به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری	دانشجو: علیرضا توفیقی محمدی
تمرین : سری ۲	
مدرّس: دکتر شهرام خزائی	شماره‌ی دانشجویی: ۹۶۱۰۰۳۶۳

مسأله‌ی ۱

هیچ کدام خوب نیست،
اولا هر الگوریتم رمزنگاری که بخواهد امنیت کامل را داشته باشد، لازم است اندازه‌ی فضای cipther-text از متن اصلی بیشتر باشد، همچنین در الگوریتم‌های معمول رمزنگاری سعی بر این است که متن رمزشده تاجای ممکن به یک متن رندم شبیه باشد و این دو توزیع PPT یکسان داشته‌باشند، پس رمزنگاری و سپس کامپرس کردن در مورد اول می‌تواند باعث کاهش امنیت و در مورد دوم اصلا کارا نیست.
همچنین ابتدا فشرده‌سازی و سپس رمزنگاری نیز می‌تواند باعث لو رفتن برخی از اطلاعات رمز اصلی شود.
می‌دانیم که طول پیام را به سادگی نمی‌توان مخفی نگه داشت، حال چون الگوریتم‌های فشرده‌سازی براساس پیام اصلی طول‌های مختلفی را می‌سازند (رشته‌های کاملا رندم را قادر به فشرده‌سازی نیستند و رشته‌های واقعی را فشرده‌تر می‌کنند.) پس یک متن کاملا رندم و یک متن غیررندم قابل تشخیص هستند و امنیت آن زیر سوال می‌رود.

مسأله‌ی ۲

برای حل مسئله می‌دانیم اگر m_1, m_2 دو متن اصلی باشند که با کلید k از طریق رمز OTP رمز شده‌باشند و رمزشده‌ي آن‌ها به ترتیب c_1, c_2 باشد، آنگاه:

$$m_1 \oplus m_2 = c_1 \oplus c_2$$

از همین ویژگی برای حدس c_2 استفاده می‌کنیم. داریم:

$$m_1 = 61747461636b206174206461776e, m_2 = 61747461636b2061742064475736b$$

$$\implies m_1 \oplus m_2 = 140405$$

حال از طرفی داریم:

$$m_1 \oplus m_2 = c_1 \oplus m_2 \implies c_2 = m_1 \oplus m_2 \oplus c_1$$

$$\implies c_2 = 140405 \oplus 09e1c5f70a65ac519458e7e53f36 = 09e1c5f70a65ac519458e7f13b33$$

مسأله‌ی ۳

آ)

برای اثبات کافی است ثابت کنید برای هر $m \in M, c \in C$ داریم:

$$Pr\{C = c|M = m\} = Pr\{M + K = c|M = m\} = Pr\{K = c - m\} = \frac{1}{|K|}$$

مشاهده می‌شود که متن رمزی مستقل از متن اصلی دارای توزیع یک‌نواخت است.

ب)

طبق قضیه‌ی شانون برای اینکه یک سیستم رمز امنیت کامل داشته‌باشد باید $|K| \leq |M|$.
پس تنها کلمات یک حرفی با کلید یک‌حرفی قادر به داشتن امنیت کامل هستند.

ج)

اولا طبق قضیه‌ی شانون باید اندازه‌ی فضای کلید به اندازه‌ی فضای متن اصلی باشد، پس طول کلید باید حداقل n باشد. همچنین کلید به طول n امنیت کامل را رقم می‌زند زیرا برای هر $m = m_1m_2...m_n \in M$ و $c = c_1c_2...c_n \in C$ داریم:

$$Pr(C = c|M = m) = Pr(c = (m_1 + K_1)(m_2 + K_2)...(m_n + K_n)|M = m_1m_2...m_n)$$

$$= Pr(K = (c_1 - K_1)(c_2 - K_2)...(c_n - K_n)) = \frac{1}{|K|}$$

که متن رمزی مستقل از متن اصلی دارای توزیع یک‌نواخت است، پس دارای امنیت کامل است.
(دقت کنید منظور از جمع و منهاها در این پاسخ سوال جمع و تفریق در پیمانه‌ی ۲۶ است.)

مسأله‌ی ۴

اولا اگر سیستمی امنیت کامل داشته باشد، یعنی به ازای هر $c \in C$ و $m_1, m_2 \in M$ داریم:

$$Pr[C = c|M = m_1] = Pr[C = c|M = m_2]$$

پس هیچ حمله‌کننده‌ای نمی‌تواند با احتمال بهتر از $\frac{1}{2}$ تشخیص دهد c رمزشده‌ی m_1 است یا m_2.
همچنین اگر سیستمی امنیت کامل در آزمایش تشخیص داشته‌باشد، یعنی هر حمله‌کننده‌ای در نظر بگیریم، احتمال درست گفتنش $\frac{1}{2}$ است.
حال به ازای هر $c \in C$ و $m_1, m_2 \in M$، حمله‌کننده‌ی $A_{m_1,m_2,c}$ را به این گونه تعریف می‌کنیم که دو متن m_1, m_2 را می‌دهد، حال اگر چالشگر رمز c را داد، حمله‌کننده یک و در غیر اینصورت یک عدد تصادفی از ۰ و ۱ را برمی‌گرداند.
می‌دانیم طبق فرض احتمال درست گفتن این حمله‌کننده نیز $\frac{1}{2}$ است. از طرفی فرض کنید احتمال اینکه چالشگر رمز c را در صورت گرفتن m_1, m_2 بدهد p باشد، در این صورت برای احتمال درست گفتن حمله کننده داریم:

$$p * \frac{Pr[C = c|M = m_1]}{Pr[C = c|M = m_1] + Pr[C = c|M = m_2]} + (1 - p) \times 0.5 = \frac{1}{2}$$

$$\implies \frac{Pr[C = c|M = m_1]}{Pr[C = c|M = m_1] + Pr[C = c|M = m_2]} = \frac{1}{2}$$
$$\implies Pr[C = c|M = m_1] = Pr[C = c|M = m_2]$$

اگر $p \neq 0$ می‌توان نتیجه‌ی بالا را گرفت، همچنین داریم:

$$p = \frac{Pr[C = c|M = m_1] + Pr[C = c|M = m_2]}{2}$$

پس اگر $p = 0$ شود، آنگاه هر دو احتمال برابر با صفر می‌شود و این حالت نیز حل می‌شود.
پس طبق استدلال بالا به ازای هر m_1, m_2, c ثابت شد $Pr[C = c|M = m_1] = Pr[C = c|M = m_2]$ و در نتیجه امنیت کامل داریم.

مسأله‌ی ۵

آ)

می‌توان تعریف را به شکل زیر ارائه داد:

$$\forall A(\text{which is PPT}):$$

$$Pr[(pk, sk) \leftarrow Gen(1^n); m \leftarrow M; c \leftarrow Enc_{pk}(m); A(pk, c) = m] \leq \frac{1}{|M_n|}(1 + \epsilon(n))$$

که ϵ یک تابع ناچیز است.

ب)

برای اینکار فرض می‌کنیم حمله‌کننده A وجود دارد که pk, c را گرفته و با احتمال بیشتر از $\frac{1}{|M_n|}(1 + \epsilon(n))$ به ازای هر تابع ناچیزی ϵای درست حدس می‌زند.
حال یک حمله کننده مثل A' برای مسئله‌ی DDH می‌سازیم، برای اینکار اگر A' ورودی G, q, g, u, v, w را گرفت، مقادیر زیر را بسازد:

$$pk = (u, G, q, g)$$

$$m \leftarrow M$$

$$c = (v, m.w)$$

$$m' = A(pk, c)$$

حال اگر $m' = m$ بود، یک را بر میگرداند و در غیر اینصورت یک عدد تصادفی از ۰ و ۱ برمی‌گرداند.
حال احتمال درست حدس زدن را حساب می‌کنیم:

$$Pr > \frac{1}{2} \times (\frac{1}{|M_n|}(1 + \epsilon(n)) + \frac{1}{2} \times (1 - \frac{1}{|M_n|}(1 + \epsilon(n))))$$

$$+\frac{1}{2} \times (\frac{1}{q} \times (\frac{1}{|M_n|}(1 + \epsilon(n)) + \frac{1}{2} \times (1 - \frac{1}{|M_n|}(1 + \epsilon(n)))) + \frac{q-1}{q} \times \frac{1}{2})$$

$$\geq \frac{1}{2}\left(\frac{1}{2} \times (1 + \frac{1}{|M_n|}(1 + \epsilon(n))) + \frac{1}{2}\right) = \frac{1}{2} + \frac{1}{4|M_n|}(1 + \epsilon(n))$$

مسأله‌ی ۶

درست نیست، اگر یک سیستم دارای امنیت کامل باشد و فضای آن بالای ۳ عضو داشته باشد، برای هر توزیع M و برای $m \in M, c \in C$ باید شرط زیر برقرار باشد:

$$Pr\{M = m|C = c\} = Pr\{M = m\}$$

حال سه عضو دلخواه M مثل m_1, m_2, m_3 را در نظر بگیرید و فرض کنید توزیع M به این حالت است که

$$Pr\{M = m_1\} = Pr\{M = m_3\} = \frac{1}{2}, Pr\{M \notin \{m_1, m_3\}\} = 0$$

اما با توزیع داریم:

$$Pr\{M = m_1|C = c\} = Pr\{M = m_1\} = \frac{1}{2}$$
$$Pr\{M = m_2|C = c\} = Pr\{M = m_1\} = 0$$

پس

$$Pr\{M = m_1|C = c\} \neq Pr\{M = m_2|C = c\}$$

پس حکم برقرار نیست.

مسأله‌ی ۷

اگر $|M| = |C| = 1$ حکم سوال برقرار نیست و سیستم رمزی داریم که امنیت کامل دوپیامه را دارد.
اما اگر $|M| > 1$:
فرض کنید $k \in K$ کلیدی دلخواه است و همچنین $m_1 \in M$ نیز پیامی دلخواه است.
حال مجموعه مقادیر ممکن برای $Enc_k(m_1)$ را D بنامید. ادعا می‌کنیم $C - D \neq \emptyset$. زیرا طبق شرط صحت $Pr[Dec_k[Enc_k(m_1)] = m_1] = 1$ و در نتیجه: $\forall d \in D : Pr[Dec_k[d] = m_1] = 1$
و اگر $C = D$ باشد، آنگاه شرط صحبت برای بقیه‌ی اعضای M نقض می‌شود.
حال $c_2 \in C - D$ و $c_1 \in D$ در نظر بگیرید که $Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$. (این کار قابل انجام است زیرا c_2 را می‌توان برای $m \in M, m \neq m_1$ یکی از مقادیر $Enc_k(m)$ در نظر گرفت.)
حال $m_2 = m_1$ در نظر بگیرید؛ ادعا می‌کنیم m_1, m_2, c_1, c_2 ساخته‌شده شرایط مسئله را نقض می‌کنند. زیرا از طرفی

$$Pr[M_1 = m_1 \wedge M_2 = m_2] \neq 0$$

است و از طرفی چون $c_2 \notin D$ و در نتیجه احتمال $Pr[M_2 = m_2 \wedge C_2 = c_2] = 0$ است، پس:

$$Pr[M_1 = m_1 \wedge M_2 = m_2|C_1 = c_1 \wedge C_2 = c_2] = 0$$

پس حکم سوال برای هر سیستم رمز دلخواهی نقض می‌شود.

مسأله‌ی ۸

برای اثبات وجود چنین سیستم رمزی، کافی است سیستم رمزی مانند OTP که امنیت کامل دارد را در نظر بگیریم، اما در کلید آن به جای ساختن کلید n بیتی، یک کلید $n-t$ بیتی بسازیم. سپس در فرایند رمزنگاری و بازگشایی رمز، ابتدا یک رشته‌ی t بیتی تصادفی ساخته و کلید کاری خود را با کنار هم قرار دادن کلید اصلی و رشته‌ی تصادفی در نظر بگیریم و فرایند XOR را با آن انجام دهیم.
در این صورت اندازه‌ي فضای کلید برابر با $\frac{|M|}{2^t}$ خواهد شد، همچنین مشابه استدلال برای OTP دارای امنیت کامل است.
همچنین شرط صحت جدید را دارد، زیرا به احتمال 2^{-t} رشته‌ی تصادفی در الگوریتم رمزنگاری و رمزگشایی یکسان شده و طبق شرط صحت OTP با این شرط به احتمال یک رمزنگاری ورمزگشایی همانی جواب می‌دهد. پس احتمال اینکه رمزنگاری و رمزگشایی با یک کلید همانی جواب دهد حداقل 2^{-t} است.
همچنین باند آن $\frac{|M|}{2^t}$ است که اثباتی برای آن ندارم.

مسأله‌ی ۹

مسأله‌ی ۱۰

آ)

$$Dec_{k_0||k_1}(c_0||c_1) = \begin{cases} k_0 \oplus c_0, & \text{if } k_0 \oplus c_0 = k_1 \oplus c_1 \\ \perp, & \text{otherwise} \end{cases}$$

ب)

بله، داریم:

$$Pr[C=00|M=0] = Pr[C=11|M=0] = Pr[C=00|M=1] = Pr[C=00|M=1] = \frac{1}{3}$$

$$Pr[C=01|M=0] = Pr[C=10|M=0] = Pr[C=01|M=1] = Pr[C=10|M=1] = \frac{1}{6}$$

پس:

$$\forall c \in C, m \in M : Pr[C = c | m = m] = Pr[C = c]$$

و طبق لم ۱ از جزوه امنیت کامل داریم.

مسأله‌ی ۱۱

مسأله‌ی ۱۲

مسأله‌ی ۱۳

مسأله‌ی ۱۴

از فرض‌های کتاب می‌دانیم که فضای کلید متناهی است، همچنین چون طبق قضیه‌ی شانون برای برقرار امنیت کامل باید $|M| \geq |K|$ باشد، پس فضای پیام نمی‌تواند نامتناهی باشد.

مسأله‌ی ۱۵

اگر حمله‌کننده‌ای وجود داشته باشد که بتواند آزمایش دوم را با احتمال بهتر از نصف به‌اضافه‌ی هر تابع جزئی حل کند، آنگاه حمله‌کننده‌ای وجود دارد که m_0, m_1 را به شکل قطعی انتخاب می‌کند و بازهم از آزمایش دوم با موفقیت بیرون می‌آید (به این شکل که یکی از حالت‌های انتخاب تصادفی m_0, m_1 از حمله کننده‌ی نخست این ویژگی را دارد.)
این m_0, m_1 ویژگی اول را ندارند.
حال اگر m_0 و m_1 ای وجود داشته باشند که قابل تشخیص محاسباتی باشند، حمله‌کننده‌ای می‌سازیم که همین m_0, m_1 را انتخاب می‌کنند و از روش تشخیص محاسباتی m_0, m_1 چالش را با advantage غیر ناچیز پاسخ می‌دهد.

مسأله‌ی ۱۶

در تعریف اول، m_0, m_1 در واقع دنباله‌هایی از متن‌های اصلی هستند (به ازای هر n یک متن اصلی). پس تعداد کل m_0, m_1ها ناشمارا است، همچنین چون هر حمله کننده را می‌توان با یک الگوریتم نشان داد و تعداد الگوریتم‌ها شمارا است، پس m_0, m_1 ای وجود دارد که هیچ حمله‌کننده‌ای قادر با ساختن آن‌ها نیست. با این حساب کافی‌است سیستم رمزی بسازیم که برای این m_0, m_1 قابل تشخیص و برای بقیه غیرقابل تشخیص باشد.