رامتین احسانی - ۹۷۵۲۱۰۱۸

تمرین دوم - امنیت سیستم های کامپیوتری

۱- الگوریتم های متعددی برای تجزیه اعداد اول معرفی شده اند. از بهترین های آن ها میتوان به الگوریتم Pollard's rho اشاره کرد که دارای پیچیدگی زمانی $O(\sqrt{P})$ است که برای اعداد کوچکتر از 2^70 مناسب است.

۲- به اعدادی نیمه اول گفته میشود که میتوان آن ها را به صورت ضرب دو عدد اول نوشت. بله تجزیه این اعداد ساده تر است.

۳- الگوریتم های متعددی برای تجزیه اعداد وجود دارند.

- الگوریتم Pollard's rho دارای پیچیدگی زمانی $O(\sqrt{P})$ است که برای اعداد کوچکتر از 2^70 مناسب است.
- برای اعداد کوچکتر از 10^50 الگوریتم Lenstra elliptic curve factorization مناسب است که دارای پیچیدگی زمانی exp[(√2 + o(1)) √ln p ln ln lnp] است.
- برای اعداد کوچکتر از 10^100 الگوریتم quadratic sieve مناسب است که دارای پیچیدگی زمانی زیر است:

$$e^{(1+o(1))\sqrt{\ln n \ln \ln n}} = L_n\left[1/2, 1\right]$$

- برای اعداد بزرگتر از 10^100 هم الگوریتم general number field sieve (GNFS) مناسب است که پیچیدگی زمانی زیر را دارد:

$$\exp\left(\left(\sqrt[3]{\frac{64}{9}} + o(1)\right)(\ln n)^{\frac{1}{3}}(\ln \ln n)^{\frac{2}{3}}\right) = L_n\left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right]$$