مستندات پروژه‌ی درس
امنیت شبکه

افراد گروه:
مینا طهماسبی ارشلو
بهروز ربیعی
روح‌الله شمیرانی

۱- نحوه‌ی اتصال مولفه‌ها

همان‌طور که در شمای کلی سیستم رای‌گیری در صورت پروژه نشان داده شده است، این سیستم از چهار مولفه‌ی اصلی تشکیل شده است:

- Client
- CA
- Authority
- Collector

که نحوه‌ی اتصال آن‌ها را در ادامه توضیح خواهیم داد.

Client کاربری است که می‌خواهد رای بدهد. برای این کار ابتدا باید برای خود گواهی تهیه کند. بنابراین کلید عمومی خود را برای CA می‌فرستد. CA نیز گواهی را برای او تولید کرده و می‌فرستد. سپس کاربر گواهی را برای Authority می‌فرستد. برای این پیغام نیازی به رمز کردن یا تایید صحت نیست زیرا خود گواهی امضا در صورتی که صحیح نباشد، verify نخواهد شد. Authority پس از تایید گواهی، یک کلید جلسه با کلید عمومی کاربر رمز کرده و برای او می‌فرستد. این کلید هم‌چنین برای اطمینان از صحت توسط Authority امضا می‌شود.

پس از طی این مراحل کاربر رای خود را با کلید جلسه رمز می‌کند و برای Collector می‌فرستد. Collector برای او یک شاخص تولید می‌کند و رمزشده‌ی رای را با شاخص نگه‌داری می‌کند، هم‌چنین شاخص را برای کاربر می‌فرستد.کاربر شاخص و گواهی خود را دوباره با کلید جلسه رمز می‌کند و به همراه گواهی به صورت ساده، با امضا برای Authority می‌فرستد. Authority نیز پس از بررسی صحت پیام و یکی بودن گواهی رمز شده و گواهی ساده، شاخص کاربر را به همراه اطلاعات کلید جلسه‌ی او در جدولی ذخیره می‌کند. پس از اعلام تمام شدن رای‌گیری به Collector، Collector با اعلام شاخص به Authority کلیدهای جلسه را از او می‌گیرد، رای‌ها را رمزگشایی کرده و برنده را

مشخص می‌کند.

۲- نحوه‌ی تولید کلیدها

برای انتقال کلید جلسه و نیز امضا، از RSA استفاده شده است، تولید کلیدهای عمومی و خصوصی با استفاده از دستور openssl در Unix انجام شده است:

```
$ openssl genrsa -out private_key.pem 2048
Convert private Key to PKCS#8 format (so Java can read it)
$ openssl pkcs8 -topk8 -inform PEM -outform DER -in private_key.pem  -out private_key.der -nocrypt
Output public key portion in DER format (so Java can read it)
$ openssl rsa -in private_key.pem -pubout -outform DER -out public_key.der
```

برای تولید hash از SHA256 استفاده شده است.

برای رمزنگاری متقارن از AES استفاده شده است. کلید جلسه‌ها ۱۲۸ بیتی هستند و با استفاده از کلاس SecureRandom در جاوا تولید می‌شوند.

۳- کلاس‌های مهم

به غیر از کلاس‌های خود پروتکل که در بخش مولفه‌ها توضیح داده شده‌اند، مهم‌ترین کلاسی که وجود دارد کلاس Msg است که برای انتقال پیام‌ها به کار می‌رود. این کلاس یک فیلد Status دارد که وضعیت پیغام را مشخص می‌کند. هم‌چنین یک map وجود دارد که برای انتقال اطلاعات به کار می‌رود. هم‌چنین کلاس‌های RSA، SHA256 و AES وجود دارند که کار رمزنگاری را انجام می‌دهند.