آزمایشگاه امنیت شبکه

الگوریتم رمز کلیدنامتقارن RSA

مقدمه: در این آزمایش قصد به بررسی مختصر الگوریتم رمز کلیدنامتقارن RSA می‌پردازیم.

آزمایش ۱-۲: طول کلید

- یک کلید عمومی ۲۵۶ بیتی RSA تولید کنید.
- یک پیام را با آن رمز کنید.
- پیمانه n را تجزیه کنید.
- با استفاده از مرحله قبل کلید خصوصی متناظر با کلید عمومی مورد نظر را ایجاد کنید.
- پیام رمز شده را با این کلید رمزگشایی کنید.
- در مورد عمل مشابه با کلید ۵۱۲ بیتی چه نظری دارید؟

آزمایش ۲-۲: کلید نشست

- برنامه کلاینت-سرور که در آزمایش قبل ایجاد کردید را بصورت زیر تغییر دهید:
  - برای سرور یک کلید عمومی RSA ایجاد کنید.
  - اگر کلاینت درخواست ارتباط به سرور داد، پس از قبولی درخواست سریعا کلید عمومی را برای آن ارسال کنید.
  - پس از دریافت کلید عمومی سرور، کلید AES تولید شده را توسط آن رمز کرده و برای سرور ارسال کنید.
  - پس از این کلیه پیام‌ها را از طریق کلید AES مشترک بین کلاینت و سرور ارسال کنید.

- توجه کنید که کلیدها نباید hardcode شوند و باید پس از دریافت، از آن‌ها استفاده شود.

- **آزمایش ۳-۲: جستجوی ساده روی داده‌های رمزنگاری شده**
- یک فایل json در نظر بگیرید که در آن برای هر رکورد یک نام و یک شماره دانشجویی تعریف شده باشد (تعداد رکوردها مهم نیست).
- با استفاده از openssl کلید ۲۰۴۸ بیتی RSA را تولید کنید.
- با نوشتن یک برنامه، فقط مقدار خصیصه‌ها را در فایل json با استفاده از کلید تولید شده رمزنگاری کنید و در یک فایل json دیگر ذخیره کنید.
- یک نام را بصورت فاش روی json رمزنگاری شده جستجو کنید. اگر نام مورد نظر در فایل وجود داشت شماره دانشجویی آن را نمایش دهید و در غیر این صورت پیامی مناسب به کاربر نمایش دهید.
- برای نیل به هدف بالا باید چه سیاستی در رمزگاری بکار گرفتید؟
- آیا این سیاست می‌تواند باعث به خطر افتادن اطلاعات درون فایل رمزشده شود؟