تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰ | **سری سوال :** یک ۱

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۱- تایید پیام به چه معنا می باشد؟

۱. اطمینان از اینکه شخصی که سیستم ادعا می کند پیام مرا 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 درست دریافت شده است یا نه

۲- نوع حمله های "دستبرد" و "تغییر" به ترتیب کدامیک است؟

۱. فعال - فعال ۲. غیرفعال - فعال ۳. غیرفعال - غیرفعال ۴. فعال - غیرفعال

۳-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

۴- در این روش رمزگذاری ابتدا یک کلمه به عنوان کلید انتخاب می شود. سپس جدولی ۵×۵ تشکیل می شود. ابتدا کلید در جدول نوشته می شود. بقیه خانه های جدول به ترتیب با حروف از A تا Z که در کلمه رمز یا کلید نیستند پر می شود.

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

۵- نقطه قوت این رمز این است که تکرار حروف تا حدی محو می شود، زیرا حروف با کلیدهای مختلف رمز می شوند؟

۱. رمز چند حرفی ۲. رمز تک حرفی ۳. رمز ورنام ۴. رمز هیل

۶- بر اساس کدام خاصیت در روش DES اگر دو متن بسیار مشابه که تفاوت آنها فقط در چند بیت باشد توسط کلید یکسانی رمز شوند, متنهای رمز شده با هم تفاوت بسیار خواهند داشت؟

۱. خاصیت بهمنی ۲. خاصیت جایگزینی ۳. خاصیت جایگشتی ۴. خاصیت انتشار

۷- در کدامیک از روشهای رمزگذاری متقارن, پیام در ابتدای مسیر رمز می شود و در انتها رمز گشایی می شود؟

۱. روش رمزگذاری ابتدا به انتها ۲. روش رمزگذاری انتها به ابتدا

۳. روش رمزگذاری ابتدا به ابتدا ۴. روش رمزگذاری انتها به انتها

۸- کدام روش حمله به RSA ، دربرگیرنده روشهای مختلف است که معادل تجزیه اعداد می باشد؟

۱. جستجوی جامع ۲. حمله ریاضیاتی ۳. حمله توان مصرفی ۴. حمله زمانی

تعداد سوالات : تستی : ۳۰ تشریحی : ۰ | زمان آزمون (دقیقه) : تستی : ۶۰ تشریحی : ۰ | سری سوال : ۱ یک

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۹- 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

۱۰- نقطه ضعف روش "مرجع مورد اعتماد" 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

۱۱- "کلمه عبور" و "پرسشنامه"، مثال هایی از کدام نوع کلیدها هستند؟

۱. کلیدهای عمومی
۲. کلیدهای اطلاعاتی
۳. کلیدهای فیزیکی
۴. کلیدهای بیولوژیکی

۱۲- روشهای اصلی احراز اصالت کاربران کدام است؟

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

۱۴- مشکل اساسی استفاده از راه حل "استفاده از شمارنده" 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
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- از لحاظ دسترسی به سیستم رایانه ای، کدامیک خارجی ترین لایه می باشد؟

۱. سخت افزار
۲. سیستم عامل
۳. برنامه های کاربردی
۴. کاربران

۱۶- استفاده از مهر زمانی, شماره سریال, و یا عدد تصادفی برای جلوگیری از کدام نوع از حملات مهم در شبکه می باشد؟

۱. وقفه
۲. تکرار
۳. تغییر
۴. جعل

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰ | **سری سوال :** ۱ یک

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۱۷- کدامیک از خصوصیات PKI بیانگر این است که پیام دست نخورده انتقال یافته و اطمینان از رسیدن پیام به مقصد و اطمینان از عدم دریافت بیش از یک نسخه پیام توسط گیرنده مسلم است؟

۱. محرمانگی ۲. تمامیت ۳. عدم انکار ۴. کنترل

۱۸- اصالت گواهی بر اساس چه ساختاری احراز میگردد؟

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

۱۹- کدامیک از روشهای اصلی حفاظت از کلید خصوصی 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- 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

۲۳- شناسه کاربر در کارفرمایی را که قرار دارد به AS اعلام می کند؟

۱. TS_1 ۲. TS_2 ۳. IDc ۴. Eks

۲۴- کدام پارامتر در بحث مجمع امنیتی که به عنوان یک مبحث کلیدی در امنیت IP مطرح است, یک عدد ۳۲ بیتی است که در سرآیه های AH یا ESP به عنوان میدان شماره سریال استفاده می شود؟

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 | **سری سوال :** ۱ یک

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۲۵- 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.

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

۱. جدول حفاظت

۲. کلمه عبور فایل

۳. مبتنی بر تواناییها

۴. لیست کنترل دسترسی

۲۷- در این روش تشخیص نفوذگر از ویژگی های کاربران استفاده می شود که در آن با بررسی فواصل زمانی که کاربر برای تایپ حروف صرف می کند کاربر واقعی شناخته می شود؟

۱. روش مبتنی بر پرونده کاربر

۲. تحلیل امضاء

۳. روش مبتنی بر عمل

۴. روش مبتنی بر پرونده نفوذگر

۲۸- رابطه ریسک نسبی چیست؟

۱. ارزش عنصر * آسیب پذیری * حملات

۲. ارزش عنصر + آسیب پذیری+ حملات

۳. ارزش عنصر * آسیب پذیری * نقاط قوت

۴. ارزش عنصر * آسیب پذیری + نقاط قوت

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

۱. Biba

۲. BLP

۳. Clark-Wilson

۴. Goguen-Meseguer

۳۰- در کدام روش مورد استفاده در دیواره آتش, عمل فیلتر کردن در سطح برنامه کاربردی اعمال می شود و معمولا برای یک سرویس خاص است؟

۱. دروازه فیلتر بسته ها

۲. دروازه در سطح مدار

۳. دروازه در سطح برنامه کاربردی

۴. دروازه شبکه