باسمه تعالی

پروژه مبانی رمزنگاری و امنیت شبکه

دکتر میرمحسن

پوریا دادخواه

۹۶۱۰۶۴۸۵

کیف پول دیجیتال

در این پروژه با زبان جاوا کیف پولی طراحی کرده ایم که کاربر در یک محیط CLI میتواند حساب کاربری ایجاد کند و اطلاعاتی که میخواهد را به طور امن ذخیره کند.

در این گزارش بـا بخش های مختلف کد و الگوریتم ها و کلاس های آن توضـــیح مختصـــری می دهیم:

برای این برنامه ما ۳ کلاس تعریف کردیم (هر چند میتوان خیلی برنامه نویســـی module تر و ملموس و تمیز تر بـه همراه محیط GUI زد کـه بـه دلیـل ذیق وقت و امتحان و کاراموزی ..! به صورت ساده تری زده شد)

User : این کلاس کـابرها را پیـاده ســـازی میکند .برای هر کـاربر بـاید اطلاعات زیر را ذخیره کنیم:

*Username به **دو** صـورت عادی و رمزگذاری شـده (با کلیدی که از پسـورد به دسـت می آید و بعدا بیشتر درباره آن توضیح میدهیم)

*Salt که یک عدد تصـــادفی و نانس بوده که هر کاربری جدیدی که ثبت نام میکند ، برای آن تولید میکنیم و برای کاربر ذخیره میکنیم.

*Data که اطلاعاتی اســت که کاربر میخواهد ذخیره شــود. این اطلاعات از کاربر گرفته شده و با همان کلیدی که از پسورد و سالت به دست می آید رمزگذاری و در این فیلد ذخیره می شود.

AES : در این کلاس رمزگذاری و رمزگشایی aes انجام می شود.

این کلاس را می توان از لایبری ها خود جاوا اسـتفاده کرد و رمز aes در مود ecb انجام داد.

طبیعتا ورودی های این کلاس متن موردنظر و کلید هسـتند. ولی کلیدی که میگیریم به فرمت string دریـافت کرده و در یکی از توابعی از همین کلاس کلید مورد نیـاز در aes را می سازیم. (استرینگ دریافتی هم ساخته شده از پسورد کاربرو سالت او می باشد)

CLI : این هم کلاس اصـلی برنامه اسـت که با کاربر در ارتباط اسـت و عملیات هایی که میخواهد را انجام میدهد. در ادامه به جزییات این کلاس و روند اجرای برنامه می پردازیم.

تابع run : در ابتدا اگر کاربر حساب نداشته باشد وارد کیس د.م می شود . در آن جا یک object User جدید می سازیم و اصلاعات یوز و سالت آن را ذخیره میکنیم.

سالت در ابتدا یک آرایه بایتی است (به طول ۱۶ بیت) که آن را به استرینگ تبدیل کرده و ذخیره میکنیم.

حالا استرینگ پسورد و سالت را concat کرده و به عنوان ورودی تابع کلید ساز در کلاس aes می دهیم تا خروجی استرینگkey را تحویل دهد . با این کلید ما هر اطلاعاتی (Data) که کاربرخواست ذخیره کند را ذخیره میکنیم.

در ادامه دیگر مثل یوزر با سابقه شده و وارد تابع Wallet میشود.

اگر از قبل حساب داشتیم یوزر و پسورد را میخواهیم. دقت می کنیم که ما دو نوع یوزر را در پایگاه سیو کرده ایم. به صورت plain text و به صورت رمز گذاری شده با کلید کاربر.

وقتی حالا برای ورود یوزر و پسورد را وارد کرد ، در ابتدا در لیست کاربران به دنبال فردی با یوزر فوق میگردیم سپس با پسوردی که زده است و داشتن سالت در پایگاه ان کاربر ، کلید فعلی را میسازیم و یوزر را رمزگذاری می کنیم . اگر این خروجی با یوزر رمز گذاری شده در پایگاه برابر بود یعنی اطلاعات درست است و وارد تابع wallet میشود.

تابع wallet : پس از لاگین شدن کاربر در این قسمت او میتواند عملیات های دلخواهش را انجم دهد :

دیدن اطلاعات فعلی : کافیست فیلد Data را با کلیدی که دوباره از پسورد زده شده توسط کاربر و سالتی که در پروفایل او ذخیره شده اینبار با تابع decrypt از کلاس aes رمزگشایی میکنیم و نشان میدهیم.

ثبت یا تغییر داده ها : او اطلاعات را وارد کرده و با کلیدش رمز میکنیم و فیلد data را برابر آن قرار میدهیم.

تغییر پسورد : در این قسمت پس از confirm شدن پسورد ،فیلد data و Enc_Username را با رمز جدید ذخیره میکنیم.

این کلیت کار پروژه است . جزئیات بیشتر (مثلا logout یا اتمام برنامه یا ..) در توضیحات شفاهی و کد آمده اند.