امنیت – تمرین جبرانی

سوال اول

احراز هویت و احراز اصالت تفاوت هایی دارند. در احراز هویت می میخواهیم هویت شخص کاربر را مورد تایید قرار دهیم تا در قدم بعدی دسترسی های او را چک کنیم، اما در احراز اصالت میخواهیم مطمئن شویم محتوای یک پیام یا شیئ دستخوش تغییر نشده باشد، حتی اگر احراز هویت انجام شده باشد زیرا خود کاربر احراز شده میتواند عامل مخرب باشد. برای مثال ابتدا باید احراز هویت یک فرد تایید شده تا بتواند پیام هایی در قالب پیام رسان برای دیگران ارسال کنید، اما در قدم بعد برای هر پیام باید احراز اصالت کرد تا مطمئن شویم پیام ها رو بین راه تغییر نکرده باشند.

سوال دوم

محرمانگی (confidentiality): هدف آن هست که محتوا یک پیام بین افراد مربوطه محرمانه بماند و دیگران قادر به خواندن آن نباشند.

صحت (Integrity): صحیح بودن داده ها را مطمئن میشود، به طوری که دستخوش تغییر یا جعل نشده باشند.

قابلیت دسترسی (availability): سرویس مورد نظر در دسترس باشد و دچار اختلالات از هر نوع نشود.

محافظت فیزیکی (physical protection): به صورت فیزیکی سرویس یا سرور و یا هر چیز دیگری که تحت امنیت ماست دچار مشکل و یا تحدید فیزیکی قرار نگیرد.

تشخیص هویت (authenticity): هویت کاربری که از سرویس ها استفاده میکند تشخیص و تایید شده باشد تا افراد غیرمجاز قادر به استفاده از آن نباشند.

حدود اختیارات (authority): دسترسی کاربران را مشخص میکند به گونه ای که هر کسی نتواند هر اقدامی را انجام دهد و نیاز به سطح اختیارات و دسترسی خاصی باشد.

حریم خصوصی (privacy): در اینجا امنیت اطلاعات شخصی و حساس افراد یک مورد امنیتی است به طوری که با لو رفتن آن ها، شخص در معرض خطر قرار میگیرد.

سوال سوم

نیاز است در هر یک از m پیام ارسال شده عبارتی که هویت فرستنده را تایید میکند ذکر شود که فرستنده را اثبات کند. در قدم بعد نیاز به عبارتی داریم تا صحیح بودن محتوا پیام ارسالی را تضمین کند. در نهایت باید خود محتوا پیام رمزنگاری شود تا محرمانگی آن حفظ شود. با استفاده از کلید خصوصی که بین هر دو نفر یکتا است میتوان هویت را تشخیص و تایید کرد و محتوا پیام را رمزنگاری و صحت آن را تایید کرد. پس تنها با دو جفت کلید میتوان ارتباط امن داشت.

سوال چهارم

صورت سوال ناواضح!

سوال پنجم

در رمز دنباله ای ما هر یک بایت را رمزنگاری کرده و ارسال میکنیم در صورتی که در رمزنگاری قطعه ای (قالبی) باید قطعه از دیتا داشته باشیم تا رمزنگاری صورت بگیرد. پس روش اول ساده تر و سریع تر نسبت به روش دوم است و دوباره کاری در رمز دنباله ای مشاهده نمیشود. همچنین در رمز قطعه ای به کد بیشتری برای طراحی سیستم نیاز داشته ولی رمزگشایی کردن آن مشکل تر از رمز دنباله ای است.

سوال ششم

امنیت – تمرین جبرانی

هر نفر دو کلی خصوصی و عمومی میتواند بسازد که کلید خصوصی را در جای امن نگه داشته و کلید عمومی توسط افرادی که به او اطلاعات ارسال میکنند استفاده میشود.

سوال هفتم

برای الگوریتم های رمزنگاری مانند DES که دو طرفه هستند، رمزنگاری و رم زگشایی هر دو توسط یک الگوریتم یا یک کلید انجام میشود. به گونه ای که در رمزگشایی round key به طور برعکس حالت رمزنگاری استفاده میشود تا رمزگشایی صورت بگیرد. حال اگر از یک Hash Function به عنوان round key استفاده کنیم، عملا دیگر round keyنخواهیم داشت و رمزنگاری و رمزگشایی با استفاده از یک الگوریتم انجام میشود. در توضیح دقیق تر، از ی ک round keyو بخشی از یک block استفاده میکند تا عمل رمزنگاری را با نصفه دیگر block انجام ده د. حال اگر ب ه جای round key یک Hash Function استفاده کنی م، رمزنگاری دو طرفه خواهد شد.

سوال هشتم

در PGP، یک مدل اطمینان (trust model) برای احراز هویت امضای دیجیتال استفاده میشود، به طوری که بجای وابستگی به یک CA مرکزی، اگر اطمینان داشته باشیم یک امضای دیجیتال هویت یک فرد را تایید کند پس تمام امضا های دیجیتال او را نیز اعتماد میکند.

سوال نهم

در حالت کلی، یک connection ارتباط بین کلاینت و سرور بوده که با استفاده از پروتکل هایی نظیر TCP صورت میگیرد و معمولا کوتاه مدت است. سرور ها پس از مدتی ارتباط را قطع میکنند. اما در Session یک وضعیت نگهداری اطلاعات سمت سرور است تا ارتباط مجدد از سر گیرد. پس یک connection میتواند قطع شود اما session از بین نرود. برای SSL هم همین داستان تکرار میشود با این تفاوت که در session پارامتر های آن رمزنگاری شده.

سوال دهم

یک session key ساخته شد تا از درخواست های متعدد برای ساخت کلید جدید از کلید master جلوگیری شود، یا به عبارتی داخل آن جلسه دیگر نیاز نیست برای هر درخواست، تیکت Kerberos جدید زده شود. این مکانیسم به صورت distributed است.

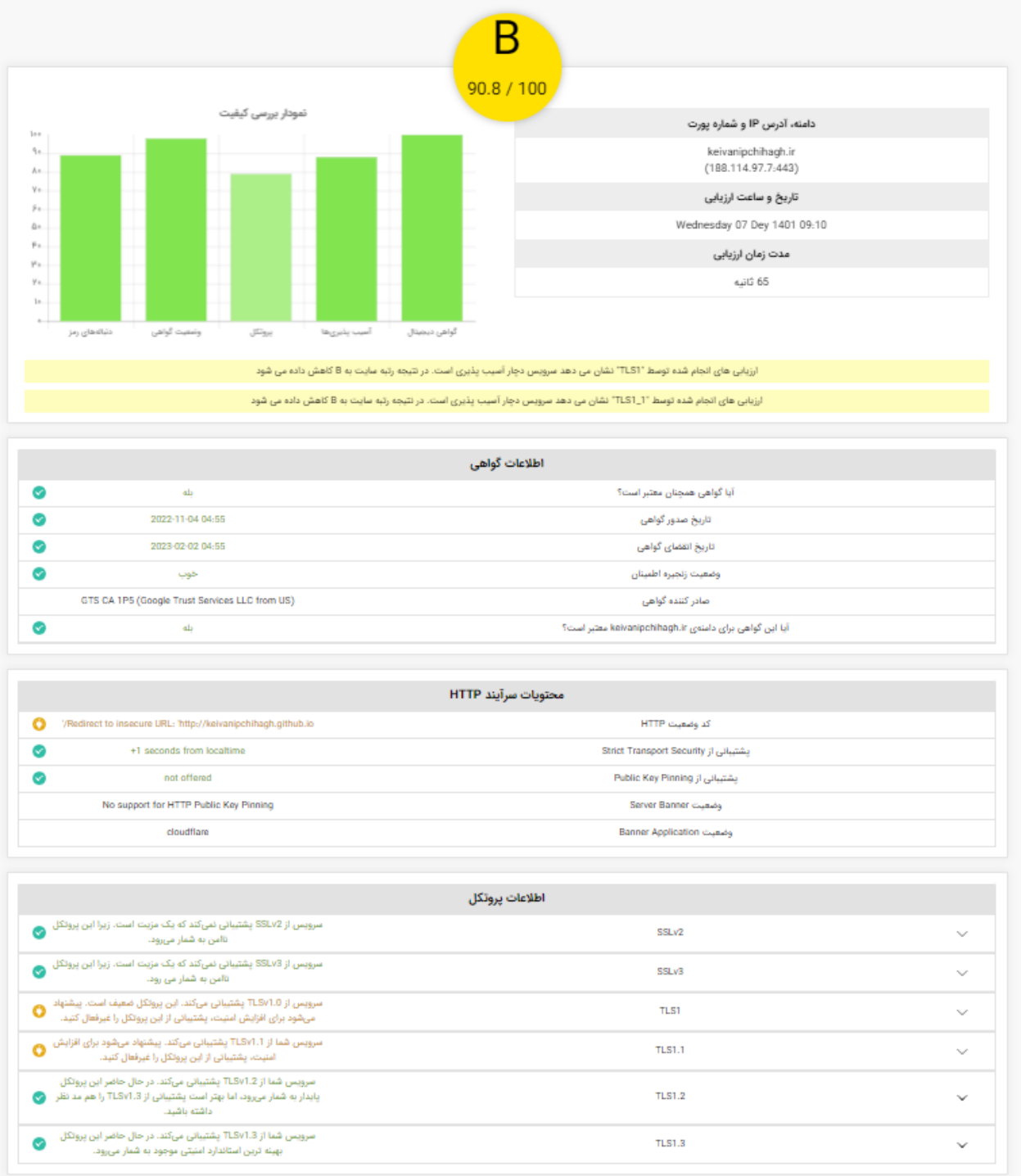
سوال یازدهم

تفاوت این دو سیستم در آن است که برای تبادل کلید، صرفا یک شیئ کلید را ساخته و به دیگری میدهد. این کار باعث ایجاد تهدید Man-In-The-Middle میشود، اما سیستم توافق کلید یک مکانیسم دو طرفه بوده که در آن هر دو طرف بر سر یک کلید مشترک توافق میکنند. منطقی است که سربار Key Agreement بیشتر باشد چرا که نیاز بیشتری به ارتباط اولیه برای ساختن کلید مشترک دارند، پس سربار زیادی دارد تا در همه جا از آن استفاده کنیم.

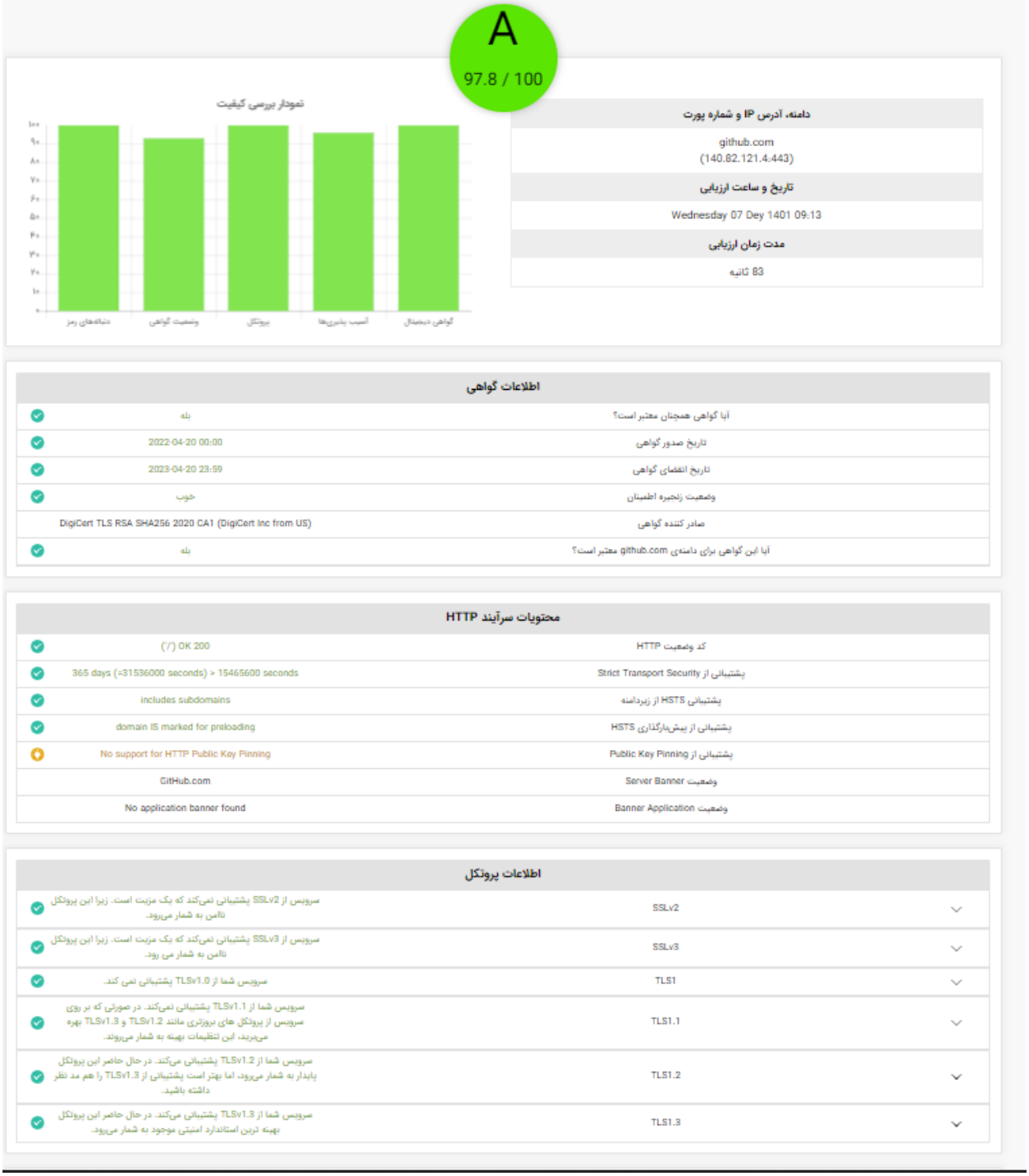
پس زمانی که بخواهیم ارتباط بلند مدت ایجاد کنیم و در آن کلید های دیگر بسازیم، بهتر است از این روش استفاده کنیم اما زمانی که ارتباط کوتاهی داشته باشیم این روش به صرفه نیست و استفاده از Key Exchange بهتر است چرا که ارتباط کوتاه تر از آن است که لو رود.

سوال دوازدهم

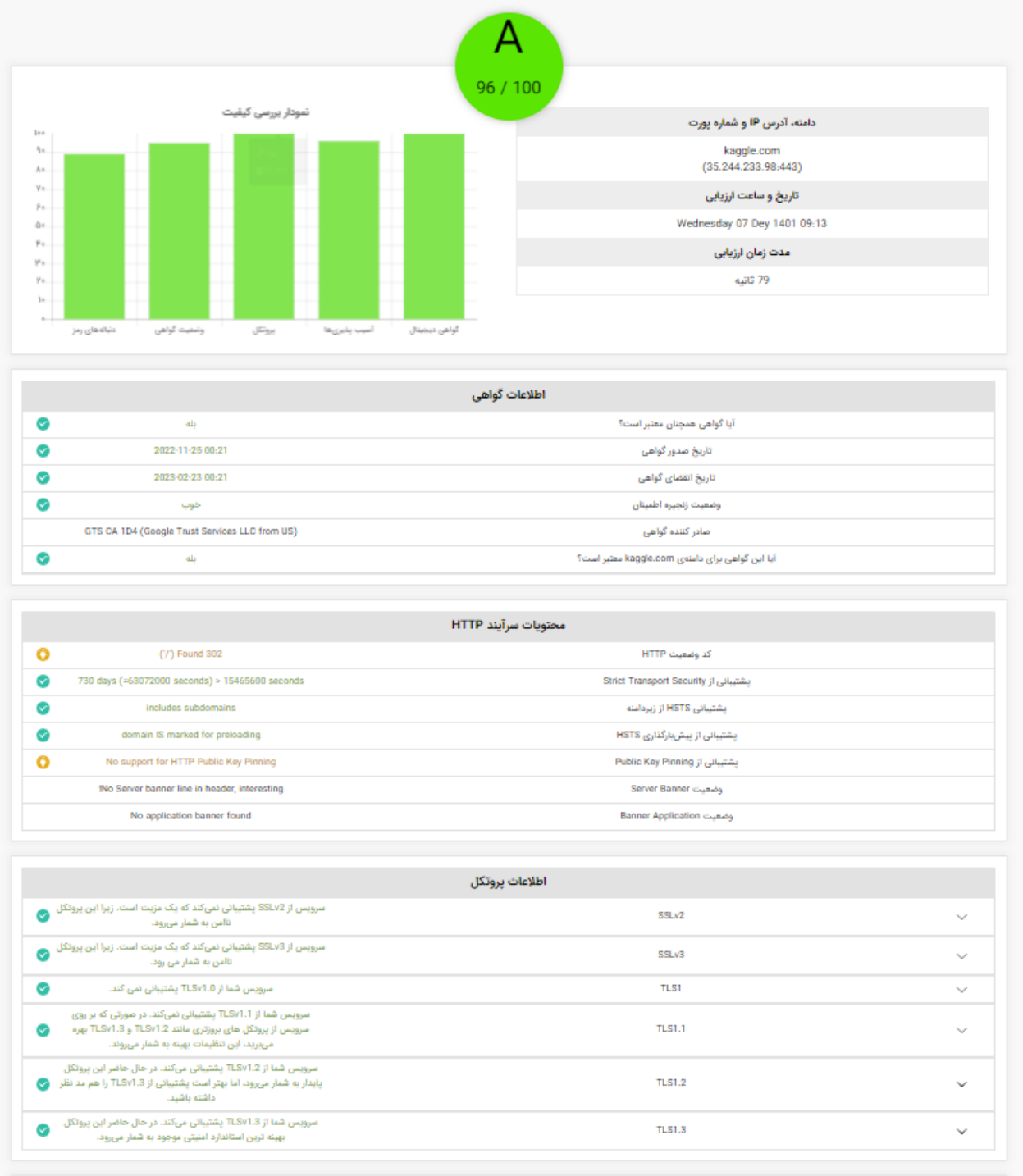
امنیت – تمرین جبرانی



امنیت – تمرین جبرانی



امنیت – تمرین جبرانی



سوال سیزده

یک پروتکل ارتباطی از جنس توافق بر SA و کلید هی مشترک ها توسط دو طرف ارتباط است که در RFC 2408 تعریف شده است. این پروتکل از UDP برای ارتباط استفاده میکند.

سوال چهاردهم

کیوان ایپچی حق - ۹۸۳۱۰۷۳

امنیت – تمرین جبرانی

سوال پانزدهم

سرویس هایی که از GPG در آنها استفاده شده است:

- Confidentiality
- Authentication
- Compression
- E-mail compatibility
- Segmentation

سوال شانزدهم

در این روش، فرستنده کلید جلسه GPG رمزنگاری شده خود را به گیرنده ارسال میکند و گیرنده با استفاده از کلید خصوصی خود قادر به رمزگشایی آن است. پس در این حال هر دو میتوانند با یکدیگر ارتباط امین داشته باشند.

سوال هفدهم

هدف وجود این پروتکل، انتقال record بین سرور و کلاینت بوده که امنیت داده را تضمین میکند. پس دو اصل را برقرار کرده که Confidentiality و Integrity بوده، حتی در محیط های غیر امن و غیر رمزنگاری شده.

سوال هجدهم

سوال نوزدهم

یک session key ساخته شد تا از درخواست های متعدد برای ساخت کلید جدید از کلید master جلوگیری شود، یا به عبارتی داخل آن جلسه دیگر نیاز نیست برای هر درخواست، تیکت Kerberos جدید زده شود. این مکانیسم به صورت distributed است.

سوال بیستم

در PGP فشرده سازی بعد از اعمال امضای دیجیتال و قبل از رمزنگاری انجام میشود که به وسیله الگوریتم ZIP انجام شده و شامل Confidentiality و Integrity در این فرایند بوده.

سوال بیست و یکم

دلیل این امر امنیت بالاتر AES نسبت به DES است به گونه ای که در AES قادر هستیم کلید های ۱۲۸ و ۱۹۲ و ۲۵۶ بیتی انتخاب کنیم، در صورتی که در DES صرفا کلید ها ۵۶ بیتی هستند. همچنین DES شکسته شده پس.. (:

سوال بیست و دوم

رمز نگاری ECC کاملا مشابه RSA است به گونه ای که سطح امنیت هر دو یکسان است اما در ECC طول کلید کمتری استفاده میشود که مزیت آن محسوب میشود. به همین دلیل سرعت ECC نیز بالاتر است.

سوال بیست و سوم

تفاوت این دو سیستم در آن است که برای تبادل کلید، صرفا یک شیئ کلید را ساخته و به دیگری میدهد. این کار باعث ایجاد تهدید Man-In-The-Middle میشود، اما سیستم توافق کلید یک مکانیسم دو طرفه بوده که در آن هر دو طرف بر سر یک کلید مشترک توافق میکنند. منطقی است که سربار Key Agreement بیشتر باشد چرا که نیاز بیشتری به ارتباط اولیه برای ساختن کلید مشترک دارند، پس سربار زیادی دارد تا در همه جا از آن استفاده کنیم.

امنیت – تمرین جبرانی

سوال بیست و چهارم

در رمزنگاری متقارن، همان کلیدی که در رمزنگاری استفاده شد در رمزگشایی نیز استفاده میشود اما در رمزنگاری نا متقارن دو کلید متفاوت جهت رمزنگاری و رمز گشای استفاده میشود.

این دو تفاوت هایی دارند برای مثال سرعت رمزنگاری متقارن بالاتر است ولی امنیت رمزنگاری نا متقارن بالاتر است پس هر کدام مور استفاده متفاوتی میتواند داشته باشد. زمان هایی که امنیت اهمیت بالاتری نسبت به سرعت دارد از کلید متقارن استفاده کنیم و برعکس زمانی که سرعت اولویت بالاتری نسبت به امنیت دارد (چیزی مهمی در اشتراک نمیگذاریم) از کلید متقارن استفاده کنیم، مخصوصا زمانی که ارتباط کوتاه است.

پس نمیتوان گفت کدام بهتر است (: هر دو خوب هستند، وقتی بجا استفاده شوند.

سوال بیست و پنجم

در واقعیت ممکن است اما احتمال این موضوع خیلی کم است. قطعا دو رشته ای وجود دارند که تابع Hash یکسانی داشته باشند به تصادف. مثل کیف پول دیجیتال است که دو نفر میتوانند به کیف پول یکسان وصل شوند، احتمال این امر وجود داشته ولی اینقدر کم است که چشم پوشی میکنیم.