**تحلیل داده‌ها با توجه به صورت مسئله**

**1. مقایسه اندازه کلیدها برای امنیت معادل**

برای مقایسه عادلانه بین الگوریتم‌های AES و RSA، از اندازه کلیدهایی استفاده شده که سطح امنیت یکسانی ارائه می‌دهند:

* **AES** با کلید ۱۲۸ بیتی، امنیتی معادل **RSA** با کلید ۳۰۷۲ بیتی دارد.
* داده‌های تولید شده با این تنظیمات رمزگذاری شده‌اند.

**2. مرور داده‌ها**

داده‌های ارائه شده فایل CSV شامل زمان پاسخ برای ۱۰۰۰ پیام تصادفی هستند:

* **AES\_Time**: زمان‌های پاسخ برای رمزگذاری با AES.
* **RSA\_Time**: زمان‌های پاسخ برای رمزگذاری با RSA.

**3. تحلیل آماری**

اندازه‌گیری‌های کلیدی برای مقایسه عملکرد AES و RSA محاسبه شدند:

|  |  |  |
| --- | --- | --- |
| معیار | AES\_Time (ثانیه) | RSA\_Time (ثانیه) |
| میانگین | ~0.002 | ~0.070 |
| **میانه** | ~0.00185 | ~0.065 |
| **انحراف معیار** | ~0.0003 | ~0.025 |

**تفسیر**:

* میانگین و میانه نشان می‌دهند که **AES** به طور قابل توجهی سریع‌تر از **RSA** است.
* انحراف معیار برای RSA بیشتر است که نشان‌دهنده تنوع بالاتر در زمان پاسخ‌هاست. این موضوع با ماهیت محاسبات سنگین RSA (به ویژه با کلیدهای بزرگ) سازگار است.

**4. نمودار Box Plot**

نمودار **Box Plot** توزیع زمان پاسخ‌ها را برای AES و RSA نشان می‌دهد. مشاهدات کلیدی:

* زمان‌های پاسخ AES به صورت فشرده در اطراف میانگین قرار دارند و تنوع کمی نشان می‌دهند.
* زمان‌های پاسخ RSA پراکندگی بیشتری دارند و گاهی اوقات دارای پاسخ‌های کندتر (outlier) هستند.

**5. نکات کلیدی**

1. **عملکرد**:
   * **AES** بسیار سریع‌تر از **RSA** عمل می‌کند. این موضوع قابل پیش‌بینی است، زیرا:
     + AES یک الگوریتم تقارن‌محور است و برای سرعت بهینه شده است.
     + RSA یک الگوریتم نامتقارن است و به دلیل عملیات‌های ریاضی پیچیده زمان بیشتری نیاز دارد.
2. **ثبات عملکرد**:
   * AES عملکردی بسیار پایدار در تمام پیام‌ها دارد.
   * RSA دارای نوسانات بیشتری در زمان پاسخ است که به دلیل سربار محاسبات کلید رخ می‌دهد.
3. **کاربردها**:
   * **AES** برای سناریوهایی که نیاز به رمزگذاری سریع یا آنی دارند (مانند رمزگذاری داده‌های ذخیره‌شده یا ارتباطات در IoT ) مناسب است.
   * **RSA** برای سناریوهایی که به تبادل کلید امن یا احراز هویت نیاز دارند (نه رمزگذاری مداوم داده‌ها) ایده‌آل است.

**6. نتیجه‌گیری**

* **AES** به دلیل سرعت و ثبات بالا، انتخاب مناسبی برای کاربردهای حساس به عملکرد است.
* **RSA** با وجود زمان پاسخ کندتر، در کاربردهایی که امنیت کلید یا تبادل کلید اهمیت دارد، ترجیح داده می‌شود.