به نام آن که هیچ رمزی برایش پوشیده نیست

تمرین سری ۷ رمزنگاری

دانشکده ریاضی، آمار و علوم کامپیوتر

رمزنگاری-ترم اول سال تحصیلی ۹۵-۹۴

تاریخ تحویل: یکشنبه ۹۴/۱۰/۲۰

۷ سؤال به دلخواه انتخاب نموده و حل نمایید

سؤال ۱

فرض کنید G یک گروه دوری متناهی با مولّد g باشد و محاسبه‌ی تابع دیفی-هلمن یعنی $DH_g(g^x, g^y)$ وقتی x, y به تصادف از $Z_{|G|}$ انتخاب می‌شوند سخت باشد. با این فرض سختی محاسبه هر یک از توابع زیر را بررسی کنید.

۱. $f(g^x, g^y) = g^{x-y}$

۲. $f(g^x, g^y) = g^{۲xy}$

۳. $f(g^x, g^y) = \sqrt{g^{xy}}$

۴. $f(g^x, g^y) = g^{x+y}$

در صورتی که حدس می‌زنید محاسبه تابع سخت است با تکنیک $reduction$ حدس خود را اثبات کنید.

سؤال ۲

سیستم رمز زیر که یکی از انواع رمز الجمال است را در نظر بگیرید:

۱. الگوریتم تولید کلید
$(G, q, g) \leftarrow \text{GroupGen}(۱^n)$ در این مرحله یک گروه دوری از مرتبه q و مولّد g تولید می‌شود.
$x \leftarrow \mathbb{Z}_q$
محاسبه $h = g^x$
$pk = (G, g, q, h)$
$sk = (G, g, q, x)$

۲. الگوریتم رمزنگاری
پیام‌ها از فضای G می‌آیند
ابتدا یک عدد تصادفی از Z_q انتخاب می‌کنیم.
$< g^r, mh^r > \leftarrow Enc_{pk}(m)$

۳. الگوریتم رمزگشایی
$Dec_{sk}(c_0, c_1) = c_1 c_0^{-x}$

- نشان دهید فضای متن رمزشده تشکیل یک گروه جبری می‌دهد.
- نشان دهید به ازای هر $m_1, m_2 \in G$ و هر زوج کلید $(pk, sk) \in \mathcal{K}$ داریم:

$$Enc_{pk}(m_1 m_2) = Enc_{pk}(m_1) Enc_{pk}(m_2)$$

- نشان دهید سیستم فوق فاقد امنیت CCA (از نوع کلید همگانی) است.

سؤال ۳

فرض کنید $N = pq$ که p, q اعداد اوّل هستند. می‌دانیم که اگر $x \in \mathbb{Z}_N^*$ و $ed = 1 \ mod \phi(N)$ آن‌گاه $(x^e)^d = x \ mod N$. نشان دهید این خاصیّت برای هر $x \in \mathbb{Z}_N$ هم برقرار است.
با این حال آیا لزومی دارد در الگوریتم رمزنگاری RSA ساده [1] پیام‌ها حتماً نسبت به پیمانه محاسبات $(N = pq)$ اوّل باشند؟ به عبارت دیگر لزومی دارد فضای پیام به جای Z_N برابر Z_N^* باشد؟

سؤال ۴

فرض کنید $\prod = (Gen, Enc, Dec)$ یک سیستم CCA -امن کلید همگانی روی فضای پیام $\{0,1\}^{128}$ باشد. کدامیک از سامانه‌های $\prod' = (Gen', Enc', Dec')$ زیر CCA -امن است؟

۱.
$$Enc'_{pk}(m) =< Enc_{pk}(m), Enc_{pk}(m) >$$
$$Dec'_{sk}(c_1, c_2) = \begin{cases} Dec_{sk}(c_1) & Dec_{sk}(c_1) = Dec_{sk}(c_2) \\ \perp & o.w \end{cases}$$

۲.
$$Enc'_{pk}(m) =< Enc_{pk}(m), Enc_{pk}(0^{128}) >$$
$$Dec'_{sk}(c_1, c_2) = \begin{cases} Dec_{sk}(c_1) & Dec_{sk}(c_1) = Dec_{sk}(0^{128}) \\ \perp & o.w \end{cases}$$

[1] Plain RSA

سؤال ۵

(به یاد اوّل ترم!)

فرض کنید آذر و بهرام در کشوری با ۵۰ استان زندگی می‌کنند. آذر هم‌اکنون در استان $a \in \{۱, ۲, ..., ۵۰\}$ و بهرام نیز در استان $b \in \{۱, ۲, ..., ۵۰\}$ است. آن‌ها می‌توانند با هم ارتباط برقرار کنند و آذر تمایل دارد که بداند آیا بهرام در همان استانی است که وی حضور دارد یا خیر؟!

اگر آذر و بهرام در یک استان باشند آذر متوجه می‌شود و در غیر این‌صورت آذر نباید از مکان بهرام مطّلع شود در ضمن در طول اجرای این تعامل یا ارتباط بین آن دو بهرام نباید هیچ اطلاعاتی از مکان آذر بدست آورد. آن‌ها به طریق زیر عمل می‌کنند:

۱. آن‌ها بر روی یک گروه G از مرتبه‌ی عدد اوّل p و مولّد g توافق می‌کنند.

۲. آذر که قصد دارد از مکان بهرام مطّلع شود اعداد $x, y \leftarrow \mathbb{Z}_p$ را به تصادف انتخاب کرده و مقدار زیر را برای بهرام ارسال می‌کند:

$$(A_۰, A_۱, A_۲) = (g^x, g^y, g^{xy+a})$$

۳. بهرام مقادیر تصادفی $r, s \leftarrow \mathbb{Z}_p$ را انتخاب کرده و مقدار زیر را برای آذر ارسال می‌کند:

$$(B_۱, B_۲) = (A_۱^r g^s, (\frac{A_۲}{g^b})^r A_۰^s)$$

- آذر چطور می‌تواند بفهمد که هر دو در یک استان هستند به عبارت دیگر آذر چطور درستی رابطه‌ی $a = b$ را بسنجد؟
- توضیح دهید چرا بهرام نمی‌تواند از مکان اذر مطّلع شود؟

سؤال ۶

می‌دانیم که در صورت داشتن زوج کلید (pk, sk) در سیستم RSA می‌توان پیمانه سیستم یا همان N را به صورت کارا تجزیه کرد. اکنون فرض کنید شرکتی بخواهد برای هر یک از کارمندانش یک زوج کلید خصوصی و عمومی متمایز در نظر بگیرد نشان دهید در این صورت هر یک از کارمندان می‌توانند پیام رمز شده کارمندان دیگر را رمزگشایی کنند و مطمئناً حریم خصوصی در این جا رعایت نمی‌شود!

سؤال ۷

۱. می‌دانیم که محاسبه‌ی $\phi(n)$ از تجزیه‌ی n آسان‌تر نیست، نشان دهید اگر در سیستم RSA حمله‌کننده $\phi(n)$ را بداند براحتی می‌تواند n را تجزیه کند.

۲. فرض کنید پیام m در سیستم RSA برای دو نفر با کلید همگانی‌های $(N, e_۱)$ و $(N, e_۲)$ رمز و ارسال شود. در ضمن فرض کنید $gcd(e_۱, e_۲) = ۱$ در این صورت چه تحدیدی از سوی مهاجمی که فقط توانایی شنود پیام‌های رمز و ارسال شده برای این دو نفر را دارد، متوجّه سیستم است؟ راه حلّ شما برای مقابله با این تحدید چیست؟

سؤال ۸

سرعت بخشیدن به رمزگشایی RSA

میدانیم که برای سرعت بخشیدن به رمزنگاری در سامانه کلید همگانی RSA معمولاً سعی می‌کنند کلید همگانی (e) را نسبت به کلید خصوصی کوچکتر بگیرند. پیشنهاد شما برای سرعت بخشیدن به الگوریتم رمزگشایی چیست؟ (راهنمایی: از قضیه‌ی باقی‌مانده چینی برای رمزگشایی استفاده کنید و به جای این که کلید خصوصی را (N, d) در نظر بگیرید، پارامترهای دیگری را به عنوان کلید خصوصی در نظر بگیرید و الگوریتم را به نحو مناسبی تغییر دهید) فرض کنید پیچیدگی عمل توان رسانی پیمانه‌ای در پیمانه‌ی یک عدد n بیتی از مرتبه‌ی $cn^۳$ به ازای یک عدد ثابت c باشد.

سؤال ۹

مدیر یک سیستم تصمیم دارد برای مدیریت کلید کاربران در سیستم RSA از روش زیر استفاده نماید:

او ابتدا پیمانه $N = pq$ را انتخاب کرده و $s \leftarrow \mathbb{Z}_N^*$ را در نظر می‌گیرد. سپس به کاربر شماره i کلیدی برابر با $s_i = s^{r_i}$ اختصاص می‌دهد که $i,\ r_i$ امین عدد اوّل است. فرض کنید او بخواهد اجازه‌ی دسترسی به یک فایل را به کاربرهای i, j و t بدهد، برای این کار عدد $k = s^{r_i r_j r_t}$ را به عنوان کلید فایل در نظر می‌گیرد و فایل را با k رمز می‌کند به این ترتیب کاربران مورد نظر براحتی می‌توانند فایل را رمزگشایی کنند. برای مثال اگر کاربر i بخواهد فایل را رمزگشایی کند کافی است تا مقدار $s_i^{r_j r_t}$ را محاسبه کند و کلید فایل را دست آورد. فرض بر این است که مدیر به کاربران اعتماد دارد و مطمئن است که آن‌ها با هم تبانی نخواهند کرد. اگر آن‌ها تبانی کنند چه خطری سامانه را تحدید می‌کند؟

مؤفّق باشید.

ح. هادی‌پور دستیار آموزشی درس رمزنگاری