





گزارش تمرین اول سیستم‌های توزیع شده

گزارش

مبینا کاشانیان

۱۴۰۰-۱۴۰۱

فهرست مطالب

۱	فصل ۱ گزارش تمرین سوکت	۱
۱	۱.۱ چکیده	۱
۱	۲.۱ شرح دقیق مسئله	۱
۱	۳.۱ پیاده سازی	۱
۲	۱.۳.۱ ایده حل مسئله	۲
۲	۲.۳.۱ رمزگذاری	۲
۲	۳.۳.۱ رمزگشایی	۲
۲	۴.۱ تصویر عملکرد برنامه	۲

۱ گزارش تمرین سوکت

۱.۱ چکیده

در تمرین اول درس سیستم‌های توزیع شده باید با استفاده از برنامه نویسی سوکت، ارتباطی میان کلاینت و سرور برقرار می‌کردیم و کلاینت رشته‌ای را از کاربر گرفته و سپس آن را به سمت سرور ارسال کرده و سرور نیز در پاسخ به این رشته، متن رمز شده آن را برمیگرداند. در قسمت دوم با داشتن متن رمز شده باید توسط سرور دیگری به متن اصلی دست پیدا می‌کردیم.

۲.۱ شرح دقیق مسئله

سرور در سمت خود یک کلید خصوصی به صورت زیر دارد :

$$\begin{bmatrix} 1 & 2 \\ -1 & 2 \end{bmatrix} \quad (۱.۱)$$

کلاینت بعد از دریافت رشته از کاربر ابتدا آن را به یک ماتریس با درایه های کد اسکی کارکترهای ورودی تبدیل کرده و به سرور جهت رمزگذاری ارسال می‌کند. سرور پس از دریافت ماتریس ورودی و رشته خروجی رمزگذاری شده را با استفاده ضرب ماتریسی کلید خصوصی و متن اصلی می‌سازد و به کلاینت برمیگرداند.

۳.۱ پیاده سازی

پیاده سازی این مسئله هم برای رمزگذاری و هم رمزگشایی انجام شده است.

- پورت سرور رمزگذار : ۳۳۳۳
- پورت سرور رمزگشا : ۴۴۴۴

۱.۳.۱ ایده حل مسئله

با توجه به اینکه متن رمز شده از طریق ضرب ماتریسی محاسبه می شود.

باید به چندین نکته در خصوص ماتریس ها توجه داشت:

۱. تعداد ستون های ماتریس اول باید با تعداد سطرهای ماتریس دوم برابر باشد.
۲. سطرهای ماتریس حاصل ضرب به تعداد سطرهای ماتریس اول و ستون های آن نیز به تعداد ستون های ماتریس دوم سطر خواهد بود.
۳. برای محاسبه ماتریس معکوس، ماتریس باید مربعی باشد و دترمینان این ماتریس باید غیر صفر باشد. (در رمزگشایی استفاده می شود)

با توجه به قواعد موجود در ماتریس ها ، در قدم اول باید ورودی را متناسب با ابعاد کلید خصوصی کرد برای اینکار، ورودی را در قالب یک ماتریس با تعداد ستون ثابت دو و سطرهای متغیر در نظر گرفتیم. اگر طول متن ورودی زوج بود سطر ها کاملا پر میشوند اما اگر طول متن فرد باشد یک سطر را به ماتریس اضافه کرده و یک درایه آن را صفر (بی اثر) می کنیم.

۲.۳.۱ رمزگذاری

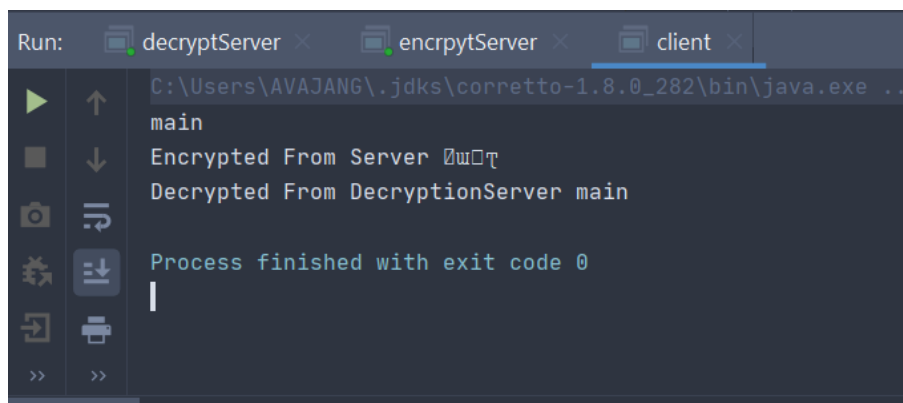
برای رمزگذاری در ابتدا ورودی کاربر را در یک متغیر ذخیره کرده و سپس طول آن را محاسبه می کنیم اگر طول را بر ۲ تقسیم کنیم تعداد سطر ها مشخص می شود حال اگر طول رشته فرد باشد یک آرایه دو ستونی و تعداد سطرها مجموع عدد یک با حاصل تقسیم طول متن ورودی بر دو می باشد. پس از مشخص شدن تعداد سطرهای ماتریس، ماتریس را تشکیل می دهیم و درایه به درایه آن را با ورودی کاربر پر میکنیم و هر حرف را متناظر کد اسکی آن را در ماتریس ثبت میکنیم. پس از آن ارتباط با سرور را برقرار کرده و طول سطر ها را به سمت سرور میفرستیم و سپس تک تک درایه ها را نیز برای سرور ارسال کرده و در سمت سرور ماتریس دوبعدی تشکیل میگردد حال پس از تشکیل این ماتریس در سمت سرور آن را با کلید خصوصی ضرب میکنیم و درایه های ماتریس حاصل درایه های متن رمزگذاری شده هستند که پس از مشخص شدن تمامی درایه ها آن را به کاراکتر تبدیل کرده و به متن رمز شده میرسیم این متن را به همراه آرایه دوبعدی به سمت کلایت ارسال میکنیم.

۳.۳.۱ رمزگشایی

برای رمزگشایی نیازمند یک سرور جدا هستیم با توجه به اینکه در مرحله رمزگذاری ماتریس رمزگذاری را برای کلایت فرستادیم. اینبار کلایت ماتریس رمزگذاری شده را برای سرور رمزگشا میفرستد و سرور رمزگشا نیز از روی کلید خصوصی ماتریس وارون را حساب کرده و سپس متن رمز شده را با کلید خصوصی وارون ضرب کرده و به متن اصلی میرسیم.

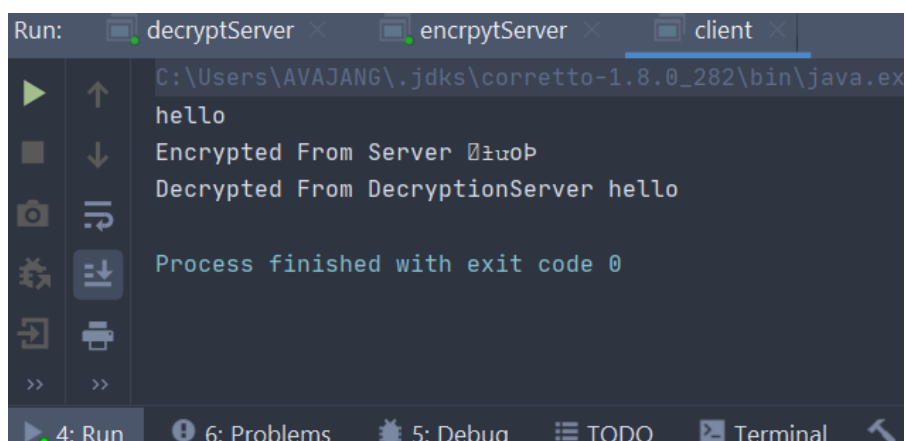
۴.۱ تصویر عملکرد برنامه

نمونه های تصویر عملکرد برنامه را در شکل ۱.۱ و شکل ۲.۱ مشاهده می کنید.



```
Run: decryptServer x encryptServer x client x
C:\Users\AVAJANG\.jdk\corretto-1.8.0_282\bin\java.exe .
main
Encrypted From Server 0x0000000000000000
Decrypted From DecryptionServer main
Process finished with exit code 0
```

شکل ۱.۱: نمونه برنامه با کلمه main



```
Run: decryptServer x encryptServer x client x
C:\Users\AVAJANG\.jdk\corretto-1.8.0_282\bin\java.exe
hello
Encrypted From Server 0x0000000000000000
Decrypted From DecryptionServer hello
Process finished with exit code 0
4: Run 6: Problems 5: Debug TODO Terminal
```

شکل ۲.۱: نمونه برنامه با کلمه hello