رامتین احسانی - ۹۷۵۲۱۰۱۸

تمرین سوم - امنیت سیستم های کامپیوتری

۱- در طی سال های مختلف حملات مختلفی به DES صورت گرفته است که به مختصر برخی از این حملات را در این قسمت توضیح داده ام. معروف ترین حملات با brute-force، Differential cryptanalysis، Linear cryptanalysis و Davies Attack صورت گرفته است.

۱۹۷۶: برای برخی از کلید های ضعیف، با پیچیدگی زمانی ۱ برخی از الگوریتم ها شکسته شدند.

۱۹۷۷: Exhaustive search با پیچیدگی زمانی 2^56

۱۹۸۰: با تبادل time/memory توانستند در زمان کوتاه تری الگوریتم ها را بشکنند.

۱۹۸۲: شکستن کلید های نسبتا ضعیف با پیچیدگی زمانی ۱

۱۹۸۵: شکستن الگوریتم های 6-round DES با meet-in-the-middle attack در پیچیدگی زمانی 2^52

۱۹۸۷: حمله Davies attack با پیچیدگی زمانی 2^56.5 (طولانی تر از brute)

۱۹۹۰: Differential cryptanalysis با دانستن 2^47 تا plaintext

۱۹۹۳: Linear cryptanalysis با دانستن 2^43 تا plaintext

۱۹۹۴: شکستن 8-round DES با 768 تا plaintext با Differential-linear cryptanalysis به همراه brute-force با پیچیدگی زمانی 2^46

۱۹۹۴: تقویت Davies attack با دانستن 2^52 تا plaintext (موفقیت ۵۱٪)

۲- AES یا همان Advanced Encryption Standard مانند DES هر دو symmetric block cipher هستند. DES بخاطر داشتن key size کوچکتر مشکل امنیتی داشت. بخاطر همین 3-DES معرفی شد ولی متوجه شدند که خیلی سرعت پایینی دارد. برای همین AES معرفی شد.

مسابقات گوناگونی در سال های مختلف برای شکستن DES برگزار شد.

در سال ۱۹۹۷ در DES I contest با یک حمله brute-force با صرف ۸۴ روز الگوریتم شکسته شد.

در سال ۱۹۹۸ هم دو مسابقه برگزار شد. در اولین مسابقه حدود ۱ ماه صرف شکستن الگوریتم شد و جمله Decipher شده "The unknown message is: Many hands make light work. " بود. دومین مسابقه هم کمتر از ۳ روز طول کشید و متن مسابقه "It’s time for those 128-, 192-, and 256-bit keys" بود.

آخرین مسابقه هم در سال ۱۹۹۹ بود که فقط ۲۲ ساعت و ۱۵ دقیقه طول کشید و به همه ثابت کرد که وقت جایگزین کردن DES فرا رسیده است. در سال ۲۰۰۱ در استاندارد FIPS 197 الگوریتم AES معرفی شد.

در الگوریتم AES حق انتخاب بین کلید های ۱۲۸ - ۱۹۲ و ۲۵۶ وجود دارد و مشخص است که از کلید های ۵۶ بیتی DES قدرت بیشتری دارد.

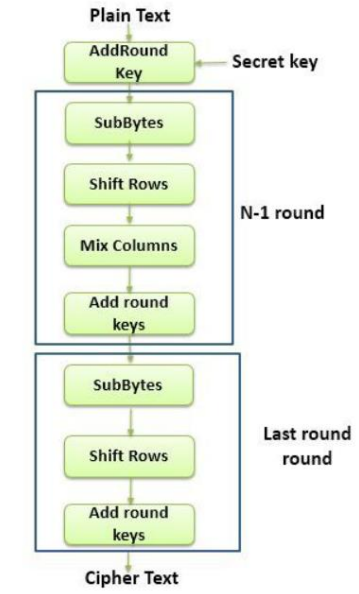
DES از شبکه فایستل برای تقسیم کلید خود به ۲ قسمت استفاده میکرد ولی در AES با استفاده از permutation-substitution با کل دیتا بلاک به عنوان یک تک ماتریکس برخورد می شود.

DES شامل ۱۶ راند بود. AES:

- برای کلید های ۱۲۸ بیتی شامل ۱۰ راند
- برای کلید های ۱۹۲ بیتی شامل ۱۲ راند
- برای کلید های ۲۵۶ بیتی شامل ۱۴ راند

این الگوریتم شامل مراحل زیر است:

- Subbytes: استفاده از S-box برای جایگزینی بایت های کل بلاک
- Shift Rows: جا به جایی ردیف های matrix
- Mix Columns: جا به جایی ستون ها
- Add round keys: در این مرحله XOR بلاک و کلید انجام میشود.



Advanced Encryption Standard

۳- برای پیاده سازی این تمرین از زبان Python استفاده کردم. برای اجرای کد باید پکیج های زیر را نصب کنید:

- Pycryptodomex
    - pip install pycryptodomex
- Scrypt
    - pip install scrypt