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- بیشترین تحقیقات در امنیت رایانه در کدامیک از حیطه های ذیل می باشد؟

۱. محرمانگی ۲. تمامیت ۳. ایمنی ۴. دسترسی پذیری

۲- در این روش رمز گذاری, هر حرف با حرف بعدی که فاصله ثابت و یکسانی از حرف قبلی دارد، جایگزین می شود؟

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

۳- 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

۴- در این الگوریتم ورودی و خروجی ۵۴ بیتی است و کلید طول متغیری بین ۸ تا ۱۰۲۴ بیت دارد. این الگوریتم برای پردازنده های ۱۶ بیتی طراحی شده است. از ساختار فیستل استفاده نمی کند بلکه MD5 است؟

۱. RC5 ۲. RC2 ۳. IDEA ۴. CAST

۵- عبارت زیر از نقاط ضعف کدام روش رمزگذاری می باشد؟
"در عمل لزومی ندارد همه پیام ها رمز شوند، اما در این روش به اجبار همه پیام ها رمز می شوند".

۱. انتها به انتها ۲. پیوند ۳. چرخشی ۴. DES

۶- در این روش رمز گذاری, پیام در ابتدای مسیر رمز می شود و در انتها رمز گشایی می شود. در این روش فقط متن اصلی پیام رمز می شود و از نقطه ای به نقطه دیگر ارسال می شود؟

۱. پیوند ۲. چرخشی ۳. انتها به انتها ۴. DES

۷- 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

۸- روش های اصلی احراز اصالت کاربران شامل کدام کلیدها می باشد؟

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

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

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

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

۱۰- کدام توپولوژی شبکه بر اساس روش نقطه به نقطه می باشد؟

۱. باس ۲. حلقه (نوع اول) ۳. خطی ۴. ستاره

۱۱- 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

۱۲- سرویس کربروس چه نوع سرویس دهنده ای می باشد؟

۱. محرمانگی ۲. تمامیت ۳. احراز اصالت ۴. عدم انکار

۱۳- کدام جزء از پیام در بین مراحل مبادله سرویس احراز اصالت کربروس، به کارفرما زمان صدور بلیط را اطلاع می دهد؟

۱. IDC ۲. TS1 ۳. TS2 ۴. ID7

۱۴- 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

۱۵- کدامیک از روشهای توزیع کلید عمومی از سایر روشها بهتر می باشد؟

۱. ارسال مستقیم توسط کاربر ۲. ذخیره در دفترچه تلفن

۳. استفاده از گواهی ۴. ذخیره در یک گره و دریافت آن با احراز اصالت

۱۶- اصالت گواهی بر اساس کدام ساختار احراز می شود؟

۱. شی گرا ۲. سلسله مراتبی ۳. شبکه ای ۴. رابطه ای

۱۷- کدامیک از راه های اصلی جهت حفاظت کلید خصوصی کاربر از سایر روش ها برتر می باشد؟

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

۳. ذخیره در دستگاه های کاملا غیرقابل نفوذ ۴. ذخیره در کارت های هوشمند

۱۸- در صورتی که کاربر بخواهد فقط وقتی اخطار داده شود که کلیدی که کاملا ارزش ندارد برای رمزگذاری استفاده شود, کدام بیت یک می شود؟

۱. buckstop ۲. warnonly ۳. contig ۴. keylegit

۱۹- کدامیک از سرآیه های زیر در MIME اجباری می باشد؟

۱. نوع محتوا ۲. شناسه محتوا ۳. توصیف محتوا ۴. تاریخ محتوا

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

۲۰- در کدام نوع از انواع کدگذاری در محتوای MIME، خطوط کوتاه هستند، اما ممکن است کاراکترهای غیر اسکی باشند؟

۱. ۷bit ۲. ۵bit ۳. binary ۴. base64

۲۱- کدام گزینه از مزایای اصلی پروتکل دیفی-هلمن می باشد؟

۱. درآن امکان حمله ملاقات در وسط وجود دارد.

۲. با توجه به اینکه کلید جلسه هر لحظه که نیاز باشد قابل تولید است، لذا کلید های رمزگذاری می توانند طول عمر کوتاه داشته باشند.

۳. به دلیل نیاز به عملیات محاسباتی سنگین امکان حمله پابند وجود دارد.

۴. اطلاعاتی راجع به دو طرف تبادل کننده کلید فراهم نمی کند به عبارتی احراز اصالت را انجام نمی دهد.

۲۲- مرورگر اسب تروا از تهدیدهای مربوط به کدامیک از خطرات وب می باشد؟

۱. تمامیت ۲. محرمانگی ۳. عدم سرویس ۴. احراز اصالت

۲۳- درخواستی است که از طرف خریدار به فروشنده ارسال می شود که شامل نوع کارت اعتباری، شناسه یکتا مربوط به این تقاضا و یک عدد تصادفی است؟

۱. درخواست اولیه ۲. پاسخ اولیه ۳. درخواست خرید ۴. پاسخ خرید

۲۴- مهمترین مشکل امنیتی موجود در سیستم های توزیع شده چیست؟

۱. قابلیت اعتماد ۲. دسترسی به منابع ۳. سرعت شبکه ۴. توزیع فرآیندها

۲۵- در این روش کنترل دسترسی محتاطانه، اجازه دسترسی هر کاربر به اشیاء به طور مستقل است. این روش مانند جدول حفاظت است با این تفاوت که هر سطر به طور مستقل ذخیره می شود؟

۱. روش کلمه عبور فایل ۲. روش مبتنی بر تواناییها

۳. روش لیست کنترل دسترسی ۴. روش بیت های حفاظتی

۲۶- یکی از مشکلات این روش، کار با گروه است. یعنی با فرض اینکه کاربر در چند گروه فعال باشد, آنگاه اجازه دسترسی به کاربر در گروه های مختلف مشکل ساز می شود؟

۱. روش کلمه عبور فایل ۲. روش مبتنی بر تواناییها

۳. روش لیست کنترل دسترسی ۴. روش بیت های حفاظتی

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

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- این سیستم برای نیروی هوایی به منظور بررسی رویدادنگاری و ابزار تشخیص نفوذگران طراحی شده است؟

۱. سیستم خبره تشخیص نفوذگر (IDES)
۲. MIDAS
۳. Haystack
۴. RSA

۲۹- "تغییر در برنامه احراز اصالت کاربر در بدو ورود به سیستم", از نکات کدامیک از موارد ذیل از زمان بازیابی حمله می باشد؟

۱. مطالعه اطلاعات رویدادنگاری
۲. شناسایی حساب های رایانه ای و داده های دزدیده شده
۳. معین کردن تغییرات در سیستم
۴. جایگزین کردن سیستم

۳۰- کدام مدل امنیتی, مبتنی بر چارچوب سلسله مراتبی از سطوح درستی است که در آن سطح درستی یک شی بر اساس میزان خرابی ناشی از استفاده نادرست یک موضوع، تعیین می شود؟

۱. مدل امنیتی Biba
۲. مدل امنیتی BLP
۳. مدل Clark-wilson
۴. مدل امنیتی goguen-meseguer