تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰

عنـــوان درس: مباحث نودرفناوری اطلاعات

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)۱۵۱۱۰۰۸

۱- کدامیک از اهداف امنیت سیستمهای رایانه ای این است که اطلاعات در سیستم رایانه ای و نیز اطلاعات مبادله شده بین سیستمهای رایانه ای از تغییرات یا حذف غیرمجاز به دور باشد؟

۱. محرمانگی ۲. تمامیت ۳. دسترس پذیری ۴. تصدیق

۲- تایید پیام به چه معنا می باشد؟

۱. اطمینان از اینکه شخصی که سیستم ادعا می کند پیام را فرستاده به راستی پیام را فرستاده است یا نه

۲. اطمینان از اینکه شخص مورد نظر پیام فرستاده شده را دریافت کرده یا نه

۳. اطمینان از اینکه پیام دریافتی به درستی ارسال شده است یا نه

۴. اطمینان از اینکه پیام ارسالی به درستی دریافت شده است یا نه

۳- بنا بر فرضیه تخمین خطر، خطر نسبی با چه فرمولی سنجیده می شود؟

۱. خطر نسبی= ارزش دارای × درجه آسیب پذیری × درجه تهدید

۲. خطر نسبی= ارزش دارای × درجه آسیب پذیری + درجه تهدید

۳. خطر نسبی= ارزش دارای + درجه آسیب پذیری × درجه تهدید

۴. خطر نسبی= ارزش دارای + درجه آسیب پذیری + درجه تهدید

۴- کدامیک از دسته حملات به سرویسهای امنیتی از نوع غیر فعال می باشد؟

۱. وقفه ۲. دستبرد ۳. تغییر ۴. جعل

۵- در صورتی که متن اصلی "the party" و متن رمز شده"WKH SDUWB" باشد, از چه روش رمزگذاری استفاده شده است؟

۱. رمزگذاری سزار ۲. رمزگذاری تک حرفی ۳. رمز پلی فر ۴. رمز هیل

۶- نقطه قوت رمز ورنام(کلید یک بار مصرف) چیست؟

۱. کلید تصادفی به آسانی قابل ذخیره کردن است و کلید فقط یک بار باید استفاده شود.

۲. تکرار حروف تا حدی محو می شود, زیرا حروف با کلیدهای مختلف رمز شده باقی می ماند.

۳. به واسطه فرکانس نسبی حروف و ساختار زبان به راحتی متن رمز شده قابل تشخیص و رمزگشایی نمی باشد.

۴. اگر کلید واقعا تصادفی باشد, پیدا کردن کلید از روی متن رمز شده غیر ممکن خواهد بود

۷- کدام نوع از روشها برای از بین بردن امکان حمله هایی است که بر اساس تحلیل آماری عمل می کنند؟

۱. DES ۲. S-DES ۳. شانون ۴. انتشار و اغتشاش

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰

عنـــوان درس: مباحث نودرفناوری اطلاعات

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)۱۵۱۱۰۰۸

۸- درکدامیک از الگوریتمهای رمز قطعه ای, هر قطعه از متن اصلی ۶۴ بیتی است و به طور مستقل رمز می شود؟

۱. روش رمز زنجیره قطعات رمز
۲. روش دفترچه الکترونیکی
۳. روش پسخور رمز
۴. روش پسخور خروجی

۹- کدام گزینه جزو نقاط ضعف روش رمزگذاری انتها به انتها می باشد؟

۱. این روش معمولا نمی تواند به صورت نرم افزاری پیاده سازی شود, ولی برای روش رمزگذاری پیوند این شدنی است.
۲. نمی توان اطلاعات مربوط به بسته مانند آدرس گیرنده و فرستنده را هم رمز کرد. یعنی فقط اطلاعات متن رمز می شود.
۳. در شبکه های بزرگ, این روش به تعداد زیادی عملگر رمز نیاز دارد.
۴. کاربران هیچ اختیاری در مورد امنیت اعمال شده ندارند, زیرا این روش معمولا عمومی است و کاربر تسلطی بر آن یٔ تغییرات در آن ندارد.

۱۰- در صورتی که پیام کوتاه باشد, از کدام نوع از حملات به سیستمهای رمز با کلید نامتقارن, میتوان استفاده کرد؟

۱. روش جستجوی جامع
۲. یافتن کلید خصوصی از کلید عمومی
۳. حدس زدن پیام رمز شده
۴. حل مساله سخت ریاضی متناظر با الگوریتم

۱۱- نقطه ضعف روش "اعلان" برای توزیع کلید عمومی کدام است؟

۱. سهولت در جعل کلید عمومی
۲. تمرکز کلیدها در یک فهرست
۳. تراکم مراجعه به یک نقطه
۴. تراکم مراجعه به چند نقطه

۱۲- کدامیک از روشهای احراز اصالت کاربران, یکتا بوده و همیشه در اختیار هستند و در ضمن رونوشت برداری و دوباره سازی آنها سخت می باشد؟

۱. کلید کلمه عبور
۲. کلید فیزیکی
۳. کلید اطلاعاتی
۴. کلید بیولوژیکی

۱۳- مزیت و عیب ارسال پیام امضاء شده به داور جهت تایید قبل از ارسال به گیرنده چیست؟

۱. مزیت آن عدم انکار امضاء توسط فرستنده - عیب آن امکان الزام در استفاده از مهر زمانی
۲. مزیت آن عدم انکار امضاء توسط فرستنده - عیب آن لزوم اعتماد دو طرف به داور
۳. مزیت آن سهولت در توزیع کلید - عیب آن لزوم اعتماد دو طرف به داور
۴. مزیت آن سهولت در توزیع کلید - عیب آن امکان الزام در استفاده از مهر زمانی

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰

عنـــوان درس: مباحث نودرفناوری اطلاعات

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)۱۵۱۱۰۰۸

۱۴- مشکل اساسی استفاده از راه حل "مهر زمانی" برای جلوگیری از ارسال مجدد پیام چیست؟

۱. دو رایانه فرستنده و گیرنده باید همزمان باشند تا مهر زمانی مفهوم یکسانی برای هر دو داشته باشد.

۲. برای هر کاربر باید شمارنده مستقلی وجود داشته باشد تا مهر زمانی قابل استفاده باشد.

۳. این روش برای ارتباطهای بدون اتصال مناسب نمی باشد. زیرا برای هر ارتباط یک بار به عمل دست دادن نیاز دارد.

۴. این روش برای ارتباطهای با اتصال مناسب نمی باشد. زیرا برای هر ارتباط یک بار به عمل دست دادن نیاز دارد.

۱۵- فناوری DES چیست؟

۱. یک استاندارد رمزنگاری است که IKE نوع CES-CBC, ۵۶ بیتی آن را پیاده سازی می کند.

۲. یک پروتکل رمزگذاری کلید عمومی است که اجازه می دهد دو کاربر بر روی یک کانال ارتباطی نا امن, یک ارتباط امن مشترک را فراهم کنند.

۳. یک الگوریتم درهمساز است که برای احراز اصالت بسته ها استفاده می شود.

۴. یک سیستم رمزنگاری کلید عمومی است که امضای RSA عدم انکار را فراهم می کند.

۱۶- در مراحل مبادله سرویس احراز اصالت, TS_2 به چه معنا می باشد؟

۱. نشان می دهد که بلیط برای TGS است.

۲. شناسه کاربر در کارفرمایی را که قرار دارد به AS اعلام میکند.

۳. به AS اعلام می کند که کاربر درخواست دسترسی به TGS دارد.

۴. به کارفرما زمان صدور بلیط را اطلاع می دهد.

۱۷- کدام گزینه خصوصیات PKI را شامل می شود؟

۱. محرمانگی- تمامیت- احراز اصالت - عدم انکار-کنترل- تولید گواهی

۲. محرمانگی- تمامیت- احراز اصالت- عدم انکار- تولید گواهی - دسترس پذیری

۳. محرمانگی- تمامیت- احراز اصالت- تولید گواهی -کنترل- دسترس پذیری

۴. محرمانگی- تمامیت- احراز اصالت - عدم انکار-کنترل- دسترس پذیری

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰

عنـــوان درس: مباحث نودرفناوری اطلاعات

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)۱۵۱۱۰۰۸

۱۸- اصالت گواهی بر اساس چه ساختاری احراز می گردد؟

۱. ساختار سلسله مراتبی ۲. ساختار فرایندی ۳. ساختار متقاطع ۴. ساختار متداخل

۱۹- کدامیک از روشهای اصلی حفاظت از کلید خصوص کاربر به عنوان روش برتر شناخته شده است؟

۱. رمز کردن کلید توسط کلمه عبور ۲. ذخیره در کارتهای حافظه دار

۳. ذخیره در کارتهای هوشمند ۴. ذخیره دردستگاه های کاملا غیرقابل نفوذ

۲۰- اشکال روش تولید زوج کلید رمزگذاری برای کاربران توسط صادرکننده گواهی چیست؟

۱. کلید تصادفی به آسانی قابل ذخیره کردن است و کلید فقط یک بار باید استفاده شود.

۲. اگر کلید واقعا تصادفی باشد, پیدا کردن کلید از روی متن رمز شده غیر ممکن خواهد بود.

۳. در شبکه های بزرگ, این روش به تعداد زیادی عملگر رمز نیاز دارد.

۴. امکان قابلیت کشف کلید در سیستم وجود دارد.

۲۱- مشکل اساسی برای ارسال کلید عمومی به روش انتقال به صورت فیزیکی چیست؟

۱. قابل اعتماد نبودن آن ۲. محدودیت طول کلید

۳. غیر عملی بودن آن در شبکه ۴. امکان استفاده از روشهای غیراستاندارد رمزگشایی

۲۲- این بیت در محتوای میدانهای کلید یک می شود در صورتی که کلید در حلقه کلید سری ظاهر شود؟

۱. Buckstop ۲. Warnonly ۳. Contig ۴. Keylegit

۲۳- کدام یک از کلمات کلیدی که به سرآیه در MIME اضافه می شوند, غیراجباری می باشد؟

۱. نسخه پروتکل MIME -توصیف محتوی ۲. نسخه پروتکل MIME - نوع محتوی

۳. نسخه پروتکل MIME - شناسه محتوی ۴. شناسه محتوی - توصیف محتوی

۲۴- در کدام نوع از کدگذاری در محتوی MIME خطوط کوتاه هستند اما ممکن است کاراکترهای غیر اسکی باشند؟

۱. ۷bit ۲. ۵bit ۳. Binary ۴. Base۶۴

۲۵- کدام پارامتر در بحث مجمع امنیتی که به عنوان یک مبحث کلیدی در امنیت IP مطرح است, معین می کند که AH و یا ESP کدام یک ارسال مجدد شده است؟

۱. شمارنده دنباله عددی ۲. سر ریز شمارنده دنباله

۳. پنجره ضد تکرار ۴. اطلاعات AH

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰

عنـــوان درس: مباحث نودرفناوری اطلاعات

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)۱۵۱۱۰۰۸

۲۶- مهمترین مشکل امنیتی در سیستمهای توزیع شده چیست؟

۱. کنترل دسترسی ۲. امنیت پروتکل ۳. استاندارد امنیتی ۴. دسترسی به منابع

۲۷- به چه علتی از دستگاه های رابط به صورت پروکسی به عنوان رابط بین ایستگاه مدیریت و کارگذار استفاده می شود؟

۱. به دلیل اینکه بعضی دستگاه ها قابلیت برخورداری از SNMP را ندارند.

۲. به دلیل عدم پیاده سازی SNMP در کارگزار نهایی

۳. جهت به حداقل رساندن ارتباطات بین مرکز مدیریت و کارگزار نهایی

۴. به دلیل اینکه کارگزار نهایی نمی داند که از کدام MIB می تواند برای مدیریت آن کارگزار استفاده کند.

۲۸- در کدامیک از روشهای ایجاد کنترل دسترسی محتاطانه اجازه دسترسی هر کاربر به اشیاء به طور مستقل است و هر ستون در آن به طور مستقل ذخیره می شود؟

۱. جدول حفاظت ۲. کلمه عبور فایل

۳. مبتنی بر تواناییها ۴. لیست کنترل دسترسی

۲۹- کدامیک از مدلهای امنیتی جزو بهترین مدلهای امنیتی است که به صورت مدل ماشین با حالت متناهی می باشد؟

۱. Biba ۲. BLP

۳. Clark-Wilson ۴. Goguen-Meseguer

۳۰- در کدامیک از روشهای دیواره آتش معمولا یک مسیریاب نقش دیوار آتش را بازی می کند که توسط نرم افزار مربوطه، بسته های مجاز و غیرمجاز به آن معرفی می شوند؟

۱. دروازه فیلتر بسته ها ۲. دروازه سطح مدار

۳. دروازه در سطح برنامه کاربردی ۴. دروازه معمولی

مباحث نو در فناوری اطلاعات نیمسال دوم ۹۲-۹۱	
1	ب
2	ب
3	الف
4	ب
5	الف
6	د
7	د
8	ب
9	ب
10	ج
11	الف
12	د
13	ب
14	الف
15	الف
16	د
17	د
18	الف
19	ج
20	د
21	ج
22	الف
23	د
24	ب
25	ج
26	د
27	الف
28	د
29	ب
30	الف