1. تفاوت بین فایل‌های pfx، cer و pem در چیست؟

فایل pfx به صورت یک باندل شامل کلید خصوصی و certificate مربوط به آن کلید خصوصی است که توسط یک پسورد محافظت می‌شود که در صورت دسترسی به فایل، امکان دسترسی به کلید خصوصی به راحتی فراهم نباشد. این فایل، یک فایل باینری است.
فایل cer که شامل certificate (که خود شامل کلید عمومی است) است. از تفاوت‌های این فایل با فایل pfx می‌توان به اینکه دارای کلید خصوصی نیست و رمزشده هم نیست، اشاره کرد. این فایل می‌تواند به صورت باینری (در حالت DER) و یا به صورت Base64 باشد. این فایل جهت استفاده عموم، به فرمت X.509 ذخیره می‌شود.
فایل PEM (Privacy Enhanced Email) نیز یک فایل است که به فرمت Base64 ذخیره می‌شود و می‌تواند شامل هر یک از مقادیر کلید عمومی، کلید خصوصی و یا certificate باشد. این مورد نیز به صورت رمز شده نیست.

2. چرا روی فایل pfx پسورد گذاشته می‌شود؟ این پسورد چه نقشی در کلیدهای عمومی و خصوصی دارد؟

همانطور که در سوال قبل ذکر شد، دلیل پسورد گذاشتن روی این فایل، وجود کلید خصوصی در فایل است. در این حالت، اگر کسی بتواند به خود فایل دسترسی پیدا کند، بازهم نمی‌تواند به کلید خصوصی دسترسی پیدا کند و از آن استفاده کند. همچنین برای ارسال ایمیل نیز می‌توان مشخص کرد که به ازای هربار دسترسی به این فایل (برای مثال برای ارسال هر ایمیل و یا خواندن ایمیل رمز شده)، پسورد هم خواسته شود.
در واقع، هدف این پسورد محافظت از کلید خصوصی است. وگرنه کلید عمومی که نیازی به محافظت ندارد و برای عموم مردم قابل دسترس است.

3. چرا برای انجام این تمرین نیاز به یک کلاینت ایمیل مانند Microsoft Outlook داریم؟

دلیل اینکه به کلاینت ایمیل برای انجام این کار نیاز داریم، این است که وب اپ‌هایی نظیر gmail از S/MIME پشیبانی نمی‌کنند و این پشتیبانی به برخی کلاینت‌های ایمیل نظیر Microsoft Outlook محدود می‌شود. در نتیجه برای اینکه قابلیت ارسال/دریافت ایمیل رمز شده و یا امضا کردن ایمیل و بررسی امضای ایمیل دریافت شده را داشته باشیم، باید از یکی از این کلاینت‌ها استفاده کنیم که از S/MIME پشتیبانی می‌کنند.

4. 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 می‌یابد؟

همانطور که در سوال قبل ذکر شد، وب اپ جیمیل از S/MIME پشتیبانی نمی‌کند و به همین دلیل اصلا امکان انتخاب کلید عمومی و کلید خصوصی را در آن نداریم. به همین دلیل، با توجه به اینکه کلید عمومی ثبت نشده، اصلا امکان رمز کردن پیام در outlook با گیرنده مورد نظر وجود ندارد. از طرفی، خود جیمیل نیز توانایی ارسال ایمیل رمزشده را نیز ندارد.

همچنین، جیمیل توانایی امضا کردن پیام را نیز ندارد. از طرفی، در صورت دریافت یک ایمیل امضا شده، امضا که یک attachment به نام smime.p7s است را به طور کلی ignore می‌کند زیرا آن را نمی‌شناسد. در واقع ایمیل نمایش داده شده به کاربر به صورتی است که انگار از ابتدا امضا نشده است.