


# ارزیابی رمزهای قطعه‌ای

## مقدمه

Baby AES یک نسخه کوچک شده از AES است. اندازه بلوک و کلید Baby AES ۱۶ بیت است، که ۴ رقم هگزا دسیمال در نظر گرفته می‌شود. الگوریتم رمزگذاری مورد نظر از چندین دور تشکیل شده، که همه آنها از نظر ساختار یکسان هستند. تعداد دورهای پیش‌فرض Baby AES ۴ است. داده ورودی به‌عنوان یک ماتریس ۲*۲ از اعداد هگزا دسیمال در نظر گرفته می‌شود. در یک الگوریتم رمزنگاری، یک الگوریتم برنامه کلید (KSA) باید دارای خواص سردرگمی و انتشار قوی باشد، و همه کلیدهای فرعی تولید شده باید مستقل از یکدیگر باشند، به‌طوری که اگر هر کلید فرعی به خطر افتاد، هیچ اطلاعاتی در مورد سایر کلیدهای فرعی یا کلیدهای مخفی بروز نکند. برای ارزیابی الگوریتم برنامه کلید، از معیارهایی نظیر تمامیت، پدیده بهمنی و پدیده بهمنی اکید استفاده می‌شود. در حال حاضر، آزمون تصادفی بودن الگوریتم عمدتاً با بررسی تصادفی بودن دنباله خروجی محقق می‌شود. آزمون تصادفی بودن دنباله خروجی از طریق خروجی نمونه انجام می‌شود، که از نظر آماری بررسی می‌شود تا مشخص شود آیا ویژگی‌های دنباله اعداد تصادفی واقعی را دارد یا خیر. در جدول ۱، آزمون‌های آماری تصادفی بودن نمایش داده شده است. همچنین در جدول ۲، مجموعه داده‌های تصادفی از طریق رویکردهای مختلف تولید شده است.

## هدف

هدف از انجام این آزمایش آشنایی با مفاهیم پایه رمزگذاری و به‌طور خاص نحوه پیاده‌سازی مفاهیمی نظیر، تمامیت، پدیده بهمنی، پدیده بهمنی اکید و رمزگذاری قطعه‌ای است. همچنین ضمن فراگیری و پیاده‌سازی این مفاهیم، با نحوه ارزیابی کیفیت تصادفی بودن خروجی داده رمزگذاری شده آشنا شده، و براساس مجموعه داده ذکر شده به بررسی هر یک از داده‌ها از طریق آزمون‌های آماری می‌پردازیم.

جدول ۱) آزمون‌های آماری تصادفی بودن

| | Randomness Test Methods | NIST | SAC | BSI |
|---|---|---|---|---|
| 1 | The Frequency (Monobit) Test | ✓ | ✓ | ✓ |
| 2 | Frequency Test within a Block | ✓ | ✓ | × |
| 3 | The Runs Test | ✓ | ✓ | ✓ |
| 4 | Tests for the Longest-Run-of-Ones in a Block | ✓ | ✓ | × |
| 5 | The Binary Matrix Rank Test | ✓ | ✓ | × |
| 6 | The Discrete Fourier Transform (Spectral) Test | ✓ | ✓ | × |
| 7 | The Non-overlapping Template Matching Test | ✓ | × | × |
| 8 | The Overlapping Template Matching Test | ✓ | × | × |
| 9 | Maurer's "Universal Statistical" Test | ✓ | ✓ | × |
| 10 | The Linear Complexity Test | ✓ | ✓ | × |
| 11 | The Serial Test | ✓ | ✓ | × |
| 12 | The Approximate Entropy Test | ✓ | ✓ | × |
| 13 | The Cumulative Sums (Cusums) Test | ✓ | ✓ | × |
| 14 | The Random Excursions Test | ✓ | × | × |
| 15 | The Random Excursions Variant Test | ✓ | × | × |
| 16 | The Poker Test | × | ✓ | ✓ |
| 17 | The Runs Distribution Test | × | ✓ | × |

| | | | | |
|---|---|---|---|---|
| 18 | The Binary Derivation Test | × | ✓ | × |
| 19 | The Autocorrelation Test | × | ✓ | ✓ |
| 20 | The Disjointness Test | × | × | ✓ |
| 21 | The Long Run Test | × | × | ✓ |
| 22 | The Uniform Distribution Test | × | × | ✓ |
| 23 | The Comparative Test for Multinomial Distributions | × | × | ✓ |
| 24 | The Entropy Estimation Test | × | × | ✓ |

جدول ۲) مجموعه داده مورد استفاده

| | **Dataset** |
|---|---|
| 1 | Avalanche Plaintext |
| 2 | Avalanche Key |
| 3 | Plaintext-Ciphertext correlation |
| 4 | Cipher Block Chaining Mode |
| 5 | Random |
| 6 | Low-Density with Plaintext |
| 7 | Low-Density with Key |
| 8 | High-Density with Plaintext |
| 9 | High-Density with Key |




## فعالیت‌های کلاسی

### ۱. مسئله

- با استفاده از زبان برنامه نویسی دلخواه رمز قطعه‌ای Baby AES را پیاده‌سازی کنید.

### ۲. نیازمندی‌ها

- استفاده از زبان‌های برنامه‌نویسی مختلف و کتابخانه‌های مورد نیاز

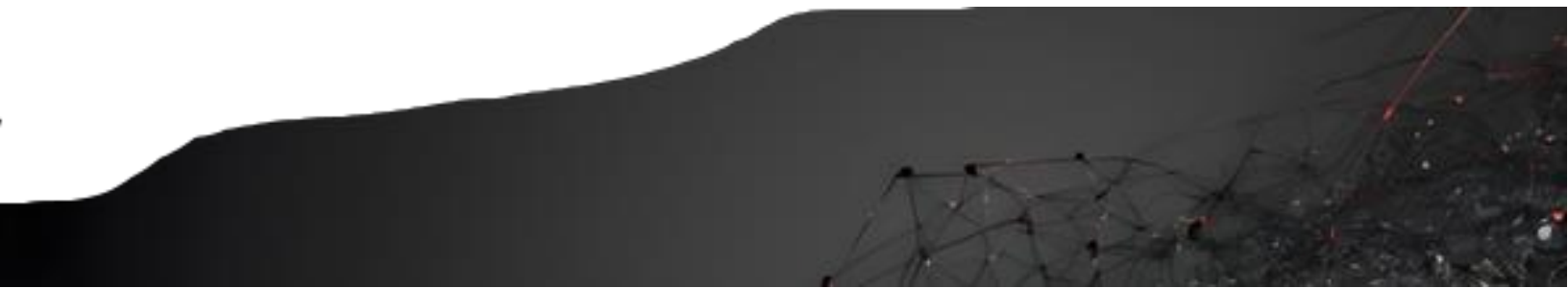
## تکالیف

### ۱. مسئله

- مراحل رمزگذاری Baby AES را به‌صورت مختصر توضیح دهید؟
- تمامیت، پدیده بهمنی و پدیده بهمنی اکید را به طور مختصر شرح دهید؟
- خروجی رمز قطعه‌ای Baby AES را از طریق معیارهای تمامیت، پدیده بهمنی و پدیده بهمنی اکید ارزیابی کنید.
- فهم دقیق، تشریح، پیاده‌سازی و اجرای یکی از آزمون‌های آماری تصادفی بودن جدول ۱ (هر دانشجو بر اساس دو رقم آخر شماره دانشجویی خود یک آزمون را انتخاب کنند) بر روی مجموعه داده‌های جدول ۲.

### ۲. نکات قابل توجه و معیارهای ارزیابی

- مهلت تحویل تکلیف، ساعت ۲۳:۵۵ روز سه‌شنبه مورخ ۱۴۰۲/۱۲/۲۲می‌باشد.




دانشگاه فردوسی مشهد

آزمایشگاه امنیت شبکه

تاریخ تحویل: ۱۴۰۲/۱۲/۲۲

- یکی از آزمون‌های
- دانشجویان گرامی تا تاریخ مشخص شده فرصت دارند تا فایل‌های زیر را در سامانه مجازی درس در آزمایش ۱ آپلود نمایند. در غیر اینصورت، تاخیر در ارسال پاسخ مشمول کسر نمره خواهد شد.
- هر دو فایل کدهای اجرایی و پیاده‌سازی شده و ضبط صفحه همراه با توضیح تکلیف بایستی در قالب فشرده تحت عنوان StudentName_StudentID (به جای StudentName نام خانوادگی و به جای StudentID شماره دانشجویی خود را وارد نمایید.)
- این تکلیف به‌صورت فردی تعریف شده و قابل انجام است.

**چه عواملی باعث می شود از این فعالیت نمره کسب نکنید:**

- عدم تحویل فایل ها در سامانه vu
- فقط انجام بخش تئوری بدون انجام بخش عملی
- عدم ضبط ویدیو بر روی بخش عملی
- مشاهده شباهت بیش از حد معقول
- عدم تسلط به موضوع در جلسه ارائه سر کلاس

**چه عواملی باعث می شود نصف نمره را کسب کنید:**

- تحویل فایل در سامانه vu، اما عدم ارائه در کلاس درس یا غیبت در روزی که ارائه باشد و نام فرد یا تیم برای ارائه تعیین شده باشد.
- عدم تحویل در زمان مقرر و تحویل با تاخیر.