باسمه تعالی

درس: آزمایشگاه امنیت شبکه

نام و نام خانوادگی: محمد هادی امینی

شماره دانشجویی: 9912762370

شماره تمرین : 01

Aes یک الگوریتم رمزنگاری متقارن است که از یک کلید برای رمزنگاری و رمزگشایی استفاده میکند. الگوریتم baby aes یک نسخه کوچک شده از AES است که از کلید و ورودی 16بیتی استفاده میکند. این الگوریتم دارای 4 دور می باشد و شامل مراحل زیر است:

آ – SubBytes: هر بایت از آرایه state با یک بایت مربوطه از یک S-box ثابت (substitution box) جایگزین می شود که باعث پیچیدگی در فرآیند رمزگذاری می شود.

ب – ShiftRows: ردیف های آرایه state به صورت چرخه ای به سمت چپ جابه جا می شوند. در این مرحله ردیف اول جابه جا نمی شودو ردیف دوم یک بایت به چپ جابجا میشود .این مرحله انتشار در فرآیند رمزگذاری را فراهم می کند.

ج – MixColumns: هر ستون از ماتریس state در یک ماتریس ثابت در یک میدان محدود ضرب می شود. این عملیات انتشار در سراسر بلاک را فراهم می کند.

د – AddRoundKey : round keyبا آرایه XOR state میشود. این مرحله رمزگذاری را با کلید دور منحصر به فرد برای دور فعلی ترکیب می کند.

دور نهایی: دور نهایی کمی با دورهای قبلی متفاوت است. این مرحله MixColumns را برای آسان‌تر کردن رمزگشایی حذف می‌کند.

ارزیابی الگوریتم

پدیده بهمنی (Avalanche) :

یک معیار تاثیرگذار در الگوریتم‌های رمزنگاری است که هنگام تغییر ورودی، تغییرات بسیار زیادی را در نتایج الگوریتم به وجود می‌آورد. وقتی یک بیت ورودی تغییر می‌کند، الگوریتم‌های با این ویژگی به

گونه‌ای هستند که تاثیرات این تغییر در خروجی‌هایشان بسیار بزرگ و قابل مشاهده است. به این ترتیب، حتی یک تغییر کوچک در ورودی می‌تواند به تغییرات چشمگیری(حدودا نصف) در خروجی منجر شود.

```
Avalanch
Bit 0: 10
Bit 1: 6
Bit 2: 10
Bit 3: 10
Bit 4: 7
Bit 5: 7
Bit 6: 10
Bit 7: 7
Bit 8: 8
Bit 9: 3
Bit 10: 8
Bit 11: 8
Bit 12: 7
Bit 13: 6
Bit 14: 9
Bit 15: 8
average: 7.75 per bit
48.44 %
```

تصویر 1 – نتیجه بررسی avalanche به ازای تغییر هر بیت

بهمنی اکید(Strict Avalanche) :

این مفهوم مشابه معیار بهمنی است. با این تفاوت که ارزیابی دقیقتری صورت میگیرد و انتظار می رود دقیقا نصف بیت های خروجی تغییر پیدا کنند.

```
Strict Avalanch
Bit 0 : 10 - Fail
Bit 1 : 6 - Fail
Bit 2 : 10 - Fail
Bit 3 : 10 - Fail
Bit 4 : 7 - Fail
Bit 5 : 7 - Fail
Bit 6 : 10 - Fail
Bit 7 : 7 - Fail
Bit 8 : 8 -  Pass
Bit 9 : 3 - Fail
Bit 10 : 8 -  Pass
Bit 11 : 8 -  Pass
Bit 12 : 7 - Fail
Bit 13 : 6 - Fail
Bit 14 : 9 - Fail
Bit 15 : 8 -  Pass
```

تصویر 2 – نتیجه بررسی معیار strict avalanche به ازای تغییر هر بیت

تمامیت (Completeness) :

تمامیت به پخش تغییرات در تمام بیت‌های خروجی یک الگوریتم رمزنگاری در پاسخ به تغییر هر بیت ورودی اشاره دارد. این بدان معناست که حتی تغییرات کوچک در ورودی می‌تواند تأثیرات قابل ملاحظه‌ای به طور یکسان در تمام بیت‌های خروجی الگوریتم ایجاد کند. به این ترتیب، اطمینان حاصل می‌شود که هر بیت از خروجی الگوریتم به طور کامل به ورودی و کلید وابسته است.

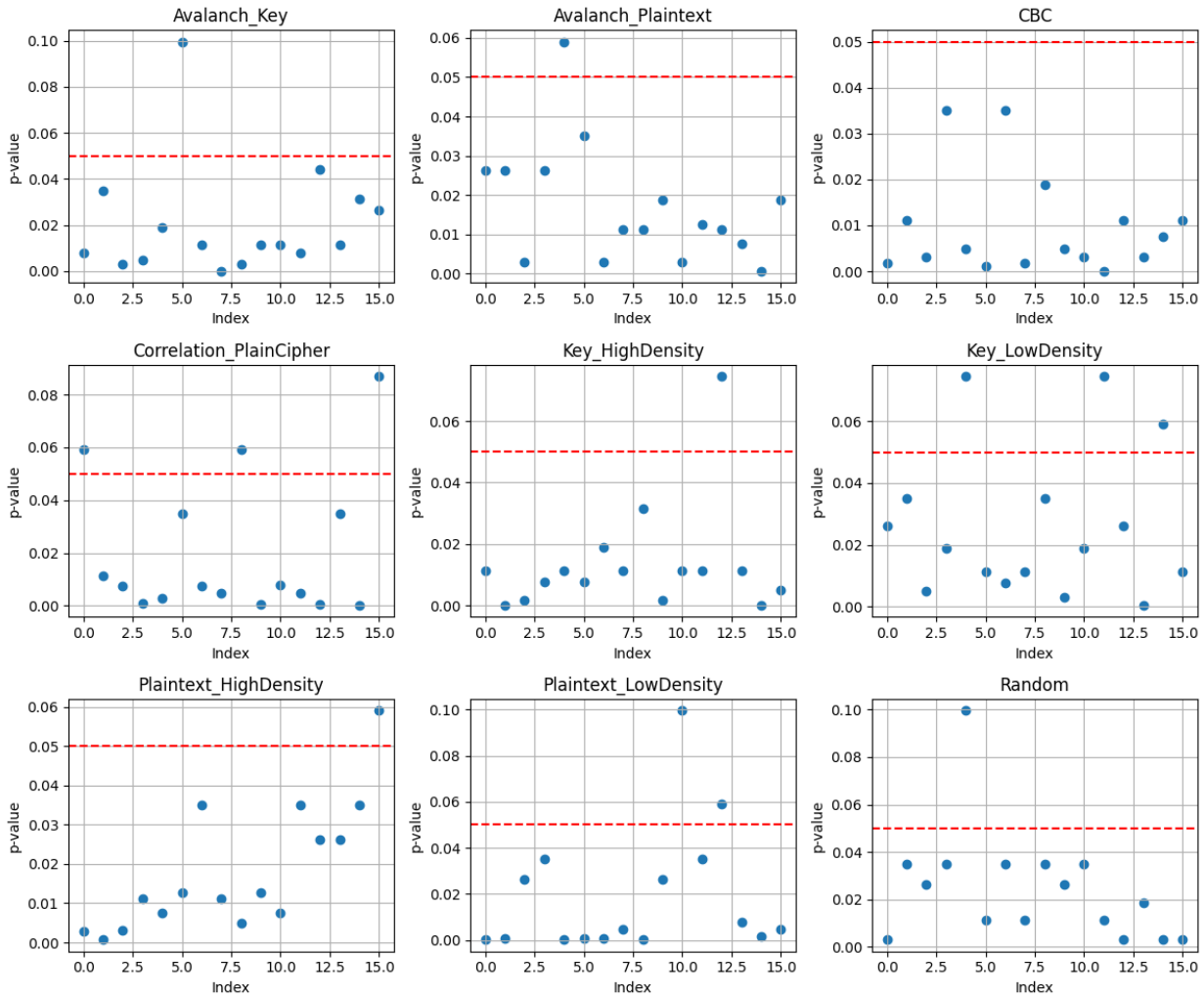
```
completeness
Bit 0 fail
Bit 1 fail
Bit 2 fail
Bit 3 fail
Bit 4 fail
Bit 5 fail
Bit 6 fail
Bit 7 fail
Bit 8 fail
Bit 9 fail
Bit 10 fail
Bit 11 fail
Bit 12 fail
Bit 13 fail
Bit 14 fail
Bit 15 fail
completeness:0.0%
```

تصویر3 – نتیجه بررسی معیار تمامیت

آزمون آماری Uniform Distribution :

آزمون توزیع یکنواخت یک آزمون آماری است که برای ارزیابی اینکه آیا مجموعه ای از داده ها از توزیع یکنواخت پیروی می کنند یا خیر استفاده می شود. در یک توزیع یکنواخت، همه مقادیر در یک محدوده معین احتمال وقوع یکسانی دارند. این بدان معنی است که داده ها به طور مساوی در سراسر محدوده پخش می شوند، بدون هیچ غلظت خاصی در فواصل زمانی خاص.

روش‌های مختلفی برای آزمایش یکنواختی در یک مجموعه داده وجود دارد، از جمله روش‌های گرافیکی (مانند هیستوگرام یا نمودارهای احتمال) و آزمایش‌های آماری. یکی از آزمون‌های آماری رایج برای یکنواختی، آزمون کولموگروف–اسمیرنوف (آزمون KS) است که تابع توزیع تجمعی تجربی (ECDF) داده‌ها را با تابع توزیع تجمعی (CDF) توزیع یکنواخت مقایسه می‌کند. اگر این دو تابع به طور قابل توجهی متفاوت باشند، نشان می دهد که داده ها ممکن است به طور یکنواخت توزیع نشده باشند.



تصویر4 – خروجی آزمون آماری برای دیتاست های مختلف