هوالحق

تمرین کامپیوتری شماره ۲
مبانی امنیت شبکه، پاییز ۱۴۰۲

این تمرین شامل دو بخش می‌باشد. در مرحله اول شما با چگونگی پیکربندی پست الکترونیک امن با استفاده از پروتکل S/MIME آشنا خواهید شد. در مرحله دوم نیز با استفاده از ابزار OpenSSL به انجام عملیات رمزنگاری و رمزگشایی متقارن و نامتقارن مبادرت خواهید ورزید.

۱) شما موظف هستید که در پاسخ ایمیل دریافته شده، یک ایمیل S/MIME با استفاده از دستور العمل ذیل ارسال نمائید:

- ایمیل S/MIME عبارت است از ایمیل که دارای امضاء دیجیتال شما می باشد و همچنین این ایمیل باید Encrypt شده نیز باشد.
- بدیهی است که برای ارسال ایمیل به همراه امضای دیجیتال، نیاز به یک کلید خصوصی و همچنین کلید عمومی دارید. کلید عمومی در S/MIME به صورت یک گواهی (Certificate) می باشد. این گواهی همان کلید عمومی شماست که توسط یک بنیاد معتمد امضاء شده است.
- برای دریافت کلید های عمومی و خصوصی (گواهی) خود باید در یک سایت ارائه دهنده ی گواهی SSL ثبت نام نمایید و گواهی را برای ایمیل خود دریافت کنید. تعداد سرویس دهندگان رایگان محدود است، پس برای راحتی کار به شما سرویس صدور گواهی رایگان از بنیاد Actalis معرفی می‌گردد.
- پس از مراجعه به سایت Actalis، عملیات ثبت نام گواهی (S/MIME) را برای ایمیل خود انجام دهید.
- پس از اتمام مراحل ثبت نام، یک ایمیل شامل فایل گواهی به آدرس ایمیل شما ارسال خواهد شد. دقت کنید که رمز عبور گواهی تنها در آخرین مرحله از ثبت نام به شما نمایش داده می‌شود، فلذا از آن محافظت به عمل آورید. فایل گواهی شما یک فایل با پسوند pfx می‌باشد. حتماً در مورد تفاوت فایل‌ها با پسوند pfx و cer تحقیق کنید.
- پس از این باید فایل pfx را در نرم افزار کلاینت ایمیل خود (Microsoft Outlook) وارد کنید. برای این کار در قسمت Trust Center از تنظیمات Microsoft Outlook جستجو کنید.
- پس از وارد کردن گواهی، نرم افزار Outlook دارای کلید عمومی و خصوصی (گواهی) شما خواهد شد. یک ایمیل جدید در پاسخ این ایمیل ایجاد کنید، در تنظیمات این ایمیل دنبال گزینه‌هایی باشید که به این ایمیل جاری **امضای دیجیتال** شما را اضافه کرده، ایمیل را **Encrypt** کرده و همچنین ایمیل را به صورت **Clear Text Sign** بفرستد و درخواست **رسید S/MIME** را نیز از گیرنده داشته باشد.

هوالحق

تمرین کامپیوتری شماره ۲
مبانی امنیت شبکه، پاییز ۱۴۰۲

در نهایت در **متن** ایمیل خود:

- نام و نام خانوادگی و شماره دانشجویی خود را بنویسید.
- پاسخ پرسش های زیر را بدهید:
  - تفاوت فایل های pfx، cer و pem در چیست؟
  - چرا روی فایل pfx پسورد گذاشته می شود؟ این پسورد چه نقشی در کلید های عمومی و خصوصی دارد؟
  - چرا برای انجام این تمرین نیاز به یک کلاینت ایمیل مانند Microsoft Outlook داریم؟
  - در صورتی که یک ایمیل به همین صورت امضا شده و رمز شده را به یک فرد بدون کلاینت ایمیل بفرستید (مثلا یک ایمیل Gmail که از طریق وب اپلیکیشن مرورگر استفاده می‌گردد)، امضای دیجیتال و رمزنگاری در سمت گیرنده چگونه بروز می یابد؟ (پیشنهاد می‌شود این کار را انجام دهید.)

همچنین می‌بایست در **پیوست** این ایمیل، فایل‌های قسمت دوم تمرین را ارسال کنید.

۲) شما (Bob) مجموعه موارد زیر را از Alice در پیوست ایمیل دریافت کرده اید:

- یک فایل کلید متقارن key_1.hex که شامل یک رشته ۱۶ بایتی به فرمت hex بوده که ۸ بایت ابتدایی آن مقدار IV و ۸ بایت انتهایی آن مقدار کلید می‌باشد.
- یک فایل رمز نگاری شده با کلید متقارن گفته شده به نام m1.enc که با الگوریتم DES CFB رمز شده است.

ابتدا می‌بایست کلید عمومی Alice را از گواهی ایمیل دریافتی استخراج کنید. در مرحله اول، فایل گواهی Alice (netsecf1402@outlook.com) را از کلاینت ایمیل خروجی بگیرید. در مرحله بعد سعی کنید تا کلید عمومی Alice را از گواهی مربوطه (در قالب یک فایل با فرمت pem) با استفاده از دستورات openssl استخراج کنید.

پس از رمزگشایی فایل message_1.enc، محتوای آن را تکمیل کرده و با نام message_2.txt ذخیره کنید. سپس موارد زیر را تولید و به Alice ارسال نمائید:

- یک فایل کلید متقارن با نام **key_2.hex.enc** که **با کلید عمومی Alice به صورت نامتقارن با الگوریتم RSA رمز شده است**. این فایل کلید متقارن باید شامل یک رشته ۴۸ بایتی با فرمت hex باشد. ۱۶ بیت اول رشته نشان‌دهنده مقدار IV و ۳۲ بیت انتهایی می‌بایست نشان‌دهنده کلید رمزگشایی باشد.
- رمز شده فایل تکمیل شده message_2.txt با نام **message_2.enc** که با کلید key_2 تولید شده در بند قبلی و با الگوریتم AES 256 CBC به صورت متقارن رمز شده است.

هوالحق

تمرین کامپیوتری شماره ۲
مبانی امنیت شبکه، پاییز ۱۴۰۲

- امضاء دیجیتال فایل message_2.txt تکمیل شده که توسط کلید خصوصی متناظر با گواهی ایمیل شما و همچنین استفاده از الگوریتم درهم‌ریزی sha3-256 تولید شده است به نام **message_2.sign.sha3256** .
- کلید عمومی شما با نام **bob_public.pem** . توجه کنید که کلید عمومی و خصوصی شما بایستی از گواهی ایمیل دریافت شده در قسمت اول تمرین استخراج گردد و به هیچ عنوان مجاز به تولید کلیدهای نامتقارن توسط OpenSSL نیستید.
- 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 استخراج کلیدهای نامتقارن از گواهی) دستور(ات) مورد نیاز باید جداگانه ذکر شوند.

همچنین به نکات زیر توجه لازم را مبذول دارید:

- تمامی عملیات 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.
- ممکن است بعضی از الگوریتم‌های رمزنگاری مورد استفاده در نسخه OpenSSL 3.x.x به صورت مستقیم پشتیبانی نگردد. در این حالت می‌توانید OpenSSL را با الگوریتم‌های Legacy فراخوانی کنید و نیازی به استفاده از ابزار دیگری نخواهد بود.
- تمامی دستورات می بایست تحت خط فرمان لینوکس قابل اجرا باشند. استفاده از کتابخانه‌های OpenSSL در این تمرین مد نظر نیست.
- لطفاً فقط از نسخه اصلی و رسمی ابزار OpenSSL استفاده کنید. نسخه‌های مشابه و Branch های غیر رسمی (مانند آنچه در بعضی نسخه‌های سیستم عامل macOS به صورت پیشفرض وجود دارد) نتایج شما را برای نسخه‌های اصلی غیر قابل استفاده خواهد کرد.
- در تمام عملیات، به نوع الگوریتم، طول کلیدها و نام فایل‌ها توجه لازم را به عمل آورید. لطفاً **فقط** ۵ فایل خواسته شده در بخش دوم این تمرین را ارسال کنید. **بخش دوم این تمرین به صورت خودکار تصحیح خواهد شد** و هر نوع مغایرت در این موارد باعث از دست رفتن نمرات قسمت‌های مربوطه می‌گردد.
- نتیجه عملیات امضاء دیجیتال در دنیای واقعی با ایجاد MAC نامتقارن (تولید Hash به صورت دستی و رمزکردن آن با کلید خصوصی نظیر آنچه در متن درس دیده‌اید) در پیاده‌سازی اندکی متفاوت است. در این تمرین **امضاء دیجیتال** از شما خواسته شده است.
- تمامی موارد خواسته شده (**۵ فایل مجزا**) باید در یک فایل فشرده با نام شماره دانشجویی شما با فرمت ZIP که با کلمه عبور netsecf1402 محافظت شده است در ضمیمه ایمیل ارسال گردد. در صورت عدم محافظت فایل فشرده با کلمه عبور، ایمیل شما به عنوان اسپم شناخته شده و به مقصد نخواهد رسید.