

# اطلاعات برنامه نویس

نام	بیثا خسروی
شماره دانشجویی	94171018
عنوان پروژه	پروژه چت رمزنگاری شده با AES الگوریتم

## 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 سیستم رمز نگاری AES است در این پروژه دو کاربر در نظر گرفته شده است که این کاربران هر کدام مازول منحصر به خود را دارند هر مازول رمز نگاری شامل چند بخش است به صورت زیر:

1. یک سیستم رمز نگاری AES
2. یک سیستم رمز گشایی بر پایه همین AES
3. یک سیستم HASH MD5
4. یک سیستم تولید کد

هر کدام از زیر مازول 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 vector به عنوان مقدار پیش فرض قرار میگیرد

### تولید کلید

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

### خروجی مازول ها

خروجی مازول 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

