هوالحق

پروژه
مبانی امنیت شبکه، پاییز ۹۶

شما (Bob) مجموعه موارد زیر را از Alice دریافت کرده اید:

- کلید عمومی Alice با نام alice_pub.pem که یک کلید ۲۰۴۸ بیتی می باشد.
- یک کلید متقارن k1.bin (به صورت Plain) که یک کلید ۲۵۶ بایتی بوده و به فرمت base64 می باشد.
- یک فایل رمز نگاری شده با کلید متقارن گفته شده به نام message.txt.enc که با الگوریتم AES 192 CBC رمز شده است.

شما باید پس از رمزگشایی فایل message، محتوای آن را تکمیل کرده و موارد زیر را تولید و به Alice ارسال کنید:

- یک فایل کلید متقارن با نام k2.bin.enc که با کلید عمومی Alice به صورت نامتقارن با الگوریتم RSA رمز شده است. این کلید متقارن باید ۱۲۸ بایتی بوده و با فرمت base64 باشد.
- رمز شده‌ی فایل تکمیل شده‌ی message.txt با نام new_message.txt.enc که با کلید k2.bin تولید شده در بند قبلی و با الگوریتم DES ECB به صورت متقارن رمز شده است.
- امضاء دیجیتال فایل new_message.txt تکمیل شده که توسط کلید خصوصی تولید شده توسط شما و همچنین استفاده از الگوریتم درهم‌ریزی sha512 تولید شده است به نام new_message.txt.sign.sha512 .
- کلید عمومی شما با نام pub.pem . توجه کنید که کلید عمومی و خصوصی شما باید ۴۰۹۶ بیتی باشد.
- یک فایل با نام instructions.txt که تمامی دستورات برای عملیات انجام شده درون آن موجود باشد. به ازای هر عملیات (رمزگشایی متقارن، رمزنگاری نامتقارن، رمزنگاری متقارن، امضاء دیجیتال، تولید کلید متقارن و تولید کلید نامتقارن) دستور(ات) مورد نیاز باید جداگانه آورده شوند.

نکات

* تمامی عملیات، حتی تولید کلید ها، می بایست توسط ابزار OpenSSL انجام گردد. OpenSSL ابزاری بسیار قدرتمند بوده که امکانات کامل کریپتوگرافی را در کنار دیگر خدمات در دسترس قرار می‌دهد.

* تمامی دستورات می بایست تحت خط فرمان لینوکس قابل اجرا باشند. استفاده از کتابخانه های OpenSSL در این تمرین مد نظر نیست.

* در تمام عملیات، به الگوریتم و طول کلید ها توجه لازم را به عمل آورید.

* نتیجه‌ی عملیات امضاء دیجیتال با ایجاد MAC (تولید Hash به صورت دستی و امضاء آن با کلید خصوصی) متفاوت است.

* تمامی موارد خواسته شده (5 فایل مجزا) باید در یک فایل فشرده با نام شماره‌ی دانشجویی شما ارسال گردد.

* با توجه به تصحیح اتوماتیک، در نام‌گذاری فایل‌های ارسالی دقت لازم به عمل آورید.