مسئله:

تصمیم داریم ارتباط بین **یک سرور و چندین کلاینت** را به گونه ای ایجاد کنیم که کلاینت ها یک رشته دریافتی از کاربر را به Encryption Server ارسال کرده و سرور با استفاده از Private Key که در اختیار دارد، رشته ارسالی را رمز گذاری کرده و رشته رمز گذاری شده را به کلاینت بر می‌گرداند.

شرح مسئله:

سرور یک ماتریس Private Key را بصورت زیر در اختیار دارد،

$$\text{Private Key}=\begin{bmatrix}1 & 2\\ -1 & 2\end{bmatrix}$$

کلاینت‌ها پس از دریافت رشته ورودی از کاربر می‌بایست آنرا به یک ماتریس با ابعاد مناسب با مقادیر درایه های کد اسکی کارکترهای ورودی تبدیل کرده و به سرور جهت رمزگذاری ارسال کنند. سرور پس از دریافت ماتریس ورودی و با داشتن ماتریس Private Key رشته خروجی رمزگذاری شده را با استفاده از ضرب ماتریس‌ها تولید کرده وآن را به کلاینت برمی‌گرداند، سپس رشته رمزگذاری شده در خروجی چاپ می‌گردد.