اطلاعات برنامه نویس

بیتا خسروی نام
94171018 شماره دانشجویی

سناریو پروژه

یک پروژه ایجاد یک چت امن به صورتی که تمام پیام های ذخیره شده در پایگاه داده رمزگذاری شده باشند و کلید هر چت متفاوت باشد الگوریتم آن به طوری طراحی شده باشد که پیدا کردن کلید به دلیل هش بودن غیر قابل بازیابی باشد

نحوه پیاده سازی

این پروژه یک چت رمز نگاری شده بر اساس سیتم رمز نگاری AES است در این پروژه دو کاربر در نظر گرفته شده است که این کاربران هر کدام ماژول منحصر به خود را دارند هر ماژول رمز نگاری شامل چند بخش است به صورت زیر:

1. یک سیستم رمز نگاریAES
2. یک سیستم رمز گشایی بر پایه همینAES
3. یک سیستمHASH MD5
4. یک سیستم تولید کد

هر کدام از زیر ماژول ها به صورت جداگانه تعریف خواهند شد

AES

- ورودی AES از سمت کاربر می آید
- کلید رمز نگاری آن نام کاربری دو کاربر در کنار هم است که HASH شده است
- initializer vectorبه عنوان مقدار پیش فرض قرار میگیرد

تولید کلید

تولید کلید با الگوریتم نام کاربری دو کاربر که HASH شده است قرار میگیرد

خروجی ماژول ها

خروجی ماژول ها در دیتا بیس به صورت HASH شده قراردارند و در صورتی که دیتابیس هک بشود عملا کلیدی در اختیار کاربران نخواهد بود برای عملیات رمز گشایی