
بسم الله الرحمن الرحیم

ارائه ارائه فصل 9

نام دانشجو: سیدساسان میرطاهری

رشته: شبکه های کامپیوتری

تاریخ ارائه: 17 آذر 1404

نام دانشگاه: جامع انقلاب اسلامی

فهرست مطالب ارائه

بخش اول: 9

نظریهٔ اعداد و فرضیات سختی رمزنگاری

سامانه‌های رمزنگاری مدرن تقریباً همیشه روی این فرض بنا شده‌اند که «حل یک مسألهٔ خاص سخت است».

در فصل‌های ۳ تا ۵ دیدیم که رمزنگاری کلید متقارن – هم طرح‌های رمزنگاری و هم کدهای تأیید پیام (– MAC) می‌توانند بر پایهٔ این فرض ساخته شوند که «چرخه‌های تصادفی شبه‌رمزی» (= pseudorandom permutations بلوک‌سیفرها) وجود دارند.

در نگاه اول، فرض وجود این چرخه‌های شبه‌تصادفی، فرضی قوی و غیرطبیعی به‌نظر می‌رسد، و طبیعی است بپرسیم:

- اصلاً این فرض درست است؟
- چه شواهدی داریم که از آن حمایت کند؟

در فصل ۷ دیدیم که بلوک‌سیفرها در عمل چطور ساخته می‌شوند. این واقعیت که این ساختارها تا الان در برابر حمله مقاومت کرده‌اند، نشانه‌ای است که وجود چنین توابع شبه‌تصادفی، «محتمل» و قابل‌باور است.

با این حال، همچنان ممکن است برایمان سخت باشد که بپذیریم **هیچ** حملهٔ کارای تمایزبخشی روی

در این قسمت عنوان اسلاید را وارد کنید

از طرف دیگر، وضعیتِ فعلیِ تئوری ما هم این است که **نمی‌دانیم** چطور «تصادفی‌بودن» هیچ‌کدام از ساختارهای عملیِ فعلی را، بر اساس یک فرض ساده‌تر یا طبیعی‌تر، **اثبات** کنیم.

خلاصه، این وضعیت خیلی رضایت‌بخش نیست.

در مقابل، همان‌طور که در فصل ۳ اشاره شد (و در فصل ۸ مفصل بررسی شد)، می‌توانیم نشان دهیم که **اگر توابع یک‌سویه (one-way functions)وجود داشته باشند، توابع شبه‌تصادفی هم وجود خواهند داشت**. (به‌طور غیررسمی، تابعی یک‌سویه است اگر «محاسبه‌اش» راحت باشد ولی «برعکس‌کردنش» سخت؛ تعریف دقیق‌تر در بخش ۹٫۴٫۱ می‌آید.)

به‌جز یک بحث کوتاه در بخش ۸٫۱٫۲، تا اینجا هیچ مثالِ مشخصی از توابعی که «باور داریم یک‌سویه‌اند» ندیدیم.

یکی از هدف‌های این فصل این است که:

- چند مسألهٔ مشهور که «باور داریم سخت‌اند» را معرفی کنیم،
- و توابعی را که **حدس می‌زنیم یک‌سویه‌اند** بر اساس این مسائل بسازیم.

از این جهت، این فصل را می‌توان اوجِ «رویکرد از بالا به پایین» در رمزنگاری کلید متقارن دانست.

۹.۱ – مقدمات و نظریهٔ پایهٔ گروه‌ها

در این بخش، با مفاهیم پایه‌ای نظریهٔ اعداد (اعداد اول، بخش‌پذیری، حساب پیمانه‌ای) و همچنین نظریهٔ گروه‌ها آشنا می‌شویم. این مفاهیم در ادامهٔ فصل و در ساخت مفاهیم رمزنگاری عددی مثل RSAنقش کلیدی دارند.

9.1.1 اعداد اوّل و بخش‌پذیری Primes and Divisibility

مجموعهٔ اعداد صحیح را با $\mathbb{Z}$ نشان می‌دهیم. برای $a, b \ni \mathbb{Z}$،

a **بر** b **بخش‌پذیر است** و می‌نویسیم A | B ، $(Yc + Xb) \mid a$.

هرگاه عدد صحیحی c وجود داشته باشد که B = ac.

•اگر a بر b بخش‌پذیر نباشد، می‌نویسیم. $b \nmid a$

در عمل ما بیش‌تر به حالتی علاقه‌مندیم که هر سهٔ a , b , c مثبت باشند، هرچند این تعریف وقتی یکی یا چندتا از آن‌ها منفی یا صفر هم باشند، همچنان معنی دارد.

یک مشاهدهٔ ساده این است که اگر آن‌وقت برای هر $c \mid a$ و $b \mid a$. داریم: $\mathbb{Z} \ni X, Y$

بخش دوم: 9.1

اگر $b \mid a$ و a مثبت باشد، به aمی‌گوییم یک **مقسوم** divisor برای b

اگر علاوه بر این، $a \notin \{b, 1\}$، آن‌وقت aرا یک **مقسومِ غیر بدیهی** یا یک **عامل factor**برای bمی‌نامیم.

یک عدد صحیحِ مثبت 1p>1 > 1p>1rا **اوّل prime**می‌گوییم اگر هیچ عامل غیر بدیهی نداشته باشد؛ یعنی فقط دو مقسوم داشته باشد: ۱ و خودش.

یک عدد صحیح مثبت بزرگ‌تر از ۱ که اوّل نباشد را **مرکّب composite** می‌نامیم.

طبق قرارداد، عدد ۱ نه اوّل است و نه مرکّب.

قضیهٔ اساسی حساب(Fundamental Theorem of Arithmetic)

$$N = \prod_i p_i^e$$

یک قضیهٔ بنیادی در حساب این است که:

هر عدد صحیح بزرگ‌تر از ۱ را می‌توان به‌صورت یکتا (تا جابه‌جاییِ عوامل) به‌صورت ضربی از اعداد اوّل نوشت.

ادبیات تحقیق: تیتر خود را وارد کنید.

تقسیم با باقیمانده – گزاره ۹.۱

ما با فرآیندِ «تقسیم با باقیمانده» از دوران دبستان آشنا هستیم.

گزارهٔ زیر این مفهوم را رسمی می‌کند:

گزاره ۹.۱

بگذار a یک عدد صحیح و b یک عدد صحیحِ مثبت باشد.

آنگاه اعداد صحیحِ یکتای q,r وجود دارند به‌طوری‌که:

$$r + qb = a \quad \text{و} \quad b > r \geq 0.$$

علاوه بر این، برای هر a و b همان‌گونه که در گزاره آمده، می‌توان q و r را در زمان چندجمله‌ای محاسبه کرد

رجوع کنید به پیوست B.1

زمان اجرای یک الگوریتم، به‌عنوان تابعی از طولِ ورودی‌هایش اندازه‌گیری می‌شود. نکتهٔ مهم در نظریهٔ عددیِ الگوریتمی این است که ورودی‌های عددی همیشه در **نمایش دودویی** در نظر گرفته می‌شوند. یعنی زمان اجرای الگوریتمی که ورودی‌اش عدد صحیح N است، بر حسب N ، طول نمایش دودوییِ Nسنجیده می‌شود. توجه کنید که:

$$\|N\| = \lfloor \log_2 N \rfloor + 1.$$

ادبیات تحقیق: تیتر خود را وارد کنید.

در این قسمت عنوان اسلاید را وارد کنید

بزرگ‌ترین مقسوم مشترک – gcd

بزرگ‌ترین مقسوم مشترک دو عدد صحیح aو b، که آن را با $\gcd(a,b)$ نشان می‌دهیم، بزرگ‌ترین عدد صحیح cاست که:

- $a \mid c$ و
- $b \mid c$.

(برای $\gcd(0,0)$ مقداری تعریف نمی‌کنیم.)

مفهوم gcd وقتی یکی یا هر دوِ aو bمنفی هم باشند، همچنان معنا دارد، اما ما معمولاً با $1 \leq a,b$ کار می‌کنیم؛ در هر حال، همیشه داریم:

$$\gcd(|a|,|b|) = \gcd(a,b).$$

ادبیات تحقیق: تیتر خود را وارد کنید.

گزاره ۹٫۲ – نمایش خطی gcd

بگذار a و b دو عدد صحیحِ مثبت باشند. آنگاه اعداد صحیح X و Y وجود دارند به‌طوری‌که:

$$\gcd(a,b) = Yb + Xa.$$

علاوه بر این، gcd(a,b) **کوچک‌ترین عدد مثبت**ی است که می‌توان آن را به این شکل نوشت

برای این‌که نشان دهیم $\gcd(a,b) = d$ باید ثابت کنیم:

1. d، هم a و هم b را تقسیم می‌کند، و
2. هیچ مقسومِ مشترکِ بزرگ‌تری از d برای a و b وجود ندارد.

در واقع، نشان می‌دهیم d هر عضو ا را تقسیم می‌کند.

یک c دلخواه از ا را بردارید و بنویسید:

$$Y_0 b + X_0 a = c$$

ادبیات تحقیق: تیتر خود را وارد کنید.

9.1.2 حساب پیمانه‌ای (Modular Arithmetic)

$$.N > r \geq r, \qquad 0 + qN = a$$

$$.r = [\text{mod } N \quad a]$$

نماد $[\text{mod } N \quad a]$ یعنی *باقیماندهٔ a هنگام تقسیم بر N.*

بر اساس گزارهٔ ۹٫۱ می‌دانیم اعداد صحیح یکتایی q,r وجود دارد که:

ادبیات تحقیق: تیتر خود را وارد کنید.

هم‌مقایسه‌گی Congruence

می‌گوییم a و b نسبت به N **هم‌مقایسه** هستند، و می‌نویسیم:

$$b = a \mod N$$

$$.[b \mod N] = [a \mod N]$$

$$.(b - a) \mid N$$

$$z = \cdots = c = b = a \mod N$$

ادبیات تحقیق: تیتر خود را وارد کنید.

وارون‌پذیر بودن Invertibility

می‌گوییم b **وارون‌پذیر پیمانهٔ N** است اگر عددی c وجود داشته باشد به‌طوری‌که:

$$bc = 1 \mod N.$$

- عدد ۰ *هیچ‌وقت* وارون‌پذیر نیست.
- اگر c معکوس b باشد، $[c \mod N]$ هم معکوس b است.
- اگر c و c' هر دو معکوس b باشند،

$$[c' \mod N] = [c \mod N]$$

- یعنی معکوس در بازهٔ ۱ تا N−۱ یکتا است.

در این صورت معکوس b را b^{-1} می‌نامیم.

$$[a/b \mod N] \overset{\text{تعریف}}{=} [ab^{-1} \mod N].$$

وقتی b وارون‌پذیر باشد، تعریف می‌کنیم:

$$ab = cb \mod N$$

و b وارون‌پذیر باشد، می‌توانیم طرفین را در b^{-1} ضرب کنیم و نتیجه بگیریم:

$$a = c \mod N.$$

پیچیدگی محاسبات پیمانه‌ای

چهار عملیات زیر، همگی در زمان چندجمله‌ای انجام‌پذیرند:

- جمع پیمانه‌ای
- تفریق پیمانه‌ای
- ضرب پیمانه‌ای
- یافتن معکوس (اگر وجود داشته باشد)

همچنین:

$$[\mathrm{mod}\ N \quad {}^{b}a]$$

توان‌گیری پیمانه‌ای

حتی اگر bبسیار بزرگ باشد، با روش «توان‌گیری سریع» (square-and-multiply) به‌صورت کارا قابل محاسبه است.

ادبیات تحقیق: تیتر خود را وارد کنید.

9.1.3 گروه‌ها (Groups)

بگذار **G**یک مجموعه باشد.

یک **عمل دوتایی** روی G، تابعی است که دو عنصر از Gرا گرفته و دوباره عنصری از Gبرمی‌گرداند.

به‌جای نوشتن:

$$(g,h)\circ$$

$$h \circ g$$

تعریف گروه – Definition 9.9

یک **گروه** مجموعه‌ای G به‌همراه یک عمل دوتایی ∘ است که چهار شرط زیر را داشته باشد:

۱) بسته‌بودن Closure

$$.G \ni h \circ g$$

۲) وجود عنصر واحد Identity Element

$$.e \circ g = g = g \circ e$$

۳) وجود معکوس Inverse

$$.g \circ h = e = h \circ g$$

این hرا **معکوس** **g**می‌نامیم.

ادبیات تحقیق: تیتر خود را وارد کنید.

بخش سوم: بخش

در این قسمت عنوان اسلاید را وارد کنید

۴) شرکت‌پذیری (Associativity) $(_3g \circ _2g) \circ _1g = _3g \circ (_2g \circ _1g)$.

اگر Gتعداد محدودی عنصر داشته باشد، آن را **گروه متناهی** می‌نامیم و تعداد عناصرش را با |G|نشان می‌دهیم و به آن **رتبهٔ گروه (order)** می‌گوییم.

گروه آبلی Abelian Group

گروه G، **آبلی** است اگر علاوه بر شرایط بالا، خاصیت جابجایی را نیز داشته باشد: $\forall g, h \circ h = h \circ g \quad |g \ni G.$

نمادگذاری جمعی Additive Notation

- عمل گروه: $h + g$
- عنصر واحد: 0:
- معکوس : $g-$
- عبارت $|g - h$

$^{1-}g \cdot h$

باز هم، صرفاً نوع نوشتن است، نه ضربِ واقعی عددی.

روش‌شناسی: تیتر خود را وارد کنید.

مثال 9.10

•مجموعهٔ اعداد صحیح $\mathbb{Z}$ تحت **جمع** → یک گروه آبلی است.

- واحد = ۰
- معکوس g = −g

•ولی $\mathbb{Z}$ تحت **ضرب** → گروه نیست، چون بسیاری از اعداد (مثل ۲) معکوس ندارند.

مثال 9.11

•مجموعهٔ اعداد حقیقی $\mathbb{R}$ تحت ضرب گروه نیست، چون ۰ **معکوس ندارد**.

•اما مجموعهٔ $\mathbb{R}\{0\}$ (حقیقی‌های غیر صفر) تحت ضرب، یک گروه آبلی کامل است.

لم 9.13 – قانون حذف Cancelation Law

$$bc = ac$$

$$.b = a$$

$$c = ac$$

روش‌شناسی: تیتر خود را وارد کنید.

توان‌گیری در گروه‌ها Group Exponentiationاغلب لازم است که «عمل گروهی را m بار روی gتکرار کنیم».

این کار در دو نوع نمادگذاری این‌گونه تعریف می‌شود:

۱) نمادگذاری جمعی

برای عدد صحیح مثبت :m

$$\underbrace{g+g+\cdots+g}_{m\text{ بار}}=mg$$

قوانین:

$$m')g+m)=(m'g)+(mg)$$
$$g('mm)=m(m'g)$$
$$g=1g$$

$$.mh+mg=(h+m(g$$

۲) نمادگذاری ضربی

$$\underbrace{g\cdot g\cdot\cdots\cdot g}_{m\text{ بار}}={}^{m}g$$

$${}^{'m+m}g={}^{'m}g^{m}g$$
$${}^{'mm}g={}^{'m}({}^{m}g)$$
$$g={}^{1}g$$

صفر و توان منفی

$0g = 0$ (واحد گروه)

$m(-g) = g(m-)$

در نمادگذاری ضربی:

$g^{0} = 1$

$g^{m-} = (g^{m})^{1-} = (g^{1-})^{m}$

تعریف مجموعهٔ Z^{*}_{N}

برای هر عدد صحیح $N > 1$، تعریف می‌کنیم:

$$Z^{*}_{N} = \{b \ni \{1-N, \dots, 1\} \mid \gcd(b, N) = 1\}.$$

- عناصر ۱ تا N-۱ را نگاه می‌کنیم
- هر کدام که با N نسبتاً اوّل باشد را نگه می‌داریم
- بقیه حذف می‌شوند

ضرب گروه روی این مجموعه همان **ضرب پیمانه‌ای N** است.

روش‌شناسی: تیتر خود را وارد کنید.

گزاره 9.18 – نتیجهٔ اصلی

برای هر $N > 1$ ، مجموعهٔ Z_N^* تحت ضرب پیمانه‌ای یک گروه آبلی است.

دلیل‌ها:

•عنصر واحد:

۱همیشه در این مجموعه است و نقش واحد را دارد.

دلیل‌ها:

•عنصر واحد:

۱ همیشه در این مجموعه است و نقش واحد را دارد.

•معکوس‌پذیری:

اگر b در Z_N^* باشد، یعنی $\gcd(b,N)=1 \rightarrow$ طبق گزاره ۹٫۷ معکوس دارد.

•بسته‌بودن:

اگر a و b هر دو نسبتاً اوّل با N باشند، آنگاه $ab \mod N$

روش‌شناسی: تیتر خود را وارد کنید.

اگر N = pq باشد (دو عدد اول متمایز):

عددهایی که نسبت به N = pq نسبتاً اوّل نیستند، یا مضرب p اند یا مضرب q، ولی نه هر دو (چون pq از N بزرگ‌تر است).

مضرب‌های p در بازه ۱ تا pq-1 = 1-دقیقاً q-1 عدد

مضرب‌های q = دقیقاً p-1 عدد

$$(1-q)(1-p) = 1+q-p-pq = (1-p)-(1-q)-(1-pq).$$

$$(1-q)(1-p) = \phi(pq).$$

فرمول عمومی برای N مرکّب

$$N = \prod_i p_i^{e_i}$$

$$\phi(N) = (p \prod_i p_i^{e_i-1}(1-p_i).$$

روش‌شناسی: تیتر خود را وارد کنید.

Corollary 9.22 توابع توان‌گیری پرموتیشن می‌شوند

$$x^e \bmod N = f_e(x)$$

یک **پرموتیشن** روی Z_N^* است *اگر شرط زیر برقرار باشد:*

$$\gcd(e, \phi(N)) = 1.$$

معکوس آن، تابع:

$$x^d \bmod N = f_d(x),$$

که d همان معکوس بیمانه‌ای e نسبت به $\phi(N)$ است:

$$e = d^{-1} \bmod \phi(N).$$

این دقیقاً پایهٔ **ساخت RSA** است:

e = توان رمزگذاری

d = معکوس آن نسبت به ϕ(N)

و چون توان‌گیری یک پرموتیشن است، $x \to x^e$ و $x \to x^d$ معکوس هم‌اند.

روش‌شناسی: تیتر خود را وارد کنید.

9.1.5 ایزومورفیسم‌ها و قضیهٔ باقی‌ماندهٔ چینی CRT

دو گروه **ایزومورف** هستند اگر **ساختار جبری یکسانی** داشته باشند.
یعنی همان «گروه» هستند ولی با نام‌گذاری یا نمایش متفاوت.
از دید ریاضی:
•ایزومورفیسم یعنی دو گروه *معادل ساختاری*‌اند.
از دید محاسباتی:
•ایزومورفیسم یعنی می‌توان محاسبات را گاهی با نمایش دیگری **سریع‌تر** انجام داد.
این نکته در رمزنگاری **بسیار حیاتی** است.

تعریف ایزومورفیسم – Definition 9.23

بگذار Gو Hدو گروه باشند با عملیات گروهی و $\cdot_H$ و $\cdot_G$.

$$H \to G : f$$

$$f(g_2) \cdot_H f(g_1) = (2g \cdot_G 1f(g$$

روش‌شناسی: تیتر خود را وارد کنید.

ین یعنی « Gو Hاز نظر ساختار گروهی کاملاً یکسان‌اند».

نکات مهم:

- اگر Gمتناهی باشد و $H \cong G$ ، آنگاه حتماً |G| = |H|.
- اگر fایزومورفیسم باشد، آنگاه f^{-1}نیز ایزومورفیسم است.
- ممکن است fکارا باشد ولی f^{-1}کارا نباشد (یا برعکس).

محصول مستقیم دو گروه Direct Product

اگر G و H دو گروه باشند، گروه **G × H** تعریف می‌شود به‌صورت:

عناصر: تمام زوج‌های (g, h) به‌طوری‌که $G \ni g$ و $H \ni h$.

عمل گروهی: اعمال روی هر مؤلفه جداگانه انجام می‌شود:

$$('h\ {}_H\circ\ g',\ h\ {}_G\circ\ g) = ('g', h) \circ (g, h)$$

روش‌شناسی: تیتر خود را وارد کنید.

قضیهٔ باقی‌ماندهٔ چینی – Theorem 9.24

p و q هر دو عدد اول و نسبتاً اول باشند

$$_q\mathbb{Z} \times _p\mathbb{Z} \cong {}_N\mathbb{Z}$$

$$_q^*\mathbb{Z} \times _p^*\mathbb{Z} \cong {}_N^*\mathbb{Z}$$

این یعنی:

محاسبات پیمانه N را می‌توان به‌صورت کاملاً معادل،

به دو محاسبهٔ جداگانه پیمانه p و پیمانه q تبدیل کرد.

این دقیقاً راز سریع شدن محاسبات در RSA است.

تابع ایزومورفیسم CRT

$$([\bmod q \quad \bmod p], [x \quad x]) = f(x)$$

روش‌شناسی: تیتر خود را وارد کنید.

چرا f عمل گروهی را حفظ می‌کند؟

$$f(b) \oplus f(a) = (\bmod q \quad \bmod p, b \quad b) + (\bmod q \quad \bmod p, a \quad a) = \big([\bmod q \quad b + \bmod p],\ [a \quad b + a]\big) = (b\ {}_N+\ f(a$$

که در آن $\oplus$ جمع مؤلفه‌به‌مؤلفه است.

بنابراین f یک **ایزومورفیسم کامل** است.

نمادگذاری $\big({}_q x_{\,p}, x\big) \leftrightarrow x$

$$\big({}_q x_{\,p}, x\big) \leftrightarrow x$$

$$.[\bmod q \quad x] = {}_q\bmod p], \qquad x \quad x] = {}_p x$$

$$3 = q\ ,5 = p \quad ,14 = x$$

$$2 = \bmod 3 \quad 14 \qquad ,4 = \bmod 5 \quad 14$$

$$.(2\ ,4) \leftrightarrow 14$$

$$\prod_{i=1}^{\ell} {}_i p = N$$

$${}_{\ell p}\mathbb{Z} \times \cdots \times {}_{1p}\mathbb{Z} \cong {}_N\mathbb{Z}$$

$${}^*_{\ell p}\mathbb{Z} \times \cdots \times {}^*_{1p}\mathbb{Z} \cong {}^*_N\mathbb{Z}$$

نسخهٔ عمومی CRT

روش‌شناسی: تیتر خود را وارد کنید.

مثال 9.25 – ایزومورفیسم $\mathbb{Z}_{15}^*$

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

x	(x mod 5, x mod 3)
1	(1,1)
2	(2,2)
4	(4,1)
7	(2,1)
8	(3,2)
11	(1,2)
13	(3,1)
14	(4,2)

روش‌شناسی: تیتر خود را وارد کنید.

اهمیت محاسباتی – CRT چرا فوق‌العاده مهم است؟

اگر G و H دو گروه باشند و ایزومورفیسم کارا بینشان وجود داشته باشد:

- می‌توان عملیات را یا در G انجام داد
- یا آن را به H منتقل کرد، محاسبه کرد، و دوباره برگرداند.

این کار فقط وقتی مفید است که عملیات در H سریع‌تر باشد.

برای حالت:N = pq

عملیات پیمانه N را می‌توان به دو عملیات پیمانه p و پیمانه q تبدیل کرد

—که فوق‌العاده سریع‌تر هستند.

این تکنیک، اساسِ:

- سریع‌سازی رمزگشاییRSA ،
- الگوریتم‌های توان‌گیری،
- و حتی بعضی حملات رمزنگاری مانند CRT-fault attacks است.

9.2 اعداد اوّل، فاکتورگیری و RSA

در این بخش، اولین نمونهٔ جدی از **مسائل سخت عددنظری** را بررسی می‌کنیم:

مسئلهٔ *فاکتورگیری یک عدد مرکّب*.

این مسئله یکی از قدیمی‌ترین مسائل سخت شناخته‌شده است،

و پایهٔ سیستم رمزنگاری RSAنیز بر همین سختی بنا شده است.

مسئلهٔ فاکتورگیری Integer Factorization

ورودی: عدد صحیح مرکّب N

هدف: پیدا کردن دو عدد $1 < p, q$ که:

$$.N = pq$$

می‌توانیم برای p از 2 تا $\lfloor \sqrt{N} \rfloor$ امتحان کنیم که آیا p، N را تقسیم می‌کند یا نه.

این روش:

تعداد حدود $\sqrt{N}$ بار تست نیاز دارد

هر تست خودش عملیات با زمان poly(log N) دارد

پس کل زمان آن تقریباً:

$$(\text{polylog}(N) \cdot \sqrt{N})O$$

روش‌شناسی: تیتر خود را وارد کنید.

برای فاکتورگیری سخت واقعی، چه می‌خواهیم؟

می‌خواهیم N فقط عامل‌های بزرگ داشته باشد.

یعنی و باید خودشان عدد اوّل باشند.

به همین دلیل، در نسخهٔ رسمی فرض سختی فاکتورگیری:

- به‌جای گرفتن دو عدد-n بیتی معمولی،
- دو عدد-n بیتیِ اوّل انتخاب می‌کنیم.

به این ترتیب، Nاحتمال بسیار کمی دارد که عامل کوچک داشته باشد،

و مسئلهٔ فاکتورگیری واقعاً سخت می‌شود.

اما برای این کار، لازم است بتوانیم:

اعداد اوّل بزرگ را کارا تولید کنیم.

این دقیقاً موضوع بخش بعد است.

آزمایش سختی فاکتورگیری

برای بررسی اینکه «آیا فاکتورگیری سخت است»، آزمایشی تعریف می‌شود:

آزمایش Aw-Factor (n)

برای یک الگوریتم A و پارامتر n:

دو عدد n-بیتی یکنواخت و تصادفی x_1, x_2 انتخاب می‌کنیم.

عدد $N = x_1 \cdot x_2$ را می‌سازیم.

الگوریتم A عدد N را می‌گیرد و تلاش می‌کند دو عدد $x'_1, x'_2 > 1$ خروجی دهد.

خروجی آزمایش ۱ است اگر:

$$N = x'_1 \cdot x'_2,$$

روش‌شناسی: تیتر خود را وارد کنید.

9.2.1 تولید اعداد اوّل تصادفی Generating Random Primes

یک روش طبیعی برای تولید یک عدد اوّل -nبیتی:

1.یک عدد -nبیتی تصادفی انتخاب کن.

2.تست کن که آیا اوّل است یا نه.

3.اگر اوّل نبود، تکرار کن.

مشکل اصلی: چگونه بفهمیم pاوّل است؟

این سؤال در ۲۰۰۰ سال ریاضیات همیشه مهم بوده.

روش‌های قدیمی

تست اوّل بودن بسیار کند بودند.

دهۀ ۱۹۷۰

اولین **آزمایش‌های تصادفی سریع** آمدند:

- اگر pاوّل بود → همیشه می‌گفت «prime»
- اگر pمرکّب بود → تقریباً همیشه درست می‌گفت «composite»

اما با احتمال بسیار ناچیز، اشتباه کرده و می‌گفت «prime»

روش‌شناسی: تیتر خود را وارد کنید.

یعنی:

•جواب compositeهمیشه قطعی است

•جواب primeاحتمال خطای بسیار کوچکی دارد

در عمل این کاملاً قابل قبول است.

سال 2002

یک الگوریتم **قطعی** و **چندجمله‌ای** برای تست اوّل بودن کشف شد (قضیهٔ .(AKS

اما:

•کندتر از نسخه‌های تصادفی است

•پس در عمل هنوز هم روش‌های تصادفی سریع (مثل Miller–Rabin)استفاده می‌شود.

9.2.2 آزمون اول‌بودن Miller–Rabin

در این بخش، آزمون میلر–رابین را توضیح می‌دهیم و درست‌بودنش را ثابت می‌کنیم.
)این آزمون برای ادامهٔ کتاب لازم نیست، اما فهم آن دید عمیقی دربارهٔ ساختار گروهی پیمانهٔ N
و تشخیص اول‌بودن می‌دهد.
کل ایده این است که:
برای تشخیص این‌که N اول است یا مرکّب،
باید یک ویژگی رفتاری پیدا کنیم که
همهٔ اعداد اول دارند
و بسیاری از اعداد مرکّب ندارند.

نقطهٔ شروع آزمون

اگر N یک عدد اول باشد، آنگاه:
مجموعهٔ $\mathbb{Z}_N^*$ دقیقاً شامل $N-1$ عضو است
و طبق قضیهٔ 9.14 داریم:

$$a^{N-1} \equiv 1 \mod N \quad \text{برای هر } a \in \{1, \ldots, N-1\}.$$

روش‌شناسی: تیتر خود را وارد کنید.

ایدهٔ کلیدی میلر–رابین

$$d \cdot {}^{s}2 = 1 - N$$

که در آن:

- dیک عدد **فرد** است
- 1 ≤ sتعدادِ توان‌های ۲ است

آنگاه:

$$\cdot {}^{s}2\left({}^{d}a\right) = {}^{d}{}^{s}2a = {}^{N-1}a$$

$$\cdot {}^{s}2\left({}^{d}a\right) = {}^{d}{}^{s}2a = {}^{N-1}a$$

پس تعیین اول‌بودن Nرا می‌توان با بررسی **توالی توان‌های مربعی‌شده** زیر انجام داد:

$$\left|\cdot {}^{N-1}a = {}^{d}{}^{s}2a^{d},\ a^{2d},\ a^{4d},\ \ldots,\ a\right.$$

روش‌شناسی: تیتر خود را وارد کنید.

ویژگی عددهای اول در این توالی

اگر Nاول باشد، آنگاه:

•یا $a^d \equiv 1 \mod N$

•یا در توالی بالا، **اولین باری که مقدار 1 ظاهر می‌شود** خروجی مرحله‌ای است که مقدار قبلی‌اش = −1 بوده باشد

یعنی در اعداد اول، «۱» در این توالی **ناگهانی** ظاهر می‌شود،

و قبل از آن باید مقدار −1 وجود داشته باشد.

اگر هیچ‌کدام از این اتفاق‌ها نیفتد، Nمرکّب است.

احتمال اشتباه $\leq \left(\frac{1}{4}\right)^t = 2^{-2t}$.

نسخهٔ کتاب که از bound ساده‌تر استفاده می‌کند، می‌گوید:

احتمال اشتباه $\leq 2^{-t}$.

رفتار اعداد مرکّب

اگر N مرکّب باشد، اکثر انتخاب‌های تصادفیa ،

توالی مناسب را تولید نمی‌کنند.

میلر–رابین ثابت می‌کند:

برای هر N مرکّب،

حداقل ¾ از انتخاب‌هایa ،

Nرا افشا می‌کنند

و نشان می‌دهند N مرکّب است.

بنابراین اگر t بار آزمایش کنیم:

روش‌شناسی: تیتر خود را وارد کنید.

بیانیهٔ رسمی — Theorem 9.33

قضیه 9.33.

اگر Nعدد اول باشد، آزمون میلر–رابین **همیشه** خروجی prime می‌دهد.

اگر Nمرکّب باشد، آزمون میلر–رابین با احتمال **حداکثر** خروجی اشتباه prime می‌دهد.

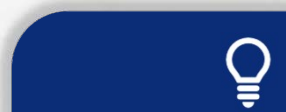
بنابراین:

- اگر میلر–رابین بگوید composite، ۱۰۰٪ درست است.
- اگر بگوید prime، با احتمال بسیار زیاد درست است.

همین باعث شده این تست **استاندارد صنعت رمزنگاری** باشد.

بخش چهارم: تحلیل داده‌ها

در این قسمت عنوان اسلاید را وارد کنید



انتخاب موضوع

لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ است.

انتخاب موضوع

لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ است.

انتخاب موضوع

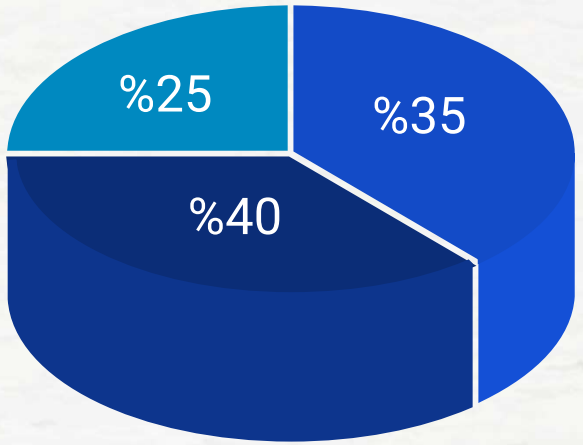
لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ است.

لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است. چاپگرها و متون بلکه روزنامه و مجله در ستون و سطرآنچنان که لازم است. لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است. چاپگرها و متون بلکه روزنامه و مجله در ستون و سطرآنچنان که لازم است.

تحلیل داده‌ها: تیتر خود را وارد کنید.

در این قسمت عنوان اسلاید را وارد کنید

لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است. چاپگرها و متون بلکه روزنامه و مجله در ستون و سطرآنچنان که لازم است.



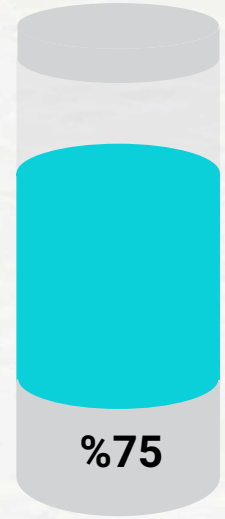
- لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است.
- لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است.
- لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است.

تحلیل داده‌ها: تیتر خود را وارد کنید.

در این قسمت عنوان اسلاید را وارد کنید

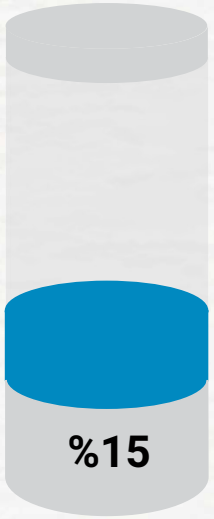
تیتر را وارد کنید.

لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از طراحان گرافیک است.



تیتر را وارد کنید.

لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از طراحان گرافیک است.



تیتر را وارد کنید.

لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از طراحان گرافیک است.

تیتر را وارد کنید.

لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از طراحان گرافیک است.

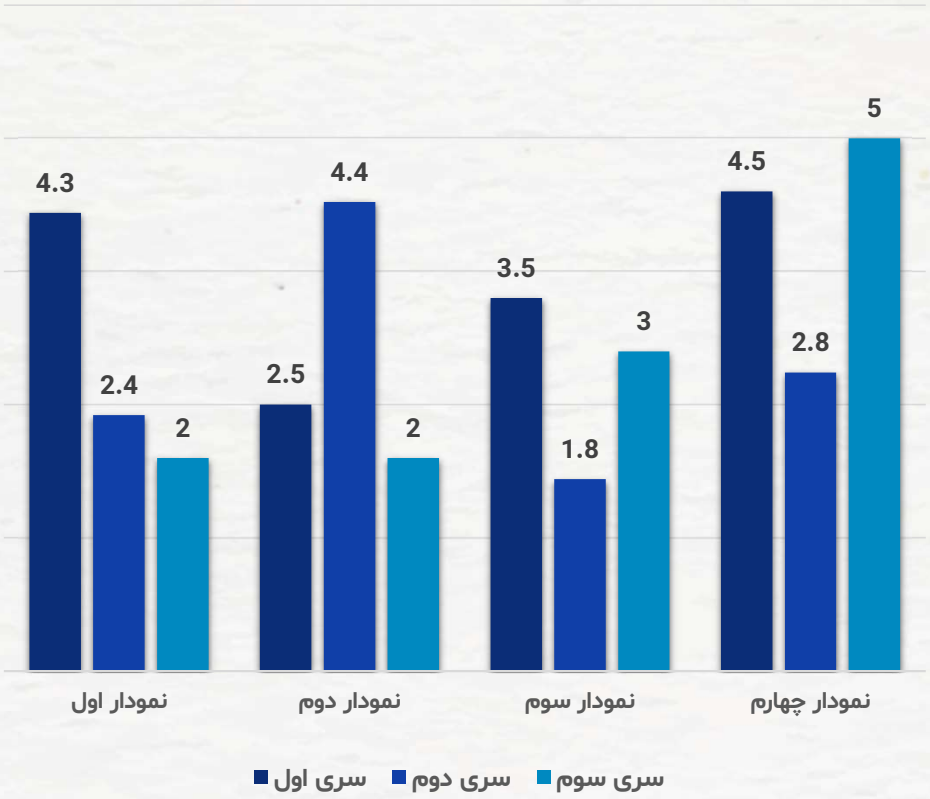
تیتر را وارد کنید.

لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از طراحان گرافیک است.

تحلیل داده‌ها: تیتر خود را وارد کنید.

در این قسمت عنوان اسلاید را وارد کنید

لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است. چاپگرها و متون بلکه روزنامه و مجله در ستون و سطرآنچنان که لازم است و برای شرایط فعلی تکنولوژی مورد نیاز و کاربردهای متنوع با هدف بهبود ابزارهای کاربردی می باشد. لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است.



تحلیل داده‌ها: تیتر خود را وارد کنید.

در این قسمت عنوان را وارد کنید

1. لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است.
2. چاپگرها و متون بلکه روزنامه و مجله در ستون و سطرآنچنان که لازم است.
3. شرایط فعلی تکنولوژی مورد نیاز و کاربردهای متنوع با هدف بهبود ابزارهای کاربردی می باشد. لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است.
4. لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است.
5. چاپگرها و متون بلکه روزنامه و مجله در ستون و سطرآنچنان که لازم است.
6. شرایط فعلی تکنولوژی مورد نیاز و کاربردهای متنوع با هدف بهبود ابزارهای کاربردی می باشد. لورم ایپسوم متن ساختگی با تولید سادگی نامفهوم از صنعت چاپ و با استفاده از طراحان گرافیک است.

منابع و مراجع: تیتر خود را وارد کنید.

با تشکر از همه شما عزیزان