دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

پروژه پیاده سازی دوم

احراز هویت و امضای دیجیتال

درس مبانی امنیت اطلاعات

استاد: دکتر نستوه طاهری جوان

تیم تدریسیاری:

رضا توسلی

سید سجاد پیشوائیان

خرداد 1399

احراز هویت:

در این فاز از پروژه قصد داریم امنیت پیام رسان خود را کمی بیشتر کنیم. بدین منظور می بایست ابتدا کاربرانی که قصد ارتباط با یکدیگر را دارند احراز هویت نماییم. همانطور که در پیام رسان های مرسوم مشاهده می کنید، کاربران زیادی به سرور پیام رسان متصل هستند و هر کاربر با کاربر یا کاربران خاصی در ارتباط می باشد. از آنجا که این سرور نیاز دارد تا از اتصال عوامل ناخواسته جلوگیری کند و در نتیجه استفاده بهینه از منابع در دسترس داشته باشد، نیاز دارد تا کاربرانی را که متصل می شوند احراز هویت کند.

بدین گونه می بایست بر اساس فاکتور های اول یا دوم احراز هویت که در پیوست مشخص شده و پروتکل های موجود(نه لزوما پروتکل های پیوست بلکه میتوانید هر پروتکل دیگری نیز استفاده نمایید) **مکانیزمی برای احراز هویت کاربرانی که به سرور پیام رسان شما وصل میشوند طراحی کنید.**

پیشنهاد می شود از روش های احراز هویت بر پایه token استفاده نمایید که کتابخانه های مرتبط با آن برای اغلب زبان های برنامه نویسی موجود است.

امتیازی: پس از آنکه مکانیزمی برای احراز هویت کلاینت به سرور پیاده سازی نمودید، مکانیزمی طراحی کنید که سرور نیز به کلاینت احراز هویت شود. در این مورد پروتکل ها و فاکتورهای مربوطه را شخصا مطالعه نمایید.

امضای دیجیتال:

در فاز اول پروژه، صحت داده را بررسی کردیم و دیدیم که با رمزنگاری نا متقارن می‌توان صحت و محرمانگی محتوای ارسال‌شده را تضمین کرد. مشکلی که هنوز وجود دارد عدم صحت منبع داده است در این بخش صحت منبع داده را با استفاده از امضای دیجیتال بررسی می‌کنیم. در امضای دیجیتال پیام با استفاده از کلید خصوصی فرستنده رمزنگاری می‌شود و با استفاده از کلید عمومی فرستنده نیز رمزگشایی می‌شود.

محتوای امضا شامل فرستنده، گیرنده، نوع داده و زمان ارسال داده است. فرستنده این محتوا را

1. با کلید خصوصی خود رمز می‌کند و برای سرور ارسال می کند،
2. سرور با کلید عمومی فرستنده رمزگشایی می کند(پس از رمز گشایی گیرنده مشخص می شود و به وسیله جدولی که در قسمت پیاده سازی نموده اید، سرور نیز گیرنده را پیدا می کند)
3. سرور با کلید خصوصی خود رمز میکند و برای گیرنده می‌فرستد.
4. گیرنده با دریافت این محتوا و مراجعه به جدولی که برای نگهداری کلیدهای عمومی و خصوصی داشته‌است، کلید عمومی سرور را پیدا می‌کند و محتوای امضا را با آن رمزگشایی می‌کند و با بررسی داده‌های آن، به صحت منبع داده پی می‌برد.

نکات پیاده سازی:

- در این قسمت شما بایستی از بخش نامتقارن که در پروژه قبلی پیاده سازی نمودید استفاده کنید و موارد بالا را در آن پیاده سازی نمایید(بخش متقارن در این بخش نیازی به آن نیست)

- نیاز است تا تدابیری بیاندیشید تا چند کلاینت بتوانند به سرور احراز هویت و وصل شوند و تبادل دیتا نمایند. بدیهی است که می بایست لیستی از کاربران احراز هویت شده به سرور برای هر کاربر نشان داده شود و بر اساس آن کاربر مقصد دیتای خود را مشخص کند و ارسال کند.
- دیتایی که بین دو کاربر مبادله می شود نباید برای سایر کاربران مشخص باشد. در این مورد تدابیر لازم را اتخاذ نمایید.
- در هنگام ارسال لیست کاربران احرازهویت شده نیز باید محرمانگي و صحت حفظ شود.

نکات دیگر

- پروژه را باید هر نفر به تنهایی پیاده سازی کند و تحویل حضوری دارد که زمان آن متعاقبا اعلام خواهد شد.
- زبان پیاده سازی پروژه آزاد است.
- کدها بررسی و در صورت وجود تطابق تقلب گرفته می شود و برای طرفین نمره **صفر** منظور میگردد.
- **تنها راه تحویل تمرین ها، آپلود آنها در مودل است. به دلیل باگ موجود در سایت درس حتما بعد از آپلود کردن یکبار فایل آپلود شده را دانلود کنید تا به درست آپلود شدن آن یقین پیدا کنید.**
- مهلت ارائه و آپلود پروژه در مودل مشخص شده است (با مقیاس ثانیه). لطفا بر اساس آن زمانبندی کنید. پروژه به هیچ وجه پس از مهلت مشخص شده تحویل گرفته نمی شود.
- پروژه را با فرمت Project2_stdName_stdNum.zip آپلود کنید.
- برای ارتباط با تدریس یاران از طریق ایمیل netsecfall2019@gmail.com در ارتباط باشید

(در قسمت subject ایمیل، **حتماً** ProjectNum(مثلا Project2) را بنویسید و سپس سوال خود را مطرح نمایید)