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

عنـــوان درس: مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات۱۱۱۵۰۶۱

۱- این مساله که اطلاعات در سیستم رایانه ای و همچنین نقل و انتقال اطلاعات بین سیستم های رایانه ای برای افراد غیر مجاز لازم است نامفهوم باشد, بیانگر چیست؟

۱. دسترسی پذیری ۲. تمامیت ۳. محرمانگی ۴. احراز هویت

۲- کدام عبارت در خصوص حمله وقفه صحیح است؟

۱. به تمامیت پیام حمله می شود. ۲. به احراز اصالت پیام حمله می شود.

۳. به محرمانگی و کنترل دسترسی پیام حمله می شود. ۴. به دسترسی پذیری پیام حمله می شود.

۳- کدام نوع از جمله به سرویس های امنیتی, بیانگر حمله به تمامیت پیام و عدم انکار است؟

۱. جعل ۲. تغییر ۳. دستبرد ۴. وقفه

۴- اهداف امنیت در رایانه در کدام گزینه به درستی ذکر گردیده است؟

۱. محرمانگی - یکپارچگی - سهولت ۲. تمامیت- یکپارچگی- سهولت

۳. دسترسی پذیری- تمامیت- سهولت ۴. محرمانگی- تمامیت - دسترسی پذیری

۵- به چه دلیلی تشخیص حمله غیر فعال معمولا بسیار دشوار است؟

۱. زیرا در این حمله پیام تغییر می کند. ۲. زیرا در این حمله پیام تغییر نمی کند.

۳. زیرا در این حمله شنود روی پیام آشکار است. ۴. زیرا در ارسال پیام وقفه ایجاد می شود.

۶- دو عامل عمده در امنیت سیستم کدام است؟

۱. قدرت الگوریتم رمز گذاری- وابستگی خروجی به کلید رمزگذاری

۲. قدرت الگوریتم رمز گذاری-وابستگی ورودی به کلید رمزگذاری

۳. قدرت کلید رمزگذاری - وابستگی خروجی به الگوریتم رمز گذاری

۴. قدرت کلید رمزگذاری - وابستگی ورودی به الگوریتم رمزگذاری

۷- امنیت محاسباتی مشروط به کدامیک از موارد زیر است؟

۱. هزینه شکستن متن رمز شده از ارزش خود پیام بیشتر باشد.

۲. هزینه شکستن متن رمز شده از ارزش خود پیام کمتر باشد.

۳. ارزش زمان مورد نظر برای شکستن رمز کمتر از ارزش پیام باشد.

۴. ارزش زمان مورد نظر برای شکستن رمز مساوی ارزش پیام است.

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

عنـــوان درس: مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات۱۱۱۵۰۶۱

۸- در کدام روش ساختار آماری متن اصلی در حوزه وسیعی از متن رمز شده پخش می شود؟

۱. اغتشاش ۲. انتشار ۳. جانشیتی ۴. جایگشتی

۹- الگوریتم های رمز متقارن عمدتاً از چه روشی استفاده می کنند؟

۱. فیستل ۲. ساده جانشینی ۳. جایگشت ۴. ترکیبی

۱۰- در الگوریتم DES که از الگوریتم لوسیفر ساخته شده, طول کلید به چه صورتی تغییر کرده است؟

۱. از ۱۲۸ به ۱۲۰ ۲. از ۱۲۸ به ۵۶ ۳. از ۵۶ به ۱۲۸ ۴. از ۶۴ به ۱۲۸

۱۱- خاصیت بهمنی در DES چگونه است؟

۱. اگر دو متن بسیار مشابه که تفاوت آنها فقط در چند بیت است توسط کلید یکسانی رمز شده باشد، متن های رمز شده باهم تفاوت بسیار خواهند داشت.

۲. اگر دو متن بسیار مشابه که تفاوت آنها فقط در چند بایت است توسط کلید یکسانی رمز شده باشد، متن های رمز شده باهم تفاوت بسیار نخواهند داشت.

۳. اگر دو متن متفاوت که تفاوت آنها فقط در چند بیت است توسط کلید یکسانی رمز شده باشد، متن های رمز شده با هم تفاوت بسیار اندکی داشت.

۴. اگر دو متن بسیار مشابه که تفاوت آنها در تعداد زیادی بیت است توسط کلید یکسانی رمز شده باشد، متن های رمز شده باهم تفاوت بسیار خواهند داشت.

۱۲- دو روش متداول که برای طراحی رمز شکن DES استفاده می شوند, کدام هستند؟

۱. تفاضلی- ترکیبی ۲. خطی- ترکیبی ۳. ترتیبی- ترکیبی ۴. تفاضلی - خطی

۱۳- یکی از روشهای حمله به سیستم های رمز با کلید نامتقارن با فرض اینکه سیستم یکطرفه باشد, کدام است؟

۱. روش جستجوی محدود

۲. یافتن کلید عمومی از کلید خصوصی

۳. حدس پیام رمز شده در صورتی که طول پیام طولانی باشد.

۴. روش جستجوی جامع

۱۴- کدم گزینه یکی از روش های حمله به RSA می باشد؟

۱. حمله تصادفی ۲. حمله ریاضیاتی ۳. حمله محاسباتی ۴. حمله جامع

۱۵- کدام گزینه از روش های جلوگیری از حمله های زمانی است؟

۱. زمان برآوردی ۲. کور کردن ۳. زمان توان مصرفی ۴. جستجوی جامع

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

عنـــوان درس: مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات۱۱۱۵۰۶۱

۱۶- کدام گزینه از جمله روشهای توزیع کلید عمومی می باشد؟

۱. فهرست- اعلان- ترمیم
۲. اعلان- گواهی- ترمیم
۳. گواهی- فهرست- ترمیم
۴. فهرست - اعلان - گواهی

۱۷- کدام گزینه جزء حمله های متداول به شبکه به شمار می رود؟

۱. وقفه
۲. عدم احراز اصالت پیام
۳. ایجاد خطا
۴. ایجاد عدم دسترسی

۱۸- در کدام گزینه, روش های کنترلی برای ایجاد امنیت به درستی ذکر شده است؟

۱. روش پخش- کنترلهای سخت افزاری - تعیین سیاستهای امنیتی
۲. روش رمزنگاری- روش پخش - تعیین سیاستهای امنیتی
۳. روش رمزنگاری- کنترلهای سخت افزاری -روش پخش
۴. روش رمزنگاری- کنترلهای سخت افزاری - تعیین سیاستهای امنیتی

۱۹- لایه های دسترسی به سیستم های رایانه ای به ترتیب از راست به چپ که به صورت سلسله مراتبی بیان شده, کدام است؟

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

۲۰- کدام مورد از سرویس های اصلی PGP می باشد؟

۱. مهر زمانی
۲. احراز اصالت
۳. امضای دیجیتال
۴. درهم سازی

۲۱- فشرده سازی روی پیام به کدام صورت انجام می شود؟

۱. فشرده سازی روی پیام بعد از رمزنگاری و قبل از امضا انجام می شود .
۲. فشرده سازی روی پیام بعد از امضا و قبل از رمزنگاری انجام می شود.
۳. فشرده سازی روی پیام بعد از امضا و قبل از ذخیره سازی انجام می شود.
۴. فشرده سازی روی پیام بعد از رمز نگاری و قبل از ذخیره سازی انجام می شود.

۲۲- کدام گزینه از حالت های اصلی انتقال بسته می باشد؟

۱. انتقال-پخش
۲. انتقال- ارسال
۳. ارسال - تونل
۴. انتقال - تونل

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

عنـــوان درس: مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات۱۱۱۵۰۶۱

۲۳- در کدام گزینه به روش های کنترل دسترسی محتاطانه اشاره شده است؟

۱. جدول وقفه- روش کنترل دسترسی - بیتهای حفاظتی

۲. جدول حفاظت- جدول وقفه - بیتهای حفاظتی

۳. جدول حفاظت- روش کنترل دسترسی - جدول وقفه

۴. جدول حفاظت- روش کنترل دسترسی - بیتهای حفاظتی

۲۴- روش کنترل دسترسی اجباری در چه سطوحی عمل می کند؟

۱. سطح امنیتی- سطح لایه ای

۲. سطح طبقاتی- سطح امنیتی

۳. سطح اولیه - سطح ثانویه

۴. سطح بیرونی - سطح دورنی

۲۵- کنترل اجباری در کدام سطوح صورت می گیرد؟

۱. امنیتی- طبقاتی ۲. طبقاتی- سطحی ۳. لایه ای - امنیتی ۴. دسترسی - لایه ای

۲۶- تفاوت بین ارزیابی خرابی و کنترل خرابی در چیست؟

۱. کنترل خرابی بعد از وقوع حمله مطرح است و ارزیابی خرابی در زمان حمله مطرح است.

۲. کنترل خرابی در زمان حمله مطرح است و ارزیابی خرابی بعد از وقوع حمله مطرح است.

۳. کنترل خرابی و ارزیابی خرابی هر دو در زمان حمله مطرح هستند.

۴. کنترل خرابی و ارزیابی خرابی هر دو بعد از حمله مطرح هستند.

۲۷- کدام مدل امنیتی زیر مبتنی بر عدم دخالت بین کاربران است؟

۱. مدل امنیتی clark - wilson

۲. مدل امنیتی biba

۳. مدل امنیتی blp

۴. مدل امنیتی goguen - meseguer

۲۸- دیوار آتش برای جلوگیری از چه چیزی می تواند استفاده می شود؟

۱. تخریب ۲. وقفه ۳. نقاب زدن ۴. جعل

۲۹- کدام گزینه به نقاط ضعف امنیتی بانک های اطلاعاتی اشاره می کند؟

۱. اسب های تروا - استنتاج - اشتراک

۲. تمامیت داده ها - استنتاج - تفاضل

۳. تمامیت داده ها - استنتاج - اشتراک

۴. تمامیت داده ها- استنتاج - اجتماع

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

عنـــوان درس: مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات۱۱۱۵۰۶۱

۳۰- برنامه ای که کار ناخواسته را در کنار عمل اصلی انجام می دهد؟

۱. ویروس
۲. کرم
۳. اسب تراوا
۴. برنامه های نفوذ کننده