به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

جلسه‌ی ۲۱: مسائل سخت رمزنگاری

مدرس: دکتر شهرام خزائی *نگارنده: رضا کابلی*

در این جلسه مقدماتی از نظریه گروه‌ها ارائه کرده سپس چند مسأله‌ی سخت نظریه اعداد مانند مسأله تجزیه و لگاریتم گسسته را معرفی می‌کنیم. این مسائل، اصول اولیه رمزنگاری را تشکیل می‌دهند که می‌توان با استفاده از آنها، امنیت سیستم‌های رمزنگاری را اثبات نمود.

مقدماتی از گروه

قضیه ۱ (قضیه لاگرانژ) *برای هر گروه متناهی G و هر زیرگروه H از آن، $|H| \mid |G|$.*

تعریف ۱ *فرض کنید G یک گروه با عضو خنثی 1 و a عضوی از G باشد. مرتبه a، که با $o(a)$ نمایش می‌دهیم، کوچکترین عدد صحیح t است که $a^t = 1$.*

تعریف ۲ *برای هر گروه G و عنصر دلخواه a از آن مجموعه همه‌ی توان‌های a زیر گروه تولید شده توسط a نامیده می‌شود و با $\langle a \rangle$ نشان داده می‌شود. یعنی،*

$$\langle a \rangle = \{1, a, \ldots, a^{o(a)-1}\}$$

قضیه ۲ *مرتبه هر عنصر، مرتبه گروه را عاد می‌کند.*

برهان. مرتبه یک عنصر همواره با مرتبه‌ی زیرگروه تولید شده توسط آن برابر است لذا از قضیه قبل می‌توان نتیجه گرفت مرتبه عنصر، مرتبه گروه را عاد می‌کند. ■

نتیجه ۳ *برای هر $a \in G$، داریم $a^{|G|} = 1$.*

نتیجه ۴ (قضیه‌ی اویلر) *برای هر عدد طبیعی N و a که $\gcd(a, N) = 1$ رابطه $a^{\varphi(N)} \equiv 1 \mod N$ برقرار است زیرا مجموعه اعداد طبیعی کمتر از N که نسبت به N اولند با عمل ضرب یک گروه از مرتبه $\varphi(N)$ تشکیل می‌دهند.*

نتیجه ۵ (قضیه‌ی کوچک فرما) *برای هر عدد اول p و هر عدد طبیعی a رابطه $a^{p-1} \equiv 1 \mod p$ برقرار است زیرا $\varphi(p) = p - 1$.*

تعریف ۶ (گروه دوری و مولد گروه) *فرض کنیم گروه متناهی G دارای عنصری مثل g باشد که زیرگروه تولید شده توسط g با گروه G برابر شود؛ یعنی $G = \langle g \rangle$. در این صورت گروه را دوری و g را مولد گروه می‌نامیم.*

نکته ۱ *عنصر g یک مولد برای G است اگر وتنها اگر $o(g) = |G|$.*

قضیه ۳ *$\mathbb{Z}_p^*$ دوری است .* $(\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\})$

قضیه ۴ *اگر گروه G دوری باشد، آنگاه گروه G دارای $\varphi(|G|)$ مولد متمایز است.*

نتیجه ۷ *گروه $\mathbb{Z}_p^*$ دارای $\varphi(p-1)$ مولد است.*

سؤال ۸ *به نظر شما $\mathbb{Z}_N^*$ برای چه N هایی دوری است؟*

محاسبه ریشه e–ام

در $\mathbb{Z}_N^*$ می‌توان به صورت کارایی عناصر را به توان رساند. سوالی که در این جا مطرح می‌شود این است که آیا عکس این کار (یعنی محاسبه ریشه) نیز به صورت کارا امکان پذیر است؟

تعریف ۹ *عنصر $y \in \mathbb{Z}_N^*$ را مانده مربعی می‌نامیم هرگاه $x \in \mathbb{Z}_N^*$ موجود باشد به طوری که $x^2 = y \mod N$.*

در $\mathbb{Z}_p^*$ برای تشخیص مانده مربعی بودن یک عنصر محک زیر را داریم:

قضیه ۵ *فرض کنید p یک عدد اول و $y \in \mathbb{Z}_p^*$ باشد. آنگاه:*

$$y^{\frac{p-1}{2}} = \begin{cases} 1 & y \text{ مانده مربعی است} \\ -1 & y \text{ نامانده مربعی است} \end{cases} \pmod p$$

دقت داشته باشید که محک فوق صرفا وجودی است و روشی برای محاسبه ریشه ارائه نمی‌کند. برای این منظور از قضیه زیر استفاده می‌کنیم:

قضیه ۶ *اگر $p = 4k+3$ و y یک مانده مربعی باشد آنگاه ریشه دوم y برابر است با $x = y^{\frac{p+1}{4}}$.*

برهان. داریم:

$$x^2 = (y^{\frac{p+1}{4}})^2 = y^{\frac{p+1}{2}} = y^{\frac{p-1}{2}} y = y$$

■

اگر $p = 4k+1$، باز هم می‌توان با یگ الگوریتم تصادفی چندجمله‌ای، یک ریشه دوم برای y یافت. پیدا کردن یک الگوریتم قطعی برای این حالت یک مسأله باز است.

نکته ۲ *اگر x ریشه ای برای y باشد به روشنی $-x = p - x$ نیز ریشه ای از y است.*

حال اگر $y \in \mathbb{Z}_N^*$ دلخواه باشد چگونه می‌توان مانده مربعی بودن y را تشخیص داد؟ چگونه می‌توان ریشه ای برای آن یافت؟
فرض کنیم تجزیه N به صورت حاصل‌ضرب عناصر اول را در اختیار داریم. برای سادگی فرض کنیم $N = pq$ که p و q اول و متمایزند. اگر y در $\mathbb{Z}_p^*$ و $\mathbb{Z}_q^*$ مانده مربعی باشد نشان می‌دهیم y در Z_N^* نیز مانده مربعی است. برای این منظور به ترتیب x_1 و x_2 را ریشه‌هایی برای y در $\mathbb{Z}_p^*$ و $\mathbb{Z}_q^*$ می‌گیریم. با استفاده از قضیه باقیمانده چینی عنصر $z \in \mathbb{N}$ را طوری می‌یابیم که در معادلات زیر صدق کند:

$$\begin{aligned} z &\equiv x_1 \mod p \\ z &\equiv x_2 \mod q \end{aligned}$$

در این صورت

$$\begin{aligned} z^2 &\equiv y \mod p \\ z^2 &\equiv y \mod q \end{aligned}$$

در نتیجه $z^2 \equiv y \mod N$ پس y در $\mathbb{Z}_N^*$ مانده مربعی است. برعکس اگر $y \in \mathbb{Z}_N^*$ مانده مربعی باشد به وضوح y در $\mathbb{Z}_p^*$ و $\mathbb{Z}_q^*$ نیز مانده مربعی خواهد بود.

نتیجه ۱۰ *اگر $y \in \mathbb{Z}_N^*$ مانده مربعی باشد، آنگاه دقیقاً چهار ریشه متمایز در $\mathbb{Z}_N^*$ دارد.*

سؤال ۱۱ *به نظر شما تشخیص مانده مربعی بودن در $y \in \mathbb{Z}_N^*$ دلخواه بدون داشتن تجزیه N آسان است؟*

سؤال ۱۲ *مسأله پیدا کردن ریشه در هنگ توانی از یک عدد اول را چگونه می‌توان حل کرد؟*

نتیجه اینکه با استفاده از تجزیه در $\mathbb{Z}$، می‌توان مسأله محاسبه ریشه دوم در $\mathbb{Z}_N^*$ را حل کرد.
برعکس، می‌خواهیم به کمک محاسبه ریشه دوم، مسأله تجزیه را حل کنیم. فرض کنیم عدد طبیعی N دلخواه باشد؛ عنصری به تصادف مثل z انتخاب می‌کنیم. عنصر $y = z^2 \mod N$ مانده مربعی است پس ریشه ای چون x دارد. از این رو

$$x^2 = z^2 \mod N \Rightarrow N | x^2 - z^2 \Rightarrow N | (x+z)(x-z)$$

پس N با $(x-z)$ یا $(x+z)$ عامل مشترک دارد که به صورت کارایی قابل محاسبه است؛ پس یک تجزیه برای N به صورت حاصل‌ضرب عوامل کوچکتر پیدا می‌کنیم که با ادامه این روند تجزیه N به عوامل اولش بدست می‌آید.

نتیجه ۱۳ *مسأله تجزیه در $\mathbb{Z}$، با مسأله محاسبه ریشه دوم در $\mathbb{Z}_N^*$ معادل است.*

سؤال ۱۴ *در مورد معادل بودن تجزیه در $\mathbb{Z}$ و مسأله محاسبه ریشه $e-$ام در $\mathbb{Z}_N^*$ چه می‌توان گفت؟*

توجه کنید که اگر $\gcd(e, \varphi(n)) = 1$ باشد، هر $y \in \mathbb{Z}_N^*$ دارای یک ریشه $e-$ام یکتا به صورت y^d است که $d = e^{-1} \mod \varphi(n)$.

فرضیات رمزنگاری

- **فرض تجزیه**: اگر p و q دوعدد اول تصادفی هم‌اندازه باشند، محاسبه p یا q از روی $N = pq$ سخت است.
- **فرض RSA (فرض ریشه e−ام)**: محاسبه x از روی $x^e \mod N$ که N حاصلضرب دو عدد اول تصادفی هم‌اندازه است و $\gcd(e, \varphi(N)) = ۱$ برای x تصادفی سخت است.
- **فرض لگاریتم گسسته**: در گروه G با مولد g، محاسبه x از روی g^x برای x تصادفی سخت است.
- **فرض دیفی‌هلمن محاسباتی**: در گروه G با مولد g، محاسبه g^{xy} از روی g^x و g^y برای x و y تصادفی سخت است.
- **فرض دیفی‌هلمن تصمیمی**: در گروه G با مولد g، تمایز (g, g^x, g^y, g^{xy}) از (g, g^x, g^y, g^r) برای x،y و rتصادفی سخت است.

فرض‌های لگاریتم گسسته، دیفی‌هلمن محاسباتی و دیفی‌هلمن تصمیمی برای همه گروه‌ها درست نیستند وبرای هر یک، باید گروهی مناسب اختیار شود.
برای مثال باور عمومی بر این است که در $\mathbb{Z}_p^\star$ مساله لگاریتم گسسته و مساله دیفی‌هلمن محاسباتی مسائلی سخت هستند. اما در همین $\mathbb{Z}_p^\star$ فرض دیفی‌هلمن تصمیمی برقرار نیست زیرا برای (u, v, w, z) داده شده می‌توان تمایزگر $\mathcal{D}$ را که به صورت زیر تصمیم می‌گیرد ارائه کرد:

$$\mathcal{D}(u, v, w, z) = \begin{cases} ۱ & \text{اگر } z \text{ مانده مربعی باشد} \\ ۰ & \text{درغیراینصورت} \end{cases}$$

تمایزگر $\mathcal{D}$ داری مزیت غیر ناچیز $\frac{۱}{۴}$ است.

سؤال ۱۵ *گروهی بیابید که مسأله دیفی‌هلمن تصمیمی در آن سخت باشد.*

پاسخ. تمایزگری که برای مسأله دیفی‌هلمن تصمیمی روی $\mathbb{Z}_p^*$ ارائه کردیم از ایده مانده مربعی برای تمایز استفاده کرد. پس اگر به نحوی بتوانیم این شرط را حذف کنیم احتمالاً فرض دیفی‌هلمن تصمیمی برقرار خواهد بود. عدد اول p را طوری انتخاب می‌کنیم که $p = ۲q + ۱$ و q خود اول باشد. می‌توان نشان داد مجموعه‌ی مانده‌های مربعی در هنگ p، یعنی مجموعه

$$\mathrm{QR} = \{x^۲ \mid x \in \mathbb{Z}_p^*\},$$

خود یک گروه از مرتبه q تشکیل می‌دهند. باور عمومی بر این است که فرض دیفی‌هلمن تصمیمی برای این گروه سخت است.

نکته ۳ *اگر g مولدی برای $\mathbb{Z}_p^*$ باشد، آنگاه $g^۲$ مولدی برای گروه مانده‌های مربعی $\mathbb{Z}_p^*$ است، یعنی $\mathrm{QR} = \langle g^۲ \rangle$.*