

# اولین دوره لیگ برنامه‌نویسی

## دانش‌آموزی به سبک ACM

### هفته هفتم سوال ۵۰ امتیازی

در یک سرزمین دورافتاده، یک پیام‌رسان شجاع به نام آریا وظیفه دارد تا پیام‌های مهم را به پادشاه برساند. اما این پیام‌ها باید به گونه‌ای رمزنگاری شوند که کسی نتواند آن‌ها را بخواند. بنابراین، آریا یک روش رمزنگاری خاص برای حفاظت از پیام‌ها ایجاد می‌کند.

مراحل رمزنگاری پیام:

۱. انتخاب کلیدها:

- آریا دو عدد اول متمایز  $p$  و  $q$  انتخاب می‌کند.
- سپس مقدار  $n$  را به صورت  $n = p \times q$  محاسبه می‌کند.
- بعد از آن، مقدار  $\phi(n)$  را محاسبه می‌کند که برابر است با  $\phi(n) = (p-1) \times (q-1)$ .

۲. انتخاب عدد  $e$ :

- آریا عددی به نام  $e$  انتخاب می‌کند که باید نسبت به  $\phi(n)$  اول باشد.

۳. رمزنگاری پیام:

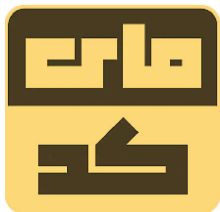
- هر کاراکتر پیام با رعایت ترتیب به عددی در بازه ۱ تا ۲۶ تبدیل می‌شود.
- سپس برای هر عدد  $M$ ، پیام رمزنگاری شده  $C$  با استفاده از فرمول  $C = M^e \bmod n$  محاسبه می‌شود.
- نتایج رمزنگاری شده به صورت یک رشته از اعداد جدا شده با کاما برگردانده می‌شود.

۴. خروجی:

- اگر  $e$  و  $\phi(n)$  نسبت به هم اول باشند، پیام رمزنگاری شده برگشت داده می‌شود.
- اگر  $e$  و  $\phi(n)$  نسبت به هم اول نباشند، عبارت  $NOK$  برگشت داده می‌شود.

ورودی:

- ورودی به صورت یک خط و شامل چهار بخش است که با , از هم جدا شده‌اند.
- دو عدد اول  $p$  و  $q$ .



# اولین دوره لیگ برنامه‌نویسی

## دانش‌آموزی به سبک ACM

هفته هفتم سوال ۵۰ امتیازی

- عدد  $e$ .
  - پیام متنی  $M$  که باید رمزنگاری شود.
- در ادامه نمونه‌ای از فایل ورودی و خروجی مورد نظر را می‌توانید مشاهده کنید.

INPUT.TXT	OUTPUT.TXT
۳,۷,۴, ZORRO	NOK
۵,۱۳,۵, HELLO	۸,۵,۱۲,۱۲,۴۵
۷,۱۳,۵, code	۶۱,۷۱,۲۳,۳۱