"باسمه تعالی"

تمرین سری اول

مبانی رمزنگاری و امنیت شبکه

"پوریا لادخواه _ ۹۴۱۰۴۲۸۵"

"دکتر میرمحسنی"

** سوال ۱ : در انتهای سوالات نوشته شده است **

۲_

a) $7x \overset{3}{\equiv} 5 \Rightarrow (1)x \overset{3}{\equiv} 2 \Rightarrow x = 3k+2$

$7 \overset{3}{\equiv} 1$, $5 \overset{3}{\equiv} 2$

b) $15x \overset{25}{\equiv} 10 \Rightarrow \frac{15}{5} x \overset{\frac{25}{5}}{\equiv} \frac{10}{5} \Rightarrow 3x \overset{5}{\equiv} 2 \Rightarrow -2x \equiv 2 \overset{(5,2)=1}{\Rightarrow} x \overset{5}{\equiv} -1$

$\Rightarrow x = 5k-1$

c) $3x \overset{12}{\equiv} 7 \Rightarrow 12 / 3x-7 \Rightarrow 12k = 3x - 7$

$3/12k$, $3/3x$ $\Rightarrow 3/7$ اصلن پذیر نیست.

=> چنین x ای وجود ندارد.

۳_

فرض) $\begin{cases} n \overset{\varphi(m)}{\equiv} n' \\ (a, m) = 1 \end{cases}$ حکم) $a^n \overset{m}{\equiv} a^{n'}$

* می‌دانیم $a^{\varphi(m)} \overset{m}{\equiv} 1$ ✓ $(a,m)=1$ اگر

* طبق فرض $n = \varphi(m) q + r$, $n' = \varphi(m) q' + r$, $r < \varphi(m)$

$\Rightarrow a^n \overset{m}{\equiv} a^{\varphi(m) q + r} \overset{m}{\equiv} (a^{\varphi(m)})^q \cdot a^r \equiv a^r$

$a^{n'} \overset{m}{\equiv} a^{\varphi(m) q' + r} \equiv \dots \equiv a^r$ ✓

$\Rightarrow a^n \overset{m}{\equiv} a^{n'}$ ∎

۴_ a)

Index	A	B	C
1	6150	704	1
2	3075	352	2
3	3075	176	2
4	3075	88	2
5	3075	44	2

Index	A	B	C
6	3075	22	2
7	3075	11	2
8	3064	11	2
9	1532	11	2
10	766	11	2

"ادامه صفحه بعد"

	A	B	C
11	765	11	2
12	383	11	2
13	372	11	2
14	186	11	2
15	93	11	2
16	82	11	2
17	41	11	2
18	30	11	2

	A	B	C
19	15	11	2
20	4	11	2
21	2	11	2
22	1	11	2
23	1	10	2
24	1	5	2
25	1	4	2
26	1	2	2
27	1	1	2

$\Rightarrow (6150, 764) = 2 \times 1$

$= 2$ ✓

توضیح روش کار الگوریتم:

ابتدا می‌بینیم که عدد $\geq$ تعداد عامل شش‌تایی "۲" در دو عدد A و B را ذخیره می‌کند. یعنی در ابتدا تا جایی که هردو عدد A و B، عدد C حداقل عامل ۲ دارند، تعداد ۲ در C افزایش می‌یابد و با رسیدن به min تعداد عامل ۲ در A یا B، عدد C در ادامه روند دست نخورده می‌ماند. چرا که C تنها در صورتی تغییر می‌کند که هردو عدد A_i و B_i زوج باشند و در ادامه باتوجه به اینکه در این مرحله یکی از ۲ عدد فرد شده است در مرحله بعد یا دیگری زوج بوده و متوالیاً تقسیم بر ۲ می‌شود تا فرد شود (که در این راه C ثابت است) یا ۲ عدد فرد (مساوی) می‌رسیم که در مرحله‌ی بعد آن‌ای نیز یکی فرد (min) و دیگری زوج ($|A_i - B_i|$) خواهد بود.

حال روند تغییر این الگوریتم تقاوتی با اقلیدس این است که از دو تغییر داده‌شده اقلیدس در حد $a-b$ بود و در این الگوریتم $\frac{a-b}{2}$ می‌باشد چرا که از آن جایی که ما تمام عامل‌های ۲ را در C ذخیره کردیم $(a', b') = (a', \frac{b'}{2})$ می‌باشد که (a', b')، همان (a, b) بدون کوچک‌ترین عوامل ۲ هستند.

پس بهبود این روش سریع‌تر انجام یافتن آن می‌باشد. ✓

$P_1 < P_2 < \cdots < P_n$

$X = 1 + P_1 P_2 \cdots P_n$

* می‌دانیم X یک عدد طبیعی است پس یا خودش اول است و یا یک عدد اول که بزرگترین عامل اول موجود است.

$X \begin{cases} \text{یا } X = P_m & \text{اول} \\ \text{یا } \exists\, 1 \quad P_m < X : \; P_m \mid X \checkmark \end{cases}$ <= P_m یک عدد اول که از همه اعداد اول بزرگتر است

* از طرفی P_m نمی‌تواند هیچ یک از P_i ($1 < i < n$) باشد چرا؟

می‌دانیم برای اعداد اول P و عدد دلخواه x : $P_m \mid X \Rightarrow (P_m, X-1) = 1$

$\Rightarrow (P_m, P_1 P_2 \cdots P_n) = 1 \Rightarrow (P_m, P_i) = 1 \quad ; \; 1 \le i \le n$

* P_m نسبت به همه‌ی اعداد اول فوق اول است $\Leftarrow$ P_m خودش یک عدد اول جدید است!

پس فرض این که $P_1, \ldots, P_n$ همه‌ی اعداد اول موجود اند غلط است و یا به این خاطر که تعداد اعداد اول ناتمامی است ■

* حال دیدیم $P_m > P_n$ و $P_m \mid 1 + P_1 \cdots P_n$ ، $P_1 < P_2 < \cdots < P_n$ پس حتماً $P_n < P_m < 1 + P_1 \cdots P_n$

بنابراین یا $P_m = P_{n+1}$ است و یا یک عدد اول دیگر P'_m وجود دارد که $P_n < P'_m < P_m$ و $P_{n+1} = P'_m$

در هر دو صورت عدد اول P_{n+1} از $1 + P_1 P_2 \cdots P_n$ کوچک‌تر خواهد بود ✓

$P_{n+1} < 1 + P_1 \cdots P_n$ ■

۶_

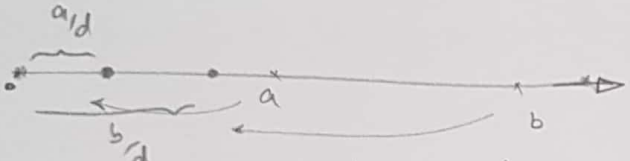
* ابتدا ارتباط می‌سنجیم اگر $(a,b)=d$ آنگاه $\left(\frac{a}{d},\frac{b}{d}\right)=1$ چرا:

$(a,b)=d \iff a=a'\times d,\ b=b'\times d \xrightarrow{\text{which}} (a',b')=1$

یعنی a' و b' سهل اول نسبی
ندارند و گرنه در d ضرب می‌شدند

$\iff (a',b')=1 \iff \left(\frac{a}{d},\frac{b}{d}\right)=1$ ✓

حال اگر $P=Pr((a,b)=1)$ آن‌گاه احتمال هر عضو a و b شود $\frac{1}{d}$ شود، احتمال نیز $(\times\frac{1}{d}\times\frac{1}{d})$ می‌شود:



$$Pr\left(\left(\frac{a}{d},\frac{b}{d}\right)=1\right) = P\times\frac{1}{d}\times\frac{1}{d} = \frac{P}{d^2}$$

* حال می‌دانیم جمع تمام احتمالات ممکن برابر ۱ است:

$$\sum_{d\geq 1} Pr((a,b)=d) = 1 \Rightarrow \sum_{d\geq 1} Pr\left(\left(\frac{a}{d},\frac{b}{d}\right)=1\right) = 1$$

$$\Rightarrow \sum_{d\geq 1}\frac{P}{d^2}=1 \Rightarrow P\left(\frac{1}{1}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots\right) = P\times\frac{\pi^2}{6} = 1$$

(مجموع زیتای عدد ۲ سؤال)

$$\sum_{i=1}^{\infty}\frac{1}{i^2}=\frac{\pi^2}{6}$$

$$\Rightarrow P=\frac{6}{\pi^2}\simeq 0.6079$$ ✓ ☑

1 -

Attack / Mechanism	Realse of message	Traffic Analysis	Masquerade	Reply	Modification of message	Denial of servic
Encipherment	Y	–	–	–	–	–
Digital Sig	–	–	Y	Y	Y	–
Access Control	Y	Y	Y	Y	–	Y
Data Integrity	–	–	–	Y	Y	–
Aunthentication exchange	Y	–	Y	Y	–	Y
Traffic padding	–	Y	–	–	–	–
Routing Control	Y	Y	–	–	–	Y
Noturization	–	–	Y	Y	Y	–

*** تمرین کامپیوتری هم در فایل ZIP آپلود شده به زبان python نوشته شده است.