}(m_2)$  را محمل کنند.

حینی که تمیز نکری جنس در

تمایز نایابی داشت

درین صورت می‌شون معمولی کانزراپتیو را بر همچشم با اطلاعات و منابع مختلف که درین طرح کاربری  
توسعه دار که به طور خلاصه به صورت زیری خود را دارد

۱ امنیت CPA: تمایز نایابی  $\neg K$ -پیام و حینه پیام / و همچنین بیانگر خودست پیام هست

حاجه که پیام و دورست پیام هر دست سابل حینه هست.

۲ امنیت KPA: تمایز نایابی  $+ (m_0, m_1, \dots, m_n, C_{n+1})$ .

۳ امنیت CPA: تمایز نایابی  $+ A$

۴ امنیت CCA: تمایز نایابی  $+ A$

۵ امنیت CA: تمایز نایابی  $+ A$

نکته: قدرتند  $\Rightarrow$  هر آن است که متن حالتی مجهودله را نیز توان در دسترس از افرادی به ماست

رفزشی موردا استفاده قرار دارد. دلیل این اصرارا برویم نهایت؟

سوال: آنایی توان در امنیت CPA، متن اصلی سوچور درست در را فیلم بعنوان منبع مخفیم را بخواهیم

حالی مطلع کرد؟ چرا؟

سوال: آنایی توان در امنیت CPA، متن اصلی مربوط به میانجی که برای اکل رفیقاری داشته اند را در بخواهیم

حالی مطلع کنیم؟ چرا؟

## ۲ مد کتاب الکترونیک

مد کتاب الکترونیک،  $ECB^*$ ، یکی از ساده‌ترین مدهای ممکن است که رمزگردن 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  $M10^t = m_1m_2 \dots m_b$  را به متن رمزی

$$c = \langle E_k(m_1), E_k(m_2), \dots, E_k(m_b) \rangle$$

کلاریس

تبديل می‌کند (شکل ۱).

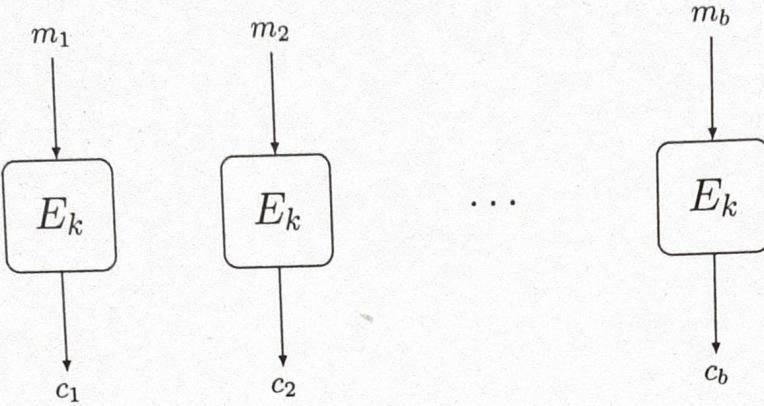
بارگذایی رمز نیز به صورت واضحی با استفاده از این حقیقت که<sup>۱</sup>  $E_k^{-1}$  به صورت می‌تواند قابل محاسبه است به دست می‌آید. البته باید توجه شود که رمزگذایی فقط در صورتی با موفقیت انجام می‌شود که رشته ورودی یک متن رمزشده معتبر باشد (یعنی، رمزشده یک متن اصلی باشد). به طور دقیق‌تر، برای رمزگذایی رشته<sup>\*</sup>  $c \in \{0, 1\}^n$  الگوریتم رمزگذایی ابتدا برسی می‌کند که  $|c|$  مضربی از  $n$  باشد. اگر نباشد<sup>۲</sup> برمی‌گرداند؛ در غیر این صورت، محاسبات زیر انجام می‌شود که  $c = c_1 \dots c_b$  و  $|c_i| = n$  :

<sup>1</sup>block ciphers

<sup>2</sup>modes of operation

<sup>3</sup>padding

<sup>4</sup>Electronic Code Book (ECB) mode



شکل ۱: مد کتاب الکترونیک (ECB)

$$m_i = E_k^{-1}(c_i) \quad \text{for } 1 \leq i \leq b.$$

سپس، اگر  $m_b$  یک بلوک تمام صفر باشد، الگوریتم رمزگشایی باز هم  $\perp$  بر می‌گرداند؛ در غیر این صورت، با حذف پدینگ متن  $M$  برگردانده می‌شود که  $m_b \dots m_1 M 10^t = m_1 m_2 \dots m_b$  و  $1 \leq t \leq n - 1$ .<sup>۵</sup>

فرآیند رمزگاری در این مورد قطعی<sup>۶</sup> (غیر احتمالی) 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 رمز شده وجود دارد. با استفاده از این مشاهده می‌توان یک مهاجم امنیت تک‌پیامی ارائه کرد. کافیست مهاجم پیام‌های  $c = \langle c_0, c_1, c_2 \rangle$  را (که دارای طول یکسان می‌باشند) به چالش‌گر فرستاده و پس از دریافت متن رمزی  $M_0 = 0^n 0^n$  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:

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

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

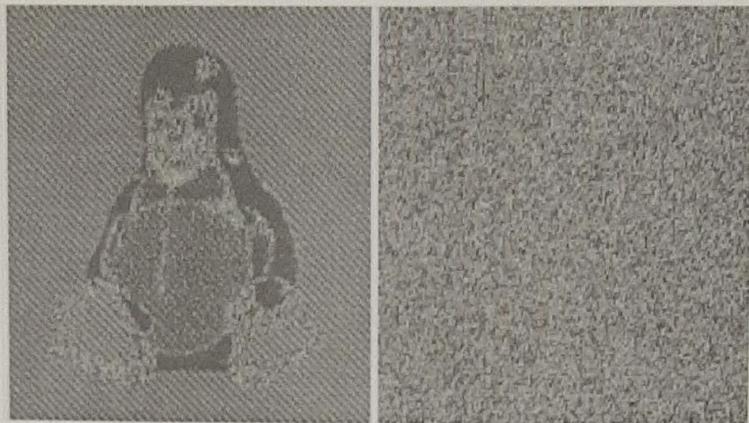
$$\Pr\{\text{Priv}_{\mathcal{A}, \Pi}^{\text{eav}} = 1\} = 1.$$

بنابراین برای مد کتاب الکترونیک (ECB)، اطلاعات زیادی را می‌توان با مشاهده متن 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 حالی است که برای رمزگاری یک تصویر بیت‌مپ<sup>۷</sup> 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 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).

<sup>5</sup>deterministic

<sup>6</sup>bitmap image

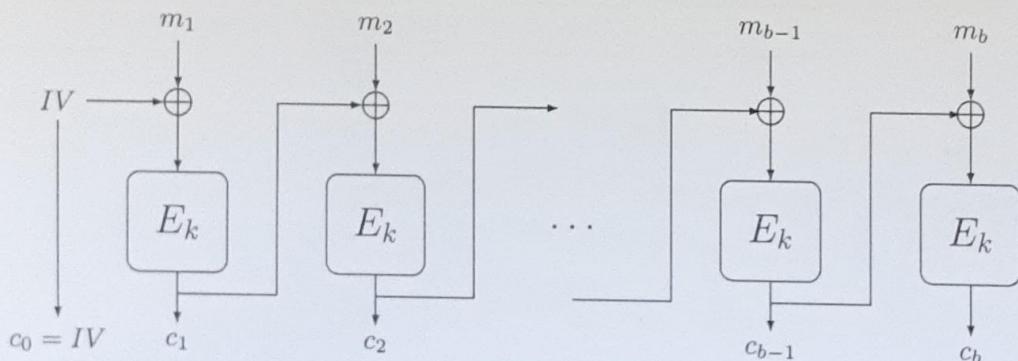


شکل ۲: [برگرفته از ویکی‌پدیا] یک تصویر بیت‌مپ و رمز شده آن با مد کتاب الکترونیک (شکل وسط) و یک مد امن (شکل سمت راست).

### ۳ مد زنجیری قالب رمز

در مد زنجیری قالب رمز<sup>۷</sup>, 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.

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



شکل ۳: روش زنجیری قالب رمز (رمزنگاری)

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

**سوال:** آفر IV در کد رمزگذاری ممکن است، هر سطح امنیت برقرار نماید؟

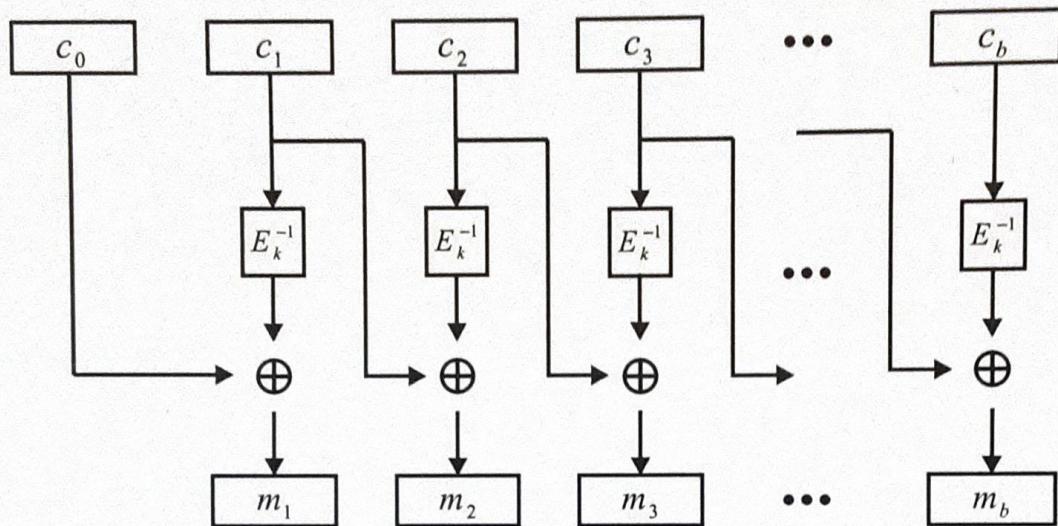
**سوال:** آفر IV ممکن است رمزگذاری اساس نیک نباشد، مقدار دهنده عینیت هرچیز هر سطح امنیت دارد.

<sup>7</sup>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 تا برگردانده می شود.



شکل ۴: روش زنجیری قالب رمز (رمزگشایی)

روش رمزگاری به روش  $CBC$  احتمالاتی است و می توان ثابت کرد که اگر  $E$  یک جایگشت شبه تصادفی باشد آنگاه روش  $CBC$  دارای امنیت در مقابل حمله متن اصلی انتخابی<sup>۸</sup> است.

قضیه ۱ اگر  $E$  یک جایگشت شبه تصادفی باشد، آنگاه روش  $CBC$  دارای امنیت متن اصلی انتخابی ( $CPA$ -secure) است.

مشکلات مد زنجیری قالب رمز. مهمترین اشکال این روش آن است که رمزگاری باید به طور متواالی 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 می شوند.

روش رمزگاری  $CBC$  دارای امنیت حمله متن رمزی انتخابی<sup>۹</sup> نمی باشد. مهاجم را به این صورت طراحی می کنیم. در آزمایش حمله متن رمزی انتخابی مهاجم دو پیام به صورت  $M_0 = 0^n$  و  $M_1 = 1^n$  به چالشگر می دهد. بیاد آورید که مهاجم دسترسی اوراکلی به الگوریتم رمزگاری و رمزگشایی دارد ولی مجاز به درخواست رمزگشایی متن رمزی چالشی  $c$  نمی باشد. به همین علت مهاجم با تغییر اندکی در آن، متن رمزی درخواستی  $\langle c_0 \oplus 1^n, c_1, c_2 \rangle = c'$  را به اوراکل رمزگشایی می فرستد و پس از دریافت پیام متناظر آن،  $M'$  بیت  $\hat{b}$  را به صورت زیر تولید می کند:

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

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

$$\Pr\{\text{PrivK}_{\mathcal{A}, \Pi}^{\text{cca}} = 1\} = 1 .$$

<sup>8</sup>Chosen-Plaintext Attack

<sup>9</sup>Chosen-Ciphertext Attack

## ۴ روش بازخورد خروجی

در اصل مد بازخورد خروجی<sup>۱۰</sup> (OFB) روشی برای تولید یک رشته شبه تصادفی 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  $c_0, z_1, \dots, c_b$  با شروع از  $z_0 = IV$  با استفاده از رابطه بازگشته

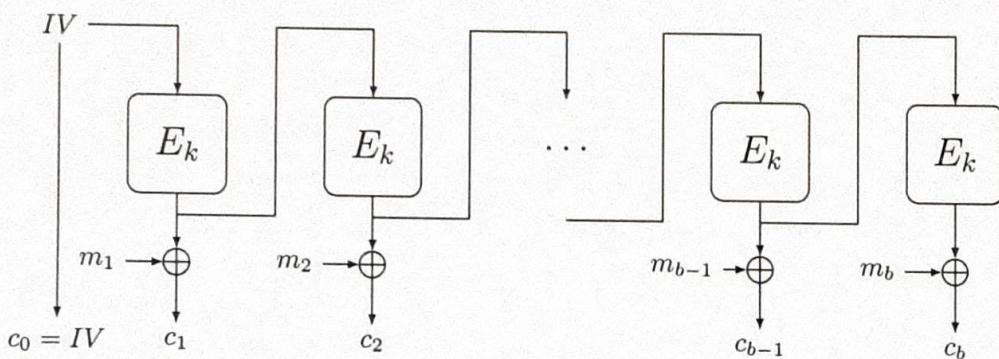
$$z_i = E(z_{i-1}), i = 1, 2, \dots, b$$

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):

$$c_i = m_i \oplus z_i, i = 1, 2, \dots, b.$$

و سرانجام متن رمزی به صورت نهایی زیر حاصل می‌شود:

$$c = \langle IV, c_1, \dots, c_b \rangle.$$



شکل ۵: رمزگاری روش تغذیه خروجی (رمزگاری)

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 شبه تصادفی نیز به جای یک جایگشت شبه تصادفی می‌توان استفاده کرد. در این روش نیز هر دو الگوریتم رمزگاری و رمزگشایی باید به صورت متواالی انجام شوند، در نتیجه این مد نیز قابلیت پردازش موازی را ندارد.

قضیه ۲ اگر  $E$  یک تابع شبه تصادفی باشد، آنگاه روش OFB دارای امنیت متن اصلی انتخابی (CPA-secure) است.

نکته ۲ در مد OFB نیازی به پد کردن پیام نیست، زیرا می‌توان به تعداد لازم از بیت‌های آخرین قالب دنباله شبه تصادفی تبرید<sup>۱۱</sup> و برای رمز کردن آخرین بیت‌های پیام که تشکیل یک قالب کامل نمی‌دهند استفاده کرد.

## ۵ 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<sup>۱۲</sup> (CTR) را همانند روش OFB می‌توان به صورت یک تولید کننده‌ی رشته تصادفی از یک رمز قالبی در نظر گرفت. ابتدا یک بردار آغازین  $IV$  به صورت تصادف از  $\{0, 1\}^n$  انتخاب می‌شود و سپس محاسبات زیر صورت می‌گیرد:

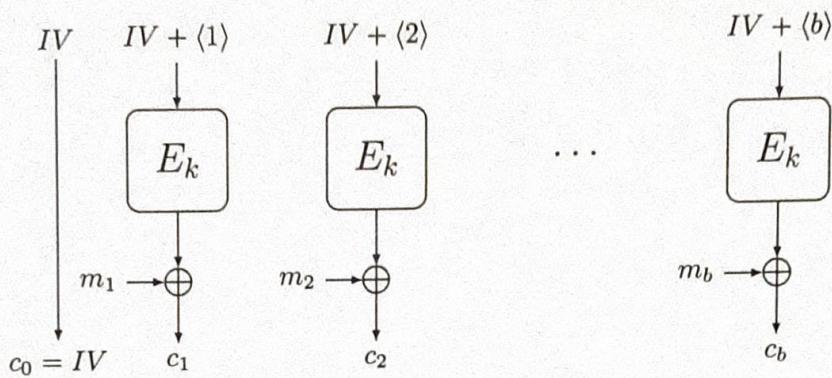
$$c_i = m_i \oplus E(IV + \langle i \rangle), i = 1, 2, \dots, b.$$

<sup>10</sup>Output Feedback (OFB) mode

<sup>11</sup>truncate

<sup>12</sup>Counter (CTR) mode

که  $\langle i \rangle$  نمایش دودویی (مینای دو) عدد  $i$  توسط یک رشته  $n$ -بیتی و  $\langle i \rangle + IV$  جمع پیمانه‌ای به هنگ  $2^n$  می‌باشد که رشته‌های  $n$  بیتی به صورت عددی بین  $0$  و  $2^n - 1$  تقسیم شوند. متن رمزنهایی به صورت  $c = \langle IV, c_1, c_2, \dots, c_b \rangle$  می‌باشد (شکل ۶).



شکل ۶: رمزگاری روش شمارگر

از مزیت‌های روش  $CTR$  می‌توان امنیت در مقابل حمله متن اصلی انتخابی، کاملاً موازی انجام شدن الگوریتم‌های رمزگاری و رمزگشایی، عدم نیاز به پدینگ متن اصلی را نام برد. همچنین این امکان را دارد که می‌تواند نامین قالب از متن رمزی را بدون رمزگشایی قالب‌های دیگر رمزگشایی کند. این ویژگی را دسترسی تصادفی می‌نامند.

قضیه ۳ اگر  $E$  یکتابع شبه‌تصادفی باشد آنگاه روش شمارگر، دارای امنیت متن اصلی انتخابی ( $CPA\text{-secure}$ ) است.