به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری ۲۹ اردیبهشت ۱۳۹۲

جلسه‌ی ۲۲: سیستم‌های رمز نامتقارن RSA و الگمال

مدرس: دکتر شهرام خزائی *نگارنده: مریم غرقانی و محمدجواد اکبری*

۱ فرضیات رمزنگاری

در آغاز این جلسه به کمک چند فرض ذیل که در جلسات گذشته بدان‌ها پرداخته شد، به طراحی چند سیستم رمز کلید عمومی می‌پردازیم:

۱. **فرض تجزیه:** اگر p و q دو عدد اول تصادفی n بیتی باشند، آن‌گاه محاسبه p یا q از روی حاصل‌ضرب $N = pq$ سخت است.

۲. **فرض RSA:** محاسبه x از روی $x^e \mod N$ که N حاصلضرب دو عدد تصادفی n بیتی است و e به تصادف از $\mathbb{Z}^*_{\phi(N)}$ انتخاب می‌شود، سخت است.

۳. **فرض لگاریتم گسسته**[۱]**:** در گروه G با مولد g محاسبه $\log_g h$ از روی عنصر تصادفی $h \in G$ سخت است.

۴. **فرض دیفی-هلمن محاسباتی (CDH**[۲]**):** در گروه G با مولد g و مرتبه q، وقتی x و y به تصادف از $\mathbb{Z}_q$ انتخاب شوند، محاسبه‌ی g^{xy} از روی g^x و g^y سخت است.

۵. **فرض دیفی-هلمن تصمیمی (DDH**[۳]**):** در گروه G با مولد g و مرتبه q، دو توزیع (g^x, g^y, g^{xy}) و (g^x, g^y, g^r) وقتی که x, y, r به تصادف از $\mathbb{Z}_q$ تولید شود، تمایزناپذیرند.

۶. **فرض دیفی-هلمن چکیده‌ای (HDH**[۴]**):** در گروه G با مولد g و مرتبه q، وقتی x و y به تصادف از $\mathbb{Z}_q$ انتخاب شوند، دو توزیع $(g^x, g^y, H(g^{xy}))$ و (g^x, g^y, r) تمایزناپذیرند که تابع درهم‌سازی H یک اوراکل تصادفی و r یك مقدار تصادفی از برد H است.

نکته ۱ *فرض RSA برای حالتی بیان شده است که e به تصادف از $\mathbb{Z}^*_{\phi(N)}$ انتخاب شده باشد، ولی می‌توان RSA را برای e ثابت نیز مطرح کرد. مثلا می‌توان فرض کرد محاسبه ریشه سوم وقتی که $\gcd(3, \phi(N)) = 1$ مسئله سختی است.*

---

[۱] Discrete Logarithm Assumption
[۲] Computational Diffie-Hellman Assumption
[۳] Decisional Diffie-Hellman Assumption
[۴] Hash Diffie-Hellman Assumption

فرضیات فوق به صورت غیر رسمی ارائه شده اند، اما همه آنها را می‌توان به صورت رسمی بیان کرد. به عنوان مثال برای رسمی کردن فرض تجزیه می‌توان آزمایش زیر را تعریف کرد:

تعریف ۱ *آزمایش تجزیه* $\mathsf{Factor}_{\mathcal{A}}(n)$ *به صورت زیر است:*

۱. *اعداد اول تصادفی* n*-بیتی* p *و* q *تولید می‌شوند و* $N = pq$ *محاسبه می‌شود.*

۲. $p' \leftarrow \mathcal{A}(N)$

خروجی این آزمایش، که با $\mathsf{Factor}_{\mathcal{A}}(n)$ *نشان داده می‌شود برابر است با ۱، اگر* $p' \in \{p, q\}$ *و در غیر این صورت، خروجی آزمایش ۰ است.*

تعریف ۲ (*فرض تجزیه*) *برای هر مهاجم چندجمله‌ای تصادفی* $\mathcal{A}$*، تابع ناچیز* $\varepsilon(n)$ *وجود دارد که:*

$$\Pr\{\mathsf{Factor}_{\mathcal{A}}(n) = ۱\} \leq \varepsilon(n)$$

لم ۱ *اگر فرض* RSA *برقرار باشد، فرض تجزیه نیز برقرار است.*

نکته ۲ *ممکن است مسئله تجزیه سخت باشد ولی* RSA *آسان باشد؛ درواقع نمی‌دانیم که مسئله تجزیه و* RSA *معادل هم هستند یا نه.*

لم ۲ *اگر فرض* DDH *برقرار باشد، فرض* CDH *نیز برقرار است.*

برهان. اگر بتوانیم مسئله دیفی-هلمن محاسباتی را حل کنیم (یعنی از روی g^x و g^y بتوانیم g^{xy} را بدست آوریم)، یقینا می‌توانیم دو توزیع $(g,\ g^x,\ g^y,\ g^{xy})$ و $(g,\ g^x,\ g^y,\ g^r)$ را تمایز دهیم و در نتیجه می‌توانیم مسئله DDH را حل کنیم. ■

لم ۳ *فرض* DDH *روی* $\mathbb{Z}_p^*$ *برقرار نیست.*

برهان. با آزمایش زیر می‌توانیم تشخیص دهیم که $y \in \mathbb{Z}_p^*$ مانده مربعی هست یا نه:
اگر $y^{\frac{p-۱}{۲}} = ۱ \mod p$ باشد، y مانده مربعی است.
اگر $y^{\frac{p-۱}{۲}} = -۱ \mod N$ باشد، y مانده نامربعی است.

از روی این نکته می‌توانیم یك تمایزگر برای تشخیص توزیع‌های $D_۱ = (g^x, g^y, g^{xy})$ و $D_۰ = (g^x, g^y, g^r)$ بسازیم.
اگر حداقل یکی از x و y مانده مربعی باشند (که با احتمال $\frac{۳}{۴}$ این اتفاق می‌افتد)، g^{xy} حتما مانده مربعی است، ولی g^r با احتمال $\frac{۱}{۲}$ مانده مربعی‌است. حال می‌توانیم تمایزگر $\mathcal{D}$ را به صورت زیر بسازیم:

$$\mathcal{D}(u, v, w) = \begin{cases} ۱\ ,\ w^{\frac{p-۱}{۲}} = ۱ \\ ۰\ ,\ w^{\frac{p-۱}{۲}} = -۱ \end{cases}$$

داریم: $|\Pr\{\mathcal{D}(D_۰) = ۱\} - \Pr\{\mathcal{D}(D_۱) = ۱\}| = |۱/۲ - ۳/۴| = ۱/۴$

تمایزگر ما دارای مزیت قابل‌توجه است، پس فرض DDH برای $\mathbb{Z}_p^*$ برقرار نیست.

■

فرضیه ۳ *فرض CDH روی $\mathbb{Z}_p^*$ برقرار است.*

فرضیه ۴ *اگر G زیرگروه با مرتبه q از $\mathbb{Z}_{۲q+۱}^*$ باشد (که q و $۲q+۱$ اولند)، فرض DDH برای G برقرار است.*

فرضیه ۵ *فرض HDH برای گروه $\mathbb{Z}_p^*$ برقرار است.*

۲ سیستم رمز RSA

برای سادگی نمایش الگوریتم GenRSA را که ماژول‌های RSA را تولید می‌کند به صورت زیر تعریف می‌کنیم.
الگوریتم GenRSA: با ورودی ۱^n، ابتدا دو عدد اول n بیتی تصادفی p و q تولید و $N = pq$ را محاسبه می‌کند. سپس عدد تصادفی e را تولید می‌کند که $\gcd(e, \phi(N)) = ۱$ باشد. در نهایت $d = e^{-۱} \mod \phi(N)$ را محاسبه می‌کند. خروجی الگوریتم (N, e, d) است.
اولین ایده‌ای که برای ساخت سیستم رمز نامتقارن به ذهن می‌رسد به صورت زیر است که به سیستم رمز RSA ساده[۵] معروف است:

۱. $(pk,\ sk) \leftarrow \mathsf{Gen}(۱^n)$
الگوریتم تولید کلید Gen با ورودی ۱^n، ابتدا $(N,\ e,\ d) \leftarrow \mathsf{GenRSA}(۱^n)$ را اجرا می‌کند و سپس کلیدهای عمومی و خصوصی را به صورت $pk = (N,\ e)$ و $sk = (N,\ d)$ محاسبه می‌کند.

۲. $c \leftarrow \mathsf{Enc}_{pk}(m)$
الگوریتم رمزنگاری تحت کلید عمومی $pk = (N, e)$ پیام $m \in \mathbb{Z}_N^*$ را به متن رمزی $c = m^e \mod N$ می‌نگارد.

۳. $m \leftarrow \mathsf{Dec}_{sk}(c)$
الگوریتم رمزگشایی تحت کلید خصوصی $sk = (N, d)$ متن رمزی $c \in \mathbb{Z}_N^*$ را به پیام $m = c^d \mod N$ می‌نگارد.

گفتیم این سیستم رمز امنیت CPA ندارد، چون الگوریتم رمزنگاری تصادفی نیست.

۱.۲ سیستم رمز RSA پد شده

به دنبال یك سیستم رمز کلید عمومی هستیم که دارای امنیت CPA باشد. اولین نکته این است که الگوریتم رمزنگاری تصادفی باشد. می‌توانیم با قرار دادن مقدار تصادفی r در ابتدای پیام m، پیام $x = \boxed{r}\boxed{m}$ را تولید کنیم و سپس x را با الگوریتم رمزنگاری RSA رمز کنیم. این شیوه رمزنگاری موسوم به سیستم رمز RSA پد شده[۶] است که توصیف رسمی آن در زیر آورده شده است:
فرض کنید مولد GenRSA مانند قسمت قبل باشد و l تابعی باشد که به ازای هر n در شرط $l(n) \leq ۲n - ۲$ صدق کند.

[۵] Plain RSA
[۶] Padded RSA

۱. $(N, e, d) \leftarrow \mathsf{GenRSA}(1^n)$
$pk = (N, e)$
$sk = (N, d)$

۲. $\mathsf{Enc}_{pk}(m)$ پیام $m \in \{0,1\}^{l(n)}$ را می‌گیرد، سپس یك رشته تصادفی $r \in \{0,1\}^{|N|-l(n)-1}$ تولید می‌کند و در نهایت متن رمز شده c را برمی‌گرداند که c به صورت زیر محاسبه می‌شود:
$x = r||m$
$c = x^e \mod N$

۳. $m \leftarrow \mathsf{Dec}_{sk}(c)$ که m به صورت زیر محاسبه می‌شود:
$\hat{m} = c^d \mod N$
m برابرست با $l(n)$ بیت کم‌ارزش $\hat{m}$

طول مقدار افزوده شده‌ی r تاثیر مستقیم بر امنیت سیستم دارد. اگر این طول نسبت به طول کل پیام ناچیز باشد (مثلا $|r| = O(\log(n))$) آن‌گاه مهاجم[۷] می‌تواند با جستجوی کامل روی تمام r ها به سیستم حمله کند.
در حالتی که به ازای یك ثابت $c < 1$، $l(n) = c \cdot n$ باشد، گرچه تابه‌حال کسی موفق به شکستن سیستم نشده، اما اثباتی نیز (تحت فرض RSA) بر امنیت سیستم ارائه نشده است. در حالاتی که طول پیام m از مرتبه‌ی لگاریتمی برحسب پارامتر امنیتی باشد، سیستم تحت فرض RSA دارای امنیت CPA است.

قضیه ۴ *سیستم رمز RSA پد شده با $l(n) = O(\log(n))$، تحت فرض RSA دارای امنیت CPA است.*

تعریف امنیت CCA در سیستم‌های رمز نامتقارن مشابه امنیت CPA است، با این تفاوت که مهاجم علاوه بر دسترسی به کلید عمومی، به الگوریتم رمزگشایی نیز دسترسی اوراکلی دارد. در ادامه آزمایش حمله متن رمزشده منتخب و امنیت CCA را برای سیستم‌های رمز نامتقارن تعریف می‌کنیم:

تعریف ۶ *آزمایش حمله‌ی متن رمزشده منتخب*[۸] $\mathsf{PubK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n)$

۱. $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
۲. $m_0, m_1 \leftarrow \mathcal{A}^{\mathsf{Dec}_{sk}(\cdot)}(1^n, pk)$ که $|m_0| = |m_1|$
۳. $b \leftarrow \{0,1\}$
۴. $c \leftarrow \mathsf{Enc}_{pk}(m_b)$
۵. $\hat{b} \leftarrow \mathcal{A}^{\mathsf{Dec}_{sk}(\cdot)}(c)$ که $\mathcal{A}$ *مجاز به درخواست رمزگشایی* c *نیست.*

خروجی آزمایش که با $\mathsf{PubK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n)$ نشان داده می‌شود، برابرست با ۱، اگر $\hat{b} = b$، در غیر این صورت خروجی آزمایش ۰ است.

[۷] Adversary
[۸] Chosen Ciphertext Attack

تعریف ۷ *سیستم رمز نامتقارن* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *را، دارای امنیت متن رمزشده انتخابی (یا* CCA*-امن*[۹]*) گوییم، اگر برای هر مهاجم چندجمله‌ای و تصادفی* $\mathcal{A}$ *که در آزمایش فوق شرکت می‌کند، تابع ناچیز* $\varepsilon(n)$ *وجود داشته باشد که:*

$$\Pr\{\mathsf{PubK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n) = ۱\} \leq \frac{۱}{۲} + \varepsilon(n)$$

۱.۱.۲ سیستم رمز PKCS#1

روشی مشابه رمزنگاری RSA پد شده در عمل نیز در سیستم رمزی به نام PKCS#1 که نسخه‌ی نخست آن در https به کار رفته، پیاده شده است. نحوه‌ی افزودن مقدار تصادفی r در این روش در شکل زیر آورده شده است. در ابتدای پیام بایت 02 قرار دارد، سپس مقدار تصادفی r که در آن بایت `ff` به کار نرفته است، سپس بایت `ff` و نهایتا پیام m.

$$x = \boxed{\texttt{02} \mid r \mid \texttt{ff} \mid m}$$
$$c = x^e$$

سیستم رمز PKCS#1 دارای امنیت CCA نیست. یك حمله واقعی به این سیستم وجود دارد که در آن مهاجم برای یافتن پیام اصلی[۱۰] متناظر با یک متن رمزشده[۱۱]، تعدادی متن رمزشده به چالشگر فرستاده و با استفاده از پاسخ وی موفق به شکستن سیستم می‌شود. اگر در ابتدای یکی از پرسش‌های مهاجم بایت 02 نباشد، چالشگر پیغامی مبنی بر نامعتبر بودن متن رمزشده به مهاجم می‌فرستد و مهاجم متوجه نامعتبر بودن پیام رمزشده‌ی اولیه می‌شود. بدین‌ترتیب با ارسال تعداد بیش‌تر پیام رمزشده و بررسی اعتبار آن‌ها به نتیجه موردنظر می‌رسد.

۲.۲ سیستم رمز RSA با تابع درهم‌سازی

رویکردی دیگر در به‌کارگیری فرض RSA، استفاده از تابع درهم‌سازی[۱۲] و سیستم رمز متقارن است. در ادامه به شرح چنین سیستمی می‌پردازیم که با پیش‌فرض درستی فرض RSA دارای امنیت CCA است.
فرض کنید $\Pi = (\mathsf{G}, \mathsf{E}, \mathsf{D})$ یک سیستم رمز متقارن با فضای کلید یکنواخت $\mathcal{K}$ و $H_N : \mathbb{Z}^*_N \to \mathcal{K}$ خانواده‌ای از توابع درهم‌سازی باشد.
همانند قبل مولد $\mathsf{GenRSA}(۱^n)$ ماژول‌های RSA را تولید می‌کند.

۱. $(N, e, d) \leftarrow \mathsf{GenRSA}(۱^n)$
$pk = (N, e)$
$sk = (N, d)$

۲. $\langle y, \mathsf{E}_k(m)\rangle \leftarrow \mathsf{Enc}_{pk}(m)$ که y و k به صورت زیر محاسبه می‌شوند:
$r \leftarrow \mathbb{Z}^*_N$ (r به تصادف از $\mathbb{Z}^*_N$ انتخاب می‌شود.)
$k = H_N(r)$
$y = r^e \mod N$

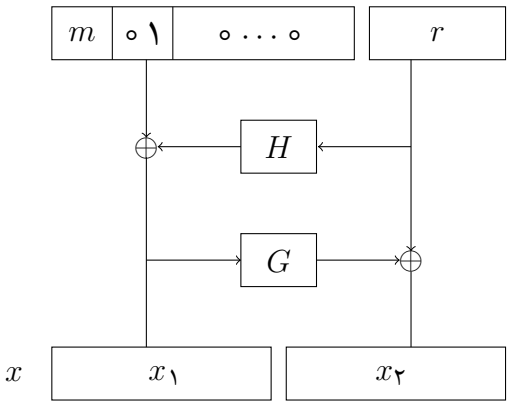
[۹] chosen ciphertext attack secure
[۱۰] Plaintext
[۱۱] Ciphertext
[۱۲] Hash Function

۳. $\mathsf{D}_k(c_2) \leftarrow \mathsf{Dec}_{sk}\langle c_1, c_2\rangle$ که k به صورت زیر محاسبه می‌شود:
$$r = c_1^d \mod N$$
$$k = H_N(r)$$

این استانداردی است به نام ISO که در عمل خیلی از آن استفاده نمی‌شود.
ثابت می‌شود اگر سیستم رمز متقارن استفاده شده دارای امنیت اصالت‌سنجی[۱۳] بوده و تابع درهم‌سازی نیز اوراکل تصادفی باشد، سیستم رمز عمومی تولیدشده دارای امنیت CCA خواهد بود. در این‌جا فرض بر ایده‌آل بودن تابع درهم‌سازی است که مصداقی ندارد؛ درنتیجه برای حل این مشکل از توابع درهم‌سازی معروف استفاده می‌شود که نمی‌توان امنیتش را اثبات کرد، اما تابه‌حال نیز شکسته نشده است.

۱.۲.۲ سیستم رمز RSA-OAEP

روشی دیگر که استاندارد بوده و امروزه پرکاربرد گشته روشی است به نام OAEP. در زیر به عنوان نمونه‌ای از این روش، نسخه‌ی OAEP PKCS 1 v.2. تشریح می‌شود:
در این سیستم دو تابع درهم‌سازی H و G استفاده می‌شود. پیام اولیه با افزوده شدن ۱ ۰ و تعداد مشخصی صفر به انتهای سمت راست آن با $H(r)$، xor شده (r پیامی تصادفی است) و حاصل، نیمه‌ی اول خروجی x، یعنی x_1 را تولید می‌کند. x_2، نیمه‌ی دوم x، برابر است با $r \oplus G(x_1)$. نهایتا پیام رمزشده برابر $c = x^e \mod N$ خواهد بود. نمودار این سیستم در زیر آمده است:



در اینجا نیز اگر سیستم رمز CCA-امن باشد و دو تابع درهم‌سازی ایده‌آل باشند، نهایتا سیستم تحت فرض RSA دارای امنیت CCA خواهد بود. نسخه‌های مشابه با یک تابع درهم‌سازی نیز وجود دارند، اما کاربرد چندانی ندارند.

۳ سیستم رمز الگمال

۱.۳ سیستم رمز الگمال با تابع درهم‌سازی

سیستم رمز دیگری که در این جلسه به آن اشاره می‌کنیم، سیستم الگمال[۱۴] است که در آن از فرض لگاریتم گسسته استفاده می‌شود. در ادامه سیستم رمز الگمال را با استفاده از یك تابع درهم‌سازی H و یك سیستم رمز متقارن

[۱۳] مشابه امنیت CCA است، اما مهاجم نمی‌تواند هیچ پیام رمزشده‌ی معتبری تولید کند

[۱۴] El Gamal

$\Pi = (\mathsf{G}, \mathsf{E}, \mathsf{D})$ معرفی می‌کنیم:

۱. $(G, q, g) \leftarrow \mathsf{GroupGen}(1^n)$ (یك گروه دوری G با مرتبه q و مولد g تولید می‌کند.)
$x \leftarrow \mathbb{Z}_q$ (x را به تصادف از $\mathbb{Z}_q$ انتخاب می‌کند.)
$h = g^x$
$pk = (G, q, g, h)$
$sk = (G, q, g, x)$

۲. $\langle u, c\rangle \leftarrow \mathsf{Enc}_{pk}(m)$ که u و c به صورت زیر محاسبه می‌شوند:
$r \leftarrow \mathbb{Z}_q$ (یك عدد تصادفي r از $\mathbb{Z}_q$ انتخاب می‌شود.)
$u = g^r\ ,\ v = h^r$
$k = H(u,\ v)$
$c = \mathsf{E}_k(m)$

۳. $m \leftarrow \mathsf{Dec}_{sk}(\langle u, c\rangle)$ که m به صورت زیر محاسبه می‌شود:
$v = u^x$
$k = H(u, v)$
$m = \mathsf{D}_k(c)$

لم ۵ *اگر تابع درهم‌سازی H اوراکل تصادفی باشد و اگر سیستم رمز متقارن Π دارای امنیت CCA باشد، تحت فرض دیفی- هلمن محاسباتی نتیجه می‌گیریم این سیستم رمز دارای امنیت CPA است. همچنین اگر سیستم رمز متقارن Π دارای امنیت CCA باشد، تحت فرض HDH سیستم رمز الگمال با تابع درهم‌سازی، دارای امنیت CPA است.*

نکته ۳ *تحت فرض HDH نمی‌توانیم امنیت CCA را برای سیستم رمز الگمال با تابع درهم‌سازی اثبات کنیم. می‌توان ثابت کرد که این سیستم رمز تحت فرض دیگری به نام فرض دیفی- هلمن چکیده‌ای تعاملی ($IHDH$)[۱۵] دارای امنیت CCA است.*

۲.۳ سیستم رمز الگمال

در فرضیات مطرح شده در بخش قبل لازم است که تابع درهم‌سازی اوراکل تصادفی باشد؛ ولی در عمل تابع درهم‌سازی ایده‌ال یا اوراکل تصافی وجود ندارد. ما تمایل داریم فرض‌های ساده‌تر و معقول‌تری در رمزنگاری مطرح کنیم. حال می‌خواهیم یك سیستم رمز کلید عمومی بسازیم که امنیت متن اصلی منتخب داشته‌باشد ولی از فرض ساده‌تری استفاده کند. به همین منظور به جای‌استفاده از فرض HDH که نیاز به اوراکل تصادفی بودن تابع درهم‌سازی دارد، از فرض DDH استفاده می‌کنیم.
می‌خواهیم بر مبنای فرض DDH و بدون استفاده از تابع درهم‌سازی، یك سیستم رمز بسازیم که امنیت متن اصلی منتخب داشته باشد. سیستم رمزی که در ادامه معرفی می‌کنیم سیستم رمز الگمال است:

۱. $(G, q, g) \leftarrow \mathsf{GroupGen}(1^n)$ (یك گروه دوری G با مرتبه q و مولد g تولید می‌کند.)
$x \leftarrow \mathbb{Z}_q$ (به تصادف x را از $\mathbb{Z}_q$ انتخاب می‌کند.)
$h = g^x$

[۱۵] Interactive Hash Diffie-Hellman

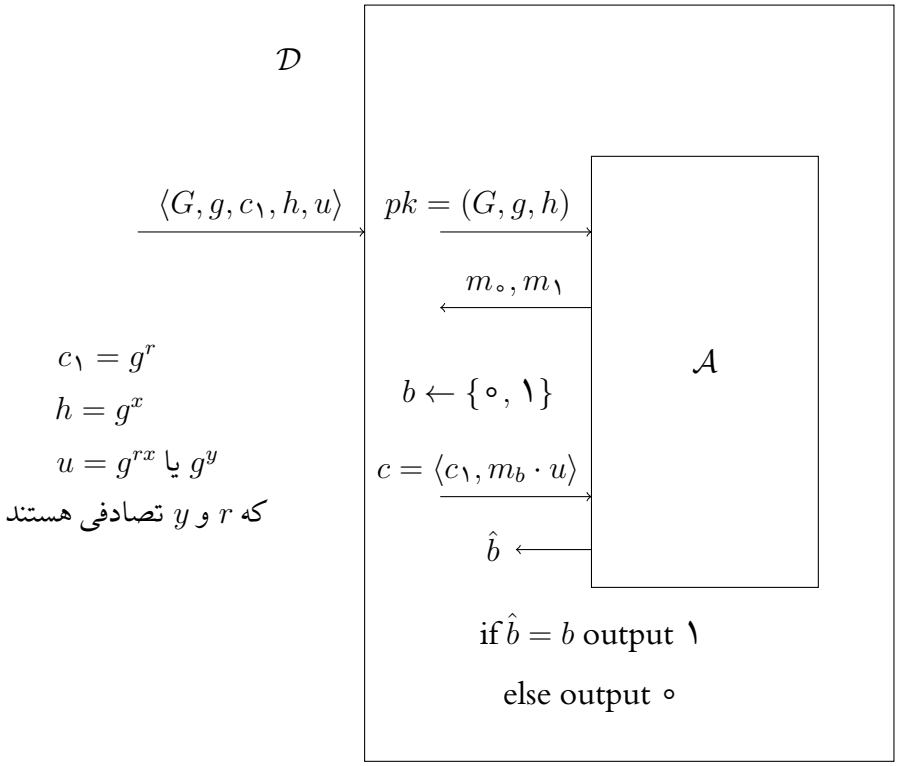
$$pk = (G, q, g, h)$$
$$sk = (G, q, g, x)$$

۲. $\langle g^r, m \cdot h^r \rangle \leftarrow \mathsf{Enc}_{pk}(m)$ که r به تصادف از $\mathbb{Z}_q$ انتخاب می‌شود.

۳. $\frac{c_1}{c_2^x} \leftarrow \mathsf{Dec}_{sk}(\langle c_1, c_2 \rangle)$

لم ۶ *سیستم رمز الگمال تحت فرض DDH، امنیت متن اصلی منتخب دارد.*

برهان. این لم را با استفاده از کاهش اثبات می‌کنیم:
فرض کنید سیستم رمز الگمال تحت فرض DDH، امنیت CPA ندارد. در این صورت یك مهاجم چندجمله‌ای $\mathcal{A}$ برای حمله به این سیستم وجود دارد که با احتمال غیرناچیز $\mu(n)$ در آزمایش تمایز موفق می‌شود. تمایزگر $\mathcal{D}$ را به صورت زیر از روی مهاجم $\mathcal{A}$ می‌سازیم:



تمایزگر $\mathcal{D}$ توزیع‌های $DH = \langle G, g, g^r, g^x, g^{rx} \rangle$ و $R = \langle G, g, g^r, g^x, g^y \rangle$ را با احتمال غیرناچیز $\mu(n)$ تشخیص می‌دهد، زیرا:

$$\Pr\{\mathcal{D} = 1 | DH\} = \Pr\{\hat{b} = b\} \geq 1/2 + \mu(n)$$
$$\Pr\{\mathcal{D} = 1 | R\} = 1/2$$
$$\Rightarrow |\Pr\{\mathcal{D} = 1 | DH\} - \Pr\{\mathcal{D} = 1 | R\}| \geq \mu(n)$$

با فرض DDH به تناقض رسیدیم. پس فرض خلف باطل و حکم برقرار است. ■

نکته ۴ *این سیستم تحت فرض DDH ، امنیت متن رمزشده منتخب ندارد. یکی از دلایل آن این است که این سیستم دارای خاصیت هومومورفیك است.*

تعریف ۸ *می‌گوییم یك سیستم رمز دارای خاصیت هومومورفیك است، اگر برای هر پیام m_1 و m_2 در فضای پیام با متن‌های رمزشده c_1 و c_2، رابطه $c_1 \cdot c_2 = \mathsf{Enc}_k(m_1 \cdot m_2)$ برقرار باشد.*

قضیه ۷ *اگر یك سیستم رمز کلید عمومی دارای ویژگی هومومورفیك باشد، دارای امنیت CCA نیست.*

از این ویژگی در ساخت پروتکل‌ها استفاده می‌شود.
یکی از کاربردهای این ویژگی این است که اگر متن رمزشده یك پیام را داشته باشیم، می‌توانیم یك متن رمزشده جدید برای همان پیام تولید کنیم، بدون اینکه بدانیم پیام اصلی یا کلید خصوصی چیست. فرض کنید $c = \mathsf{Enc}_{pk}(m)$ را داریم. کافیست c را در یك متن رمزشده از ۱ ضرب کنیم، تا به یك متن رمزشده جدید برای m برسیم.
این موضوع کاربردهای زیادی دارد؛ مثلا در رای‌گیری الکترونیکی چنین کاری انجام می‌شود.