به نام آن که هیچ رمزی برایش پوشیده نیست

تمرین سری ۴ رمزنگاری

دانشکده ریاضی، آمار و علوم کامپیوتر

رمزنگاری-ترم اول سال تحصیلی ۹۵-۹۴

تاریخ تحویل: دوشنبه ۹۴/۰۹/۲۳

سؤال ۱

۱. فرض کنید $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ جایگشت شبه تصادفی امن باشد، آیا سیستم رمزنگاری $(Enc_k(m) = F_k(m), Dec_k(c) = F_k^{-1}(c))$ cpa -امن است؟(دلیل بیاورید)

۲. نشان دهید اگر الگوریتم رمزنگاری قطعی باشد آن‌گاه سیستم مورد نظر cpa -امن نخواهد بود.

سؤال ۲

فرض کنید مهاجم متن رمز شده‌ی زیر را رهگیری کند: (کد شده به صورت هگزادسیمال)

20814804c1767293b99f1d9cab3bc3e7
ac1e37bfb15599e5f40eef805488281d

فرض کنید او بداند که پیام اصلی متناظر با متن رمز شده فوق کد اسکی رشته‌ی ((Pay Bob 100 $)) باشد، همچنین او می‌داند که سیستم رمزنگاری از نوع CBC بوده و رمزقالبی مورد استفاده AES بوده. نشان دهید که مهاجم می‌تواند متن رمز شده را طوری تغییر دهد که حاصل رمزگشایی عبارت زیر باشد:

Pay Bob 500 $

و متن رمز شده مورد نظر را بدست آورید. این نشان می‌دهد که با استفاده از مد کاری CBC نمی‌توان جامعیت و یا درستی پیام را سنجید.

سؤال ۳

می‌دانیم که به کار بردن رمزهای قالبی به روش CBC امنیت CPA را فراهم می‌کند، نشان دهید در این حالت امنیت CCA (متن رمز شده انتخابی) فراهم نمی‌شود. (راهنمایی: در $CCA - Security$ فرض بر این است که مهاجم به الگوریتم‌های رمزنگاری و رمزگشایی دسترسی اوراکلی دارد فقط مجاز به درخواست رمزگشایی متن رمز چالشی که چالشگر برای او فرستاده نیست، این یعنی هر پیام را می‌تواند رمزکرده و یا

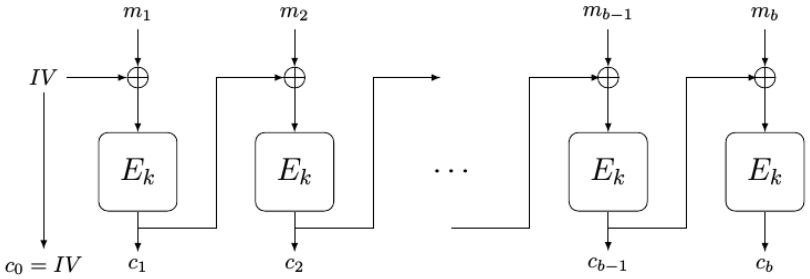
رمزگشایی کند جز رمزی که چالشگر برای او فرستاده است) روش رمزنگاری مورد استفاده در این سؤال به صورت دقیق در زیر شرح داده شده:

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. به این عمل پدینگ [۱] گفته می‌شود. به عبارت دیگر اگر $M \in \{0,1\}^*$ یک رشته به طول دلخواه از فضای پیام باشد، رشته پد شده به صورت $M10^t$ می‌باشد که $0 \leq t \leq n-1$ کوچکترین عددی است که به ازای آن $|M10^t|$ مضرب n است که ما آن را به صورت زیر نشان می‌دهیم:

$$M10^t = m_1 m_2 ... m_b \qquad |m_i| = n$$

تصویر مد کاری CBC با طول قالب n در زیر نشان داده شده است.

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

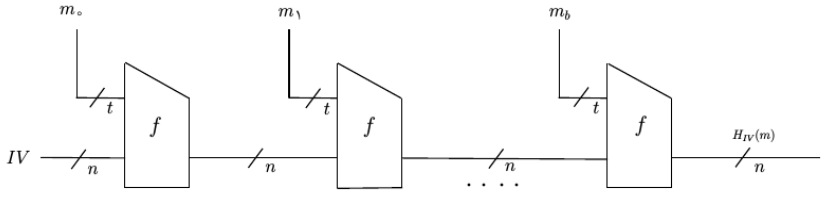


شکل ۱: مد زنجیری قالب رمز

سؤال ۴

فرض کنید f در برابر برخورد مقاوم باشد و $m10^* = m_1 m_2 ... m_b$ گسترش یافته‌ی پیام وردی باشد طوری که طول هر m_i برابر t باشد آیا تابع چکیده سازی که به صورت زیر ساخته‌ایم در برابر برخورد مقاوم است؟ (حدس خود را اثبات کنید)

IV یک مقدار ثابت است و تابع $H_{IV}(m)$ به شکل زیر است: دقت کنید عمل padding پیام ورودی



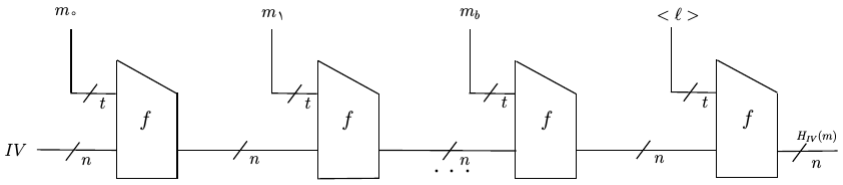
شکل ۲: $H_{IV}(m)$

به صورت پیش فرض انجام می‌شود حتّی اگر طول پیام ورودی از همان آغاز مضربی از t باشد.

[۱] padding

سؤال ۵

فرض کنید f در برابر برخورد مقاوم باشد تابع چکیده‌ساز $H_{IV}(m)$ را به همان شکلی که در سؤال ۴ ذکر شد می‌سازیم با این تفاوت که یک بلوک به انتهای آن اضافه می کنیم و ورودی آن بلوک را طول پیام در نظر می‌گیریم (البته فرض کرده‌ایم طول پیام‌های ورودی حداکثر 2^t باشد تا برای نمایش طول پیام حداکثر t بیت نیاز باشد. t طول قالب است.) پیام ورودی m به صورت $m1\circ^* < l >= m_1 m_2 ... m_b m_{b+1}$ که l نشان دهنده‌ی طول پیام اصلی است، پد شده و وارد الگوریتم می‌شود. نمودار زیر روش کار تابع چکیده ساز را نشان می‌دهد:



شکل ۳: $H_{IV}(m)$

آیا تابع چکیده ساز فوق در مقابل برخورد مقاوم است؟ (حدس خود را اثبات کنید)

سؤال ۶

سناریویی را در نظر بگیرید که فردی ادعا می‌کند که نتیجه قطعی انتخابات آتی را می‌داند و قصد دارد ضمن اثبات این موضوع به همگان، هیچ موجودی تا قبل از انتخابات از پیش بینی وی مطلع نشود پروتوکولی طراحی کنید که در آن فرد مورد نظر بتواند به هدف خود دست یابد. (راهنمایی: از توابع چکیده ساز استفاده کنید.)

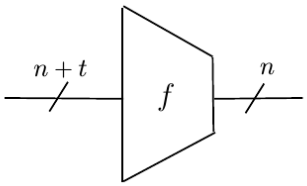
سؤال ۷

وجود تابع چکیده ساز مقاوم در برابر برخورد هنوز ثابت نشده است! همچنین وجود توابع رمزنگاری امن و کارا نیز ثابت نشده، با این همه امکان ساخت توابع چکیده ساز از روی تابع فشرده سازی که علی الظاهر در برابر برخورد مقاوم باشد وجود دارد. از طرفی امکان ساخت تابع فشرده ساز از روی تابع رمزنگاری که علی الظاهر امن باشد میسر است. توابع فشرده ساز توابعی هستند که ورودی با طول ثابت را به خروجی با طول ثابت ولی کوچکتر می‌نگارند (شکل ۴) توابع فشرده ساز نیز باید در برابر برخورد مقاوم باشند. فرض کنید $Enc_k(.)$ یک الگوریتم رمزنگاری امن باشد، در مورد برخورد تابی (مقاوم بودن در برابر برخورد) توابع فشرده ساز زیر بحث کنید.

۱. $H(k||m) = Enc_k(m)$

۲. $H(k||m) = Enc_k(m) \oplus m$

۳. $H(k||m) = Enc_k(m \oplus k) \oplus m$



شکل ۴: تابع فشرده ساز

سؤال ۸

در حمله روز تولّد به توابع چکیده ساز تا آن‌جا که زمان و فضا اجازه می‌دهد مقادیر درهم (چکیده) محاسبه کرده و این مقادیر به همراه پیش تصویرشان را مرتب کرده و در یک جدول ذخیره می‌کنیم، سپس در جدول مذکور به دنبال یک برخورد می‌گردیم. فرض کنید $h : \{۰,۱\}^* \to \{۰,۱\}^n$ یک تابع چکیده ساز باشد و مقادیر $\{۰,۱\}^*$ را می‌توان طوری تعیین کرد که توزیع مقادیر درهم متناظر یکنواخت باشد. حداقل تعداد اعضای $\{۰,۱\}^*$ که باید چکیده‌ی آن‌ها محاسبه شود تا با احتمال بزرگتر یا مساوی $\frac{۱}{۲}$ یک برخورد پیدا کنیم را بدست آورید. (جواب را به صورت پارامتری بر حسب n محاسبه کنید.)

سؤال ۹

فرض کنید $h : \mathcal{X} \to \mathcal{Y}$ یک تابع چکیده ساز باشد و $|\mathcal{X}| = N, |\mathcal{Y}| = M$ قرار می‌دهیم:

$$S = |\{\{x_۱, x_۲\} : h(x_۱) = h(x_۲)\}|.$$

و برای هر $y \in \mathcal{Y}$ فرض کنید $s_y = |h^{-۱}(y)|$ (در واقع S برابر تعداد زوج‌های نامرتب در $\mathcal{X}$ است که تحت h برخورد می‌کنند.)

۱. نشان دهید که

$$\sum_{y \in \mathcal{Y}} s_y = N,$$

که این یعنی میانگین s_y ها برابر است با

$$\overline{s} = \frac{N}{M}$$

۲. ثابت کنید که:

$$S = \sum_{y \in \mathcal{Y}} \binom{s_y}{۲} = \frac{۱}{۲} \sum_{y \in \mathcal{Y}} s_y^۲ - \frac{N}{۲}$$

۳. نشان دهید:

$$\sum_{y \in \mathcal{Y}} (s_y - \overline{s}) = ۲S + N - \frac{N^۲}{M}$$

۴. با استفاده از نتیجه بدست آمده در قسمت قبل نشان دهید:

$$S \geq \frac{۱}{۲}(\frac{N^۲}{M} - N).$$

همچنین ثابت کنید تساوی برقرار است اگر و تنها اگر:

$$s_y = \frac{N}{M}$$

سؤال ۱۰

h را تابع چکیده ساز سؤال ۹ در نظر بگیرید و فرض کنید ϵ نشان‌دهنده احتمال $h(x_۱) = h(x_۲)$ ، وقتی که $x_۱$ و $x_۲$ به صورت تصادفی از $\mathcal{X}$ (و نه لزوما متمایز) انتخاب می‌شوند باشد. ثابت کنید:

$$\epsilon \geq \frac{۱}{M}$$

و تساوی برقرار است اگر و تنها اگر

$$\forall y \in \mathcal{Y} \qquad |h^{-۱}(y)| = s_y = \frac{N}{M}$$