تمرین شماره ۵

درس: مبانی امنیت شبکه‌های کامپیوتری

نیمسال دوم سال تحصیلی ۰۵-۱۴۰۴

این تمرین شامل دو بخش مي‌باشد. در مرحله اول شما با چگونگي پيكربندی پست الكترونيك امن با استفاده از پروتكل S/MIME آشنا خواهيد شد. در مرحله دوم نيز با استفاده از ابزار OpenSSL به انجام عمليات رمزنگاری و رمزگشايي متقارن و نامتقارن مبادرت خواهيد ورزيد.

دستور کار اول:

به آدرس درج شده در پاورقی[1]، يك ايميل S/MIME با استفاده از دستور العمل ذيل ارسال نمائيد :

- ايميل S/MIME عبارت است از ايميل كه دارای امضاء ديجيتال شما مي باشد و همچنين اين ايميل بايد Encrypt شده نيز باشد.

- بديهي است كه برای ارسال ايميل به همراه امضای ديجيتال، نياز به يك كليد خصوصي و همچنين كليد عمومي داريد. كليد عمومي در S/MIME به صورت يك گواهي (Certificate) مي باشد. اين گواهي همان كليد عمومي شماست كه توسط يك مرجع معتمد امضاء شده است.

- برای دريافت كليد های عمومي و خصوصي (گواهي) خود بايد در يك سايت ارائه دهنده ی گواهي SSL ثبت نام نماييد و گواهي را برای ايميل خود دريافت كنيد. تعداد سرويس دهندگان رايگان محدود است، پس برای راحتي كار به شما سرويس صدور گواهي رايگان از مرجع Actalis معرفي مي‌گردد.

- پس از مراجعه به سايت Actalis، عمليات ثبت نام گواهي (S/MIME) را برای ايميل خود انجام دهيد.

[1] matin.nabizadeh@ut.ac.ir

- پس از اتمام مراحل ثبت نام، يك ايميل شامل فايل گواهي به آدرس ايميل شما ارسال خواهد شد. دقت كنيد كه رمز عبور گواهي تنها در آخرين مرحله از ثبت نام به شما نمايش داده مي‌شود، فلذا از آن محافظت به عمل آوريد. فايل گواهي شما يك فايل با پسوند ۱۲p مي‌باشد حتماً. **در مورد تفاوت فايل‌ها با پسوند (p) ۱۲pfx و cer تحقيق كنيد.**

- پس از اين بايد فايل ۱۲p را در نرم افزار كلاينت ايميل خود (Microsoft Outlook) وارد كنيد. براى اين كار در قسمت Trust Center از تنظيمات Microsoft Outlook جستجو كنيد.

- پس از وارد كردن گواهي، نرم افزار Outlook داراى كليد عمومي و خصوصي (گواهي) شما خواهد شد. يك ايميل جديد در پاسخ اين ايميل ايجاد كنيد، در تنظيمات اين ايميل دنبال گزينه‌هايي باشيد كه به اين ايميل جارى امضاى ديجيتال شما را اضافه كرده، ايميل را **Encrypt** كرده و همچنين ايميل را به صورت **Clear Text Sign** بفرستد و درخواست رسيد **S/MIME** را نيز از گيرنده داشته باشد

در متن ایمیل خود، پس از درج نام و نام خانوادگی‌تان، به پرسش‌های زیر پاسخ دهید:

- تفاوت فایل های cer، pem و pfx(12) در چیست؟

- چرا روی فایل p12 پسورد گذاشته مي شود؟ این پسورد چه نقشي در کلید های عمومي و خصوصي دارد؟
- چرا برای انجام این تمرین نیاز به یك کلاینت ایمیل مانند Microsoft Outlook داریم؟

- در صورتي که یك ایمیل به همین صورت امضا شده و رمز شده را به یك فرد بدون کلاینت ایمیل بفرستید (مثلا یك ایمیل Gmail که از طریق وب اپلیکیشن مرورگر استفاده مي‌گردد)، امضای دیجیتال و رمزنگاری در سمت گیرنده چگونه بروز مي یابد؟ (پیشنهاد مي‌شود این کار را انجام دهید.)

همچنین مي‌بایست در پاسخ این ایمیل، لینك گوگل درایو فایل‌های قسمت دوم تمرین را ارسال کنید.

دستور کار دوم:

شما (Bob) مجموعه موارد زیر را از Alice در پیوست ایمیل دریافت کرده اید (به همراه تمرین داده شده است):

- يك فايل كليد متقارن key_1.hex كه شامل يك رشته ٣٢ بايتي به فرمت hex بوده كه ٨ بايت ابتدايي آن مقدار IV و ٢٤ بايت انتهايي آن مقدار كليد مي‌باشد.

- يك فايل رمز نگاری شده با كليد متقارن گفته شده به نام message_1.enc كه با الگوريتم DES EDE3 CBC رمز شده است.

ابتدا مي‌بايست كليد عمومي Alice را از گواهي ايميل دريافتي استخراج كنيد. در مرحله اول، فايل گواهي Alice (آدرس ايميل ارسال كننده صورت سؤال) به همراه تمرين در اختيار شما قرار داده شده است. در مرحله بعد سعي كنيد تا كليد عمومي Alice را از گواهي مربوطه (در قالب يك فايل با فرمت pem با استفاده از دستورات openssl استخراج كنيد.

پس از رمزگشايي فايل message_1.enc محتوای آن را تکمیل کرده و با نام message_2.txt ذخيره كنيد. سپس موارد زير را توليد و به Alice ارسال نمائيد (به همراه پاسخ تمرين در اسلرن طبق دستورالعمل انتهای تمرین قرار دهید):

- يك فايل كليد متقارن با نام **.key۲hex.enc-** كه با كليد عمومي **Alice** به صورت نامتقارن با الگوريتم **RSA** رمز شده است. اين فايل كليد متقارن بايد شامل يك رشته ١٦ بايتي با فرمت hex باشد. ٨ بايت اول رشته نشاندهنده مقدار IV و ٨ بايت انتهايي مي‌بايست نشاندهنده كليد رمزگشايي باشد.

- رمز شدهٔ فایل تکمیل شده message_2.txt با نام **message_2.enc** که با کلید key_2 تولید شده در بند قبلي و با الگوریتم DES CBC به صورت متقارن رمز شده است.
- امضاء دیجیتال فایل message_2.txt تکمیل شده که توسط کلید خصوصي متناظر با گواهي ایمیل شما و همچنین استفاده از الگوریتم درهم‌ریزی sha 256 تولید شده است به نام message_2.sign.sha256 .

- کلید عمومي شما با نام . **bob-public.pem** توجه کنید که کلید عمومي و خصوصي شما بایستي از گواهي ایمیل دریافت شده در قسمت اول تمرین استخراج گردد و به هیچ عنوان مجاز به تولید کلیدهای نامتقارن توسط OpenSSL نیستید.

- یك فایل با نام **instructions.txt** که تمامي دستورات برای عملیات انجام شده درون آن موجود باشد. به ازای هر عملیات (رمزگشایي متقارن، رمزنگاری نامتقارن، رمزنگاری متقارن، امضاء دیجیتال، تولید کلید متقارن و استخراج کلیدهای نامتقارن از گواهي) دستور(ات) مورد نیاز باید جداگانه ذکر شوند.

همچنین به نکات زیر توجه لازم را مبذول دارید:

- تمامي عملیات مي بایست توسط ابزار OpenSSL انجام گردد. OpenSSL ابزاری بسیار قدرتمند بوده که امکانات کامل کریپتوگرافي را در کنار دیگر خدمات در دسترس قرار مي‌دهد.

- ممکن است بعضي از الگوریتم‌های رمزنگاری مورد استفاده در نسخه .OpenSSL x.x۳ به

صورت مستقيم پشتيباني نگردد. در اين حالت مي‌توانيد OpenSSL را با الگوريتم‌های Legacy فراخواني كنيد و نيازی به استفاده از ابزار ديگری نخواهد بود.

- تمامي دستورات مي بايست تحت خط فرمان لينوكس قابل اجرا باشند. استفاده از كتابخانه‌های OpenSSL در اين تمرين مد نظر نيست.

- لطفاً فقط از نسخه اصلي و رسمي ابزار OpenSSL استفاده كنيد. نسخه‌های مشابه و Branch های غير رسمي (مانند آنچه در بعضي نسخه‌های سيستم عامل macOS به صورت پيشفرض وجود دارد) نتايج شما را برای نسخه‌های اصلي غير قابل استفاده خواهد كرد.

- در تمام عمليات، به نوع الگوريتم، طول كليدها و نام فايل‌ها توجه لازم را به عمل آوريد. فقط ۵ فايل خواسته شده در بخش دوم اين تمرين را ارسال كنيد. بخش دوم اين تمرين به صورت خودكار تصحيح خواهد شد و هر نوع مغايرت در اين موارد باعث از دست رفتن نمرات قسمت‌های مربوطه مي‌گردد.

- نتيجه عمليات امضاء ديجيتال در دنيای واقعي با ايجاد MAC نامتقارن (توليد Hash به صورت دستي و رمزكردن آن با كليد خصوصي نظير آنچه در متن درس ديده‌ايد) در پياده‌سازی اندكي متفاوت است. در اين تمرين امضاء ديجيتال از شما خواسته شده است.

- تمامي موارد خواسته شده (۵ فايل مجزا) بايد در يك فايل فشرده با نام و نام خانوادگی شما با فرمت ZIP در سامانه ارسال شود.

ملاحظات تمرین

- تمرین‌ها به صورت انفرادی انجام می‌شوند.
- لطفا پاسخ خود را در قالب یک فایل PDF با فرمت زیر در سامانه Elearn بارگذاری کنید:

StudentID_Lastname_HW5

- امکان ارسال تمرین نهایتاً با دو روز تاخیر با کسر ۱۰ درصد نمره به ازای هر روز وجود دارد.
- در صورت استفاده از منابعی غیر از کتاب مرجع در انجام تمرین، لطفاً حتماً نام منبع خود را ذکر کنید. در صورت مشاهده شباهت غیرمعمول میان پاسخ‌های دو نفر یا در صورتی که پاسخ‌ها برابر با محتوای منابعی غیر از کتاب مرجع باشد و نام منابع مورد استفاده ذکر نشده باشد، نمره‌ای برای شما منظور نخواهد شد.

موفق باشید!