به نام او

تمرین دوم درس رمزنگاری و امنیت شبکه

مهلت تحویل: ۹۰/۳/۹

الف) سیستم رمز نامتقارن

۱- شبه برنامه الگوریتم مجذور- ضرب را برای محاسبه $a \bmod n$ که در آن نمایش دودویی b به صورت $B_k b_{k-1} \ldots b_1 b_0$ است, به دو صورت زیر ارائه دهید:

الف) در نظر گرفتن بیتهای b به ترتیب از سمت راست به چپ (شروع کردن با بیت با کمترین وزن)

ب) در نظر گرفتن بیتهای b به ترتیب از سمت چپ به راست (شروع کردن با بیت با بیشترین وزن)

۲- مثالی از گونه مینیاتوری الگوریتم کلید عمومی دیفی-هلمن با پارامترهای زیر ارائه دهید :

- پیمانه اول (q) چهار رقمی دلخواه
- ریشه (α) یک رقمی دلخواه

(دقت کنید که عدد α انتخابی شما بایستی مولد گروه ضربی Z_q^* باشد.)

۳- گونه مینیاتوری الگوریتم کلید عمومی RSA (با پیمانه n=p.q سه رقمی) را برای موجودیتهای A و B طراحی نموده ازسوی موجودیت A، پیام دودویی m=01010101 را به طور محرمانه و اصیل برای موجودیت B ارسال نمایید.

۴- الگوریتم کلید عمومی RSA در کدامیک از نحوه های کاری ECB ، CBC ، CFB و OFB قابل بکارگیری است؟ دلیل خود را بیان کنید.

ب) مدیریت کلید

۱- مدیریت کلید مبتنی بر سیستم رمز متقارن را با مدیریت کلید مبتنی بر رمز کلید عمومی از جهات مختلف مقایسه کنید.

۲- توزیع کلید متمرکز و نامتمرکز یعنی چه؟ مزایا و معایب هر یک را برشمرید.

۳- پروتکل احراز اصالت و تبادل کلید VSP در زیر تشریح شده است:

مجموعه پروتکل VSP جهت برقراری سرویس‌های امنیتی مورد نیاز در کاربرد صدارسانی روی IP (VOIP) طراحی شده است. این مجموعه شامل پروتکل‌هایی برای احراز اصالت و تبادل کلید، ایجاد هماهنگی بین عناصر سیستم صدارسانی و تغییر پارامترهای امنیتی عناصر سیستم است.

یکی از پروتکلی های VSP برای انجام فرآیند احراز اصالت دو طرفه بین کاربر و میزبان صدارسانی و برقراری یک کلید نشست بین آنها طراحی شده است. به دلیل نیاز به سرعت و کارایی زیاد در کاربرد مورد نظر، این پروتکل بر مبنای روش تحدی-تقابل و با استفاده از تابع درهم سازی کلید دار یا MAC طراحی شده است. در این پروتکل فرض می‌شود که هر کاربر در سیستم دارای یک کلمهٔ عبور است که تنها در انحصار خود اوست و سرویس دهنده تنها مقدار درهم شدهٔ کلمهٔ عبور همهٔ کاربران را در اختیار دارد (که البته از روی آن نمی‌تواند به کلمهٔ عبور دست پیدا کند). از این مقدار درهم شده به عنوان یک کلید مخفی از پیش مشترک بین کاربر و میزبان استفاده می‌شود بنابر این، مقدار درهم شدهٔ کلمهٔ عبور کاربر A در ارتباط با میزبان B را با K_{AB} نشان می‌دهیم.

پروتکل احراز اصالت و تبادل کلید VSP بین کاربر A و میزبان B در شکل زیر نشان داده شده است. نماد $<M>_K$ به معنی MAC پیام M با کلید K است.

$$
\begin{array}{ll}
(1) & A \rightarrow B : A \\
(2) & B \rightarrow A : N_B \\
(3) & A \rightarrow B : N_A, < N_B, N_A >_{K_{AB}} \\
(4) & B \rightarrow A : K_1, K_2, < N_A, K_1 >_{K_{AB}}
\end{array}
$$

در قدم اول پروتکل، عامل A شناسهٔ خود را برای شروع پروتکل به B ارسال می‌کند. عامل B در پاسخ، نانس N_B را تولید و به عنوان تحدی برای A ارسال می‌کند. در قدم سوم، عامل A نیز نانس خود N_A را به عنوان پیام تحدی خود و مقدار MAC روی نانس N_B و نانس خودN_A با کلید K_{AB} را به عنوان مقابله با تحدی قبلی B برای وی ارسال می‌کند. عامل B به محض دریافت این پیام، مقدار $<N_B,N_A>K_{AB}$ را به کمک اطلاعات قبلی خود مجدداً محاسبه نموده با مقدار MAC دریافتی مقایسه می‌کند. در صورت مساوی بودن این دو با یکدیگر، عامل B اصالت عامل A را احراز می‌کند. در قدم آخر پروتکل نیز عامل B دو زیر کلید K_1 و K_2 را به صورت تصادفی تولید نموده، به همراه مقدار MAC روی نانس N_A و K_1 با کلید K_{AB} برای A ارسال می‌کند. عامل A با دریافت این پیام، بازسازی مقدار MAC دریافتی و مقایسهٔ آن با مقدار دریافتی اصالت B را بررسی می‌کند.

اکنون هر دو عامل A و B قادر به ساختن کلید نشست جدید خود هستند. این کلید نشست عبارت است از:

$$K = <N_A , K_2> K_{AB}$$

تمام ارتباطات بعدی عوامل A و B به کمک این کلید امن خواهد شد.

- پروتکل فوق را از لحاظ امنیتی تحلیل کنید یعنی نشان دهید که اصالت طرفین برای یکدیگر محرز می شود و کلید نیز به صورت امنی مبادله می شود.

- حمله ای بر علیه پروتکل VSP به صورت زیر قابل طرح است. این حمله را شرح دهید:

$$
\begin{array}{ll}
(1) & A \rightarrow E_B : A \\
(2) & E_B \rightarrow A : N_B \\
(3) & A \rightarrow E_B : N_A, < N_B, N_A >_{Kab} \\
\quad (1') & A \rightarrow E_B : A \\
\quad (2') & E_B \rightarrow A : N_A \\
\quad (3') & A \rightarrow E_B : N'_A, < N_A, N'_A >_{Kab} \\
(4) & E_B \rightarrow A : N'_A, N'_A, < N_A, N'_A >_{Kab}
\end{array}
$$

دقت کنید که E_B به معنی "نفوذی در نقش B" است و قسمت های تورفته نشان دهنده شروع یک نشست جدید از پروتکل است.

ج) زیرساخت کلید عمومی

۱- تفاوت گونه های مختلف استاندارد x509 را در تعیین ساختار گواهینامه شرح دهید (اینترنت)

۲- تعریف, ضرورت و روش اجرایی ابطال یک گواهینامه دیجیتال را بیان کنید.

۳- فرض کنید که اشخاص A و B گواهینامه خود را به ترتیب از مراجع صدور گواهینامه CA_A و CA_B دریافت کرده اند. اگر دو مرجع مذکور نیز به نوبه خود تحت نظارت مستقیم مرجع ریشه صدور گواهینامه (Root CA) قرار داشته باشند, جزئیات روند احراز اصالت شخص A را توسط شخص B شرح دهید.

۴- راجع به استانداردهای PKCS تحقیق کنید. به طور خاص مشخص کنید که هرکدام از این استانداردها (که با شماره از یکدیگر جدا می شوند) چه چیزهایی را تعیین می کنند؟

۵- OpenCA یک نرم افزار متن باز تحت لینوکس برای انجام عملیات مرکز صدور گواهی است. به کمک اینترنت راجع به این نرم افزار تحقیق نموده سئوالات زیر را پاسخ دهید:

- OpenCA چه سرویس هایی از CA را ارائه میدهد؟
- OpenCA برای انجام عملیات رمزنگاری خود از چه نرم افزاری استفاده میکند؟
- OpenLDAP و OpenOCSP چه نقشی در فعالیت مرکز صدورگواهی دارند؟
- آیا نرم افزارهای متن باز دیگری برای ارائه خدمات CA وجود دارند؟

۶- HSM (Hardware Security Module) چیست و چه اهمیتی در فعالیت CA دارد؟