بسم الله الرحمن الرحیم

دانشکده مهندسی کامپیوتر

استاد : آقای دکتر ابوالفضل دیانت

بالاترین درجه دانایی، تشخیص اخلاق از یکدیگر و آشکارکردن اخلاق پسندیده و سرکوب اخلاق ناپسند است. حضرت علی(علیه السلام)

سید مهدی رضوی - امیرحسین مجتهدی

فروردین ۱۴۰۲

فهرست مطالب

فهرست تصاویر

۱ تمرین اول

انواع حملات صورت‌گرفته بر روی الگوریتم DES را بررسی کنید.

- Differential Cryptanalysis

هدف اصلی تحلیل رمزی تفاضلی ، مشاهده توزیع‌های آماری و الگوهای موجود در متن رمزی برای ارائه عنصر استنباط در مورد کلید مورد استفاده در رمز است.

رمزنگاری تفاضلی بخشی از مطالعه در رمزنگاری است که تفاوت روش در ورودی مرتبط با تفاوت در خروجی رمزگذاری شده را مقایسه می‌کند. این می تواند اساساً در مطالعه رمزهای بلوکی برای تصمیم گیری در مورد اینکه آیا تغییرات در متن ساده منجر به نتایج غیر تصادفی در متن رمزگذاری شده می شود استفاده شود.

در واقع در کلی‌ترین حالت ، مطالعه این موضوع است که چگونه تغییر در ورودی می‌تواند بر روی خروجی سیستم رمزنگاری تاثیربگذارد.

- Related-key Cryptanalysis

هکر تعریف می‌کند که چگونه کلید باید اصلاح شود و حملات با کلیدهای شناخته‌شده ، حملاتی هستند که تفاوت کلیدی آنها تایید شده است ، اما هکر نمی‌تواند آن را انتخاب کند.

می‌توان بر این نکته تاکید کرد که هکر رابطه بین کلیدها را درک کند.

به عبارت بهتر در رمزنگاری ، حمله با کلید مرتبط به هر شکلی از تحلیل رمز گفته‌می‌شود که در آن مهاجم می‌تواند عملکرد یک رمز را تحت چندین کلید مختلف مشاهده‌کند که مقادیر آن‌ها در ابتدا ناشناخته است.

اما در آن رابطه‌ای ریاضی که کلیدها را به هم متصل‌می‌کند برای مهاجم(هکر) شناخته‌شده‌است.

- Linear Cryptanalysis

رمزنگاری خطی یک شکل کلی از رمزنگاری است که به تحلیل رمز خطی یک حمله متن ساده شناخته شده است (بدان معنا که متن اولیه برای هکر معلوم است) که در آن مهاجم روابط خطی احتمالی را که به عنوان تقریب های خطی در بین بیت های برابری متن ساده، متن رمز و کلید پنهان شناخته می شود، مطالعه می کند.

- Brute-Force Cryptanalysis

احتمالا بدون دانش‌ترین حمله این نوع حمله خواهد بود که فرد هکر دانش کمی نسبت به سیستم‌رمزنگاری ما خواهد داشت.

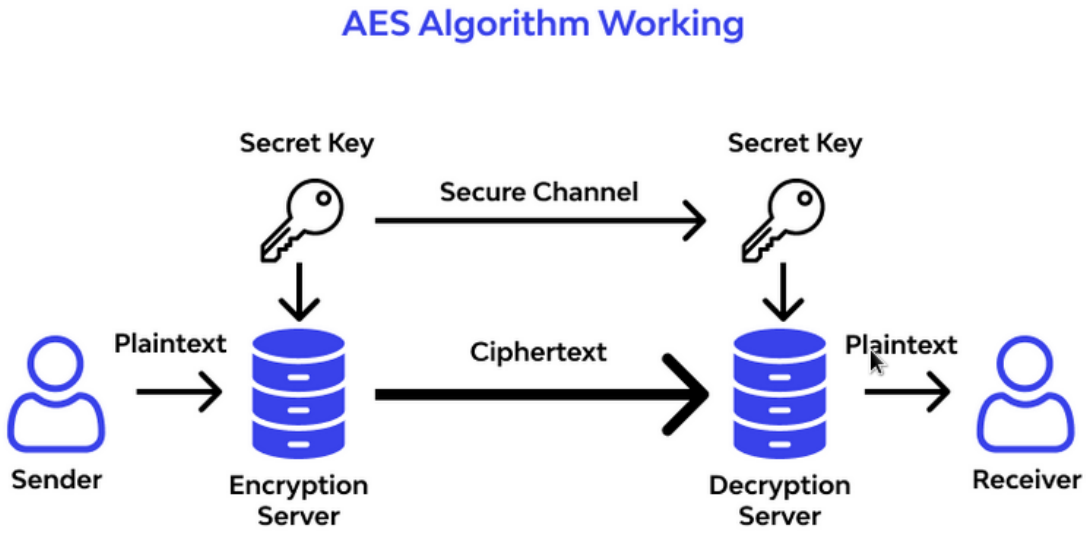
در تحلیل رمز ، حمله brute force روشی برای شکست‌دادن یک طرح رمزنگاری با آزمایش تعداد زیادی از احتمالات است.

به عنوان مثال ، به طور جامع از طریق تمام کلیدهای ممکن به منظور رمزگشایی یک پیام کار کنید.

۲ تمرین دوم

با شکسته‌شدن الگوریتم DES ، در سال ۲۰۰۱ الگوریتم AES به عنوان استاندارد رمزنگاری انتخاب شد. در مورد نحوه این انتخاب ، ساختار و چگونگی کارکرد این الگوریتم تحقیق کنید.

در استاندارد رمزنگاری پیشرفته کامل ، AES - Advanced Encryption Standard یک استاندارد رمزنگاری داده تایید شده توسط موسسه ملی استانداردها و فناوری ایالات متحده به عنوان جایگزینی برای الگوریتم DES خواهد بود.
در ژانویه ۱۹۹۷ NIST یک درخواست عمومی برای ایجاد یک الگوریتم برای جایگزینی الگوریتم DES ایجاد کرد.
۱۵ کاندیدا از ۱۲ کشور برای این درخواست الگوریتم‌های خود را ارائه کردند.
در اکتابر ۲۰۰۰ دو رمزنگار بلژیکی ، ریژمان و دیمن الگوریتمشان به عنوان یک استاندارد جدید مورد پذیرش قرار گرفت.
اداره ملی استانداردها ، NIST انتظار داشت که DES در سخت‌افزار با هدف خاص پیاده‌سازی شود و از این‌رو به اجرای کارآمد آن در نرم‌افزار توجه چندانی نکرده بود.
به عنوان مثال استفاده از ریزپردازنده‌های همه‌منظوره .
در نتیجه DES نتوانست از پیشرفت سریع ریزپردازنده‌ها که در دو دهه آخر قرن بیستم رخ داد ، استفاده کند.
از سوی دیگر ، مشخصات AES بر پیاده‌سازی سخت‌افزاری و نرم‌افزاری به طور مساوی تاکید داشت.
این امر تا حدی نیازهای کارت‌های هوشمند و سایر تجهیزات نقطه‌فروشی را که معمولاً قابلیت‌های محاسباتی بسیار محدودی دارند، شناسایی کرد.
اما مهمتر شناخت نیازهای روبه‌رشد اینترنت و تجارت الکترونیک بود.
بر اساس تجربه آن‌ها با DES ، که در آن پیشرفت‌ها در محاسبات به سادگی بر ضریب کارکلید کد ۵۶ ثابت فائق آمد.
همچنین سازمان ملی استانداردهای آمریکا یا همان
خواستار این شد که الگوریتم بتواند در صورت لزوم طول کلید را افزایش دهد.
Rijndael ثابت کرد که کلیدها هم به اندازه کافی کوچک است که بتوان بر روی کارت‌های هوشمند پیاده‌سازی کرد و هم به اندازه کافی انعطاف پذیر است که طول کلیدهای طولانی تری را ایجاد کند.



شکل ۱: رویه کلی الگوریتم

استاندارد رمزنگاری پیشرفته یا همان AES ، یک الگوریتم رمزنگاری بلوکی ۱۲۸ بیتی متقارن است که داده ورودی را پس از انجام عملیات رمزنگاری یا Encryption تبدیل به یک کلید رمز می‌کند.
کلمه متقارن در اینجا به این معنی است که یک Secret Key مشترک برای رمزنگاری و رمزگشایی داده استفاده‌می‌شود و باید در هر دو سمت یک رمز مشترک وارد شود.
به عبارت ساده‌تر ، AES یک بلوک رمزنگاری ۱۲۸ بیتی است که داده‌هایی با طول ۱۲۸ بیتی وارد آن می‌شوند و روی آن عملیات رمزنگاری را انجام می‌دهد که در اولین مرحله از رمزنگاری داده‌ها داخل یک آرایه قرار گیرند، سپس عملیات منطقی XOR است که روی هر ستون و کلید مربوطه اعمال می‌شود.
سپس بسته به طول رمزنهایی و ساختار آن مراحل بعدی به تعداد مشخصی تکرار می‌شوند که خروجی نهایی آن یک کلید برای دسترسی به اطلاعات رمزنگاری شده‌است.

۳ تمرین سوم

یک پیام را با الگوریتم AES در زبان Python یا C++ رمزگذاری یا رمزگشایی کنید.

برای این منظور پیام Shahid Ghasem Soleimani را در نظر گرفته‌ایم.
با استفاده از کتابخانه pycryptodome عملیات رمزگذاری را انجام داده‌ایم.
یک کلید ۱۶ بیتی را ایجاد خواهیم کرد. سپس رشته بیتی رمزشده را (Cipher Text) در فایل encrypted.bin ذخیره‌سازی خواهیم کرد.
در سلول بعدی عملیات رمزگشایی را انجام خواهیم داد.

```
[ ] !pip3 install pycryptodome

    Looking in indexes: https://pypi.org/simple, https://us-python.pkg.dev/colab-wheels/public/simple/
    Collecting pycryptodome
      Downloading pycryptodome-3.17-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (2.1 MB)
         ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.1/2.1 MB 26.1 MB/s eta 0:00:00
    Installing collected packages: pycryptodome
    Successfully installed pycryptodome-3.17

[ ] from Crypto.Cipher import AES
    from Crypto.Random import get_random_bytes

    data = b'Shahid Ghasem Soleimani'

    key = get_random_bytes(16)
    cipher = AES.new(key, AES.MODE_EAX)
    ciphertext, tag = cipher.encrypt_and_digest(data)

    file_out = open("encrypted.bin", "wb")
    [ file_out.write(x) for x in (cipher.nonce, tag, ciphertext) ]
    file_out.close()

    from Crypto.Cipher import AES

    file_in = open("encrypted.bin", "rb")
    nonce, tag, ciphertext = [ file_in.read(x) for x in (16, 16, -1) ]
    file_in.close()

    # let's assume that the key is somehow available again
    cipher = AES.new(key, AES.MODE_EAX, nonce)
    data = cipher.decrypt_and_verify(ciphertext, tag)

    print(data)

    b'Shahid Ghasem Soleimani'
```

شکل ۲: تصویری از اجرای این الگوریتم