به نام خدا

رمزنگاری و امنیت شبکه

پروژه

استاد درس: دکتر محمدرضا سعیدی

دستیاران حل تمرین: نگین نوشادی - مریم حسینی

بهار ۱۴۰۲

نکات کلی:

- پروژه در دو بخش اجباری و اختیاری تعریف شده است که توضیح هرکدام در ادامه داده شده است.
- پروژه میتواند بصورت تکی یا گروهی (حداکثر دو نفره) انجام شود.
- هر گروه یا قسمت اجباری پروژه را انجام میدهد و یا قسمت اختیاری را. در صورتیکه قسمت اختیاری انجام شود نمره قسمت اجباری نیز به گروه تعلق میگیرد.
- پاسخ‌های خود را به صورت یک فایل zip تا حداکثر تا ساعت ۲۳:۵۹ روز ۳۰ خرداد در قسمت مربوطه در کلاس کوئرا ارسال کنید. از هرگروه ارسال یک نفر کافی است.
- در صورت نیاز می‌توانید سوالات خود را در تلگرام بپرسید.
- **همراه با کد خود یک گزارش کتبی از نحوه کارکرد کدتان و یا یک ویدئو (۵ تا ۱۵ دقیقه)که در آن کد خود را توضیح داده اید ارسال کنید.**

قسمت اجباری پروژه :

یک الگوریتم رمزنگاری DES را هم برای encryption و هم برای decryption پیاده سازی کنید. بطوریکه بتوانیم هر plaintext ای را با هر تعداد کاراکتر رمزنگاری کنیم و بتوانیم ciphertext مربوط به آن را رمزگشایی کنیم.

استفاده از کتابخانه ها مجاز است ولی از کتابخانه هایی مثل des که تمام الگوریتم را پیاده سازی میکنند استفاده نکنید. باید هر بخش از الگوریتم des (مثل initial permutation، p-box ها، s-box و...) در کد شما مشخص باشد.

کد شما یک ورودی دریافت میکند، سپس آن را encrypt و ciphertext حاصل را decrypt میکند و رشته ی decrypt شده را به عنوان خروجی چاپ میکند.

قسمت اختیاری پروژه:

فرض کنید آلیس میخواهد چند پیام را با استفاده از روش DES و با استفاده از یک round رمزنگاری کند و آن را برای باب بفرستد.(یعنی در این الگوریتم از ۱۶ راند استفاده نمیشود و فقط از یک راند استفاده میشود.) شما به عنوان EVE توانستید به این جفت plaintext و ciphertext دسترسی پیدا کنید. هدف شما این است که یکی از پیام های رمزنگاری شده توسط آلیس را رمزگشایی کنید (یعنی یک ciphertext وجود دارد که شما به plaintext متناظر با آن دسترسی نداشتید و میخواهید آن را decrypt کنید) همچنین توانستید به کلید نیز دسترسی داشته باشید. با این حال نتوانستید که پیام موردنظر را رمزگشایی کنید. پس از بررسی متوجه میشوید که straight p-box ای که در ماشین رمزنگاری استفاده شده است با استاندارد الگوریتم DES متفاوت است. پس شما باید با استفاده از این جفت plaintext-ciphertext های شنود شده و با استفاده از کلید و پیاده سازی بقیه ی بخش های DES، اینstraight p-box استفاده شده در ماشین آلیس را بیابید و پس از آن، ciphertext داده شده را رمزگشایی کنید.

جفت plaintext-ciphertext های شنود شده و کلید بصورت هگزادسیمال در یک فایل تکست در همین فایل زیپ وجود دارد. همچنین expansion p-box و s-box ها و اطلاعات مربوط به ساخت کلید نیز در همین فایل زیپ قرار داده شده است.

متن رمزشده ای که میخواهید رمزگشایی کنید(متن بصورت هگزادسیمال است):

Ciphertext:

59346E29456A723B62354B61756D44257871650320277C741D1C0D0C4959590D

کلید (بصورت هگزادسیمال است):

Key:

4355262724562343