

زمان آزمون (دقیقه): تستی: ۸۰ تشریحی: ۰

تعداد سوالات: تستی: ۳۰ تشریحی: ۰

عنوان درس: مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات ۱۱۵۰۶۱

۱- در ادبیات امنیت رایانه "hash" یعنی:

۰۱. روشی برای پختن سیب زمینی  
۰۲. مقدار رمز شده  
۰۳. کلید رمزنگاری  
۰۴. روش رمزنگاری

۲- در روش رمزنگاری و رمزگشایی ..... ، کلید را فقط طرف فرستنده و گیرنده می دانند.

۰۱. e - signature  
۰۲. گواهی دیجیتال  
۰۳. کلید خصوصی  
۰۴. ژتون امن (Security Token)

۳- ..... یعنی پنهان کردن یک پیام سری در داخل یک پیام معمولی و استخراج پیام سری در مقصد.

۰۱. الگوریتم کلید سری  
۰۲. bytecode  
۰۳. spyware  
۰۴. steganography

۴- عاقبت download پی در پی فایل از اینترنت چیست؟

۰۱. پیدا کردن تعداد زیادی نرم افزار بازی  
۰۲. پیدا کردن تعداد زیادی فایل موزیک  
۰۳. پر کردن رایانه با تعداد زیادی فایل  
۰۴. برخورد تصادفی با یک ویروس رایانه ای و آلوده کردن رایانه و شبکه متصل به آن

۵- برای حفاظت رایانه خود از حملات ویروسی چه می کنید؟

۰۱. من فقط به website های مشهور و معتبر سر می زنم، لذا خطری مرا تهدید نخواهد کرد.  
۰۲. من برای حفاظت رایانه، آنتی ویروس مشهوری را روی رایانه ام نصب می کنم.  
۰۳. من آنتی ویروس مشهوری را روی رایانه ام نصب می کنم و مرتباً با نصب "update" های شرکت سازنده، آنرا به روز می نمایم.  
۰۴. من آنتی ویروس مشهوری را روی رایانه ام نصب می کنم و قسمت "update" آنتی ویروس را روی "بروز رسانی خودکار" قرار می دهم.

۶- ..... آمیزه ای است از علم و هنر برای مصونیت پیام ها از حملات.

۰۱. رمز نگاری  
۰۲. تحلیل رمز  
۰۳. تحلیل رمز و احراز هویت  
۰۴. مکانیزم احراز هویت

## کارشناسی ارشد

حضرت علی(ع): ارزش هر کس به میزان دانایی و تخصص اوست

تعداد سوالات: تستی: ۳۰ تشریحی: ۰  
زمان آزمون (دقیقه): تستی: ۸۰ تشریحی: ۰

عنوان درس: مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات ۱۱۱۵۰۶۱

۷- کدامیک از اقدامات احتیاطی زیر در اتصال اینترنتی به حساب بانکی موثر است.

الف. سرکشی مرتب به حساب اینترنتی برای بررسی فعل و انفعالات بانکی

ب. عدم اتصال به حساب از طریق رایانه های عمومی نظیر کافی نت ها

ج. عدم افشای رمز حساب به سایر افراد، حتی کسانی که مدعی هستند که کارمند بانک یا پلیس می باشند.

۱. الف و ب ۲. ب و ج ۳. الف و ج ۴. الف و ب و ج

۸- در روش رمزنگاری ..... ، یک کلید یکسان مورد استفاده ارسال کننده و هم برای دریافت کننده است.

۱. کلید نامتقارن ۲. کلید متقارن ۳. نا متقارن و hash ۴. hash

۹- روش رمزنگاری کلید خصوصی، روش ..... نیز نامیده می شود.

۱. کلید متقارن ۲. کلید نامتقارن

۳. کلید نامتقارن و Transposition ۴. Transposition

۱۰- در کدام نوع از الگوریتم های رمزنگاری یک جفت کلید مورد استفاده قرار می گیرد؟

۱. کلید متقارن ۲. کلید نامتقارن

۳. کلید متقارن و نامتقارن ۴. کلید عمومی و کلید خصوصی

۱۱- در روش رمزنگاری نا متقارن، فرستنده از چه کلیدی برای رمزنگاری پیامش استفاده می کند؟

۱. خصوصی ۲. عمومی ۳. خصوصی و عمومی ۴. کلید ۱۶ بیتی

۱۲- در روش رمزنگاری نامتقارن دریافت کننده پیام از چه کلیدی برای رمزگشایی پیامش استفاده می کند؟

۱. خصوصی ۲. عمومی ۳. کلید ۱۶ بیتی ۴. کلید ۳۲ بیتی

۱۳- در کدام روش از گزینه های زیر یک کاراکتر با کاراکتر دیگر برای رمزگزاری جا به جا می شود؟

۱. جانشینی ۲. Transposition ۳. DES ۴. RSA

۱۴- در روش ..... ، برای بدست آوردن متن رمز شده از متن اصلی، ترتیب قرارگیری کاراکترها در متن

اصلی تغییر می یابد.

۱. جانشینی ۲. سزار ۳. Transposition ۴. DES

۱۵- الگوریتم رمزنگاری DES که توسط دولت آمریکا اقتباس گردید، می تواند جز کدام نوع از الگوریتم های رمزنگاری

محسوب می شود؟

۱. کلید متقارن ۲. کلید نامتقارن ۳. کلید ۱۶ بیتی ۴. کلید ۳۲ بیتی

زمان آزمون (دقیقه): تستی: ۸۰ تشریحی: ۰

تعداد سوالات: تستی: ۳۰ تشریحی: ۰

عنوان درس: مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات ۱۱۱۵۰۶۱

۱۶- ..... ، یک الگوریتم متداول رمزنگاری کلید عمومی است.

DES .۱      RAS .۲      RSA .۳      RAA .۴

۱۷- ..... ، یعنی رسیدن پیام به گیرنده بدون هیچ تغییری در آن.

۱. محرمانگی (Confidentiality)      ۲. یکپارچگی (Integrity)

۳. احراز هویت (Authentication)      ۴. Cipher

۱۸- امضای دیجیتال نیازمند روش رمزنگاری ..... است.

۱. کلید متقارن      ۲. کلید نامتقارن      ۳. کلید ۳۲ بیتی      ۴. DES

۱۹- فایروال یعنی .....

۱. نرم افزار آنتی ویروس

۲. نرم افزاری که ارتباط با اینترنت را ثبت می کند.

۳. نرم افزاری که ارتباط با اینترنت را ثبت می کند و آنتی ویروس هم هست.

۴. فیلتری که برای اتصال به اینترنت بکار می رود.

۲۰- درمد ..... ، **Ipsec** از اطلاعات تحویل گرفته شده از لایه انتقال به لایه شبکه محافظت به عمل می آورد.

۱. انتقال      ۲. تونل      ۳. انتقال و تونل      ۴. جانشینی

۲۱- **Ipsec** در کدام مد نمی تواند از هدر IP حمایت به عمل آورد؟

۱. انتقال      ۲. تونل      ۳. تونل و انتقال      ۴. Transposition

۲۲- وقتی ما نیازمند به حفاظت از داده به صورت انتها به انتها (host to host) هستیم، معمولاً مد ..... مورد استفاده قرار می گیرد.

۱. انتقال      ۲. تونل      ۳. جانشینی و تونل      ۴. جانشینی

۲۳- کدامیک از شبکه های زیر در داخل یک سازمان بکار گرفته می شود.

۱. خصوصی      ۲. عمومی      ۳. نیمه خصوصی      ۴. نیمه عمومی

۲۴- کدام گزینه زیر بیانگر یک شبکه خصوصی است که از مدل اینترنت استفاده می کند؟

۱. اینترنت      ۲. اینترنتان      ۳. اکسترانت      ۴. VPN

## کارشناسی ارشد

حضرت علی(ع): ارزش هر کس به میزان دانایی و تخصص اوست

تعداد سوالات: تستی: ۳۰ تشریحی: ۰

زمان آزمون (دقیقه): تستی: ۸۰ تشریحی: ۰

عنوان درس: مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات ۱۱۱۵۰۶۱

۲۵- امکان دسترسی مجاز را به کاربران خارج از شبکه را می دهد؟

۱. اینترنت  
۲. اینترانت  
۳. اکسترانت  
۴. اینترنت و اینترانت و اکسترانت

۲۶- مسئولین اینترنت آدرس ها را برای کدامیک از گزینه های زیر رزرو کرده اند؟

۱. اینترنت  
۲. اینترانت  
۳. اکسترانت  
۴. هیچکدام

۲۷- فراهم کننده امن برای LAN ها یی است که از طریق شبکه عمومی اینترنت با یکدیگر در ارتباط هستند.

۱. VPP  
۲. VPN  
۳. VNN  
۴. VNP

۲۸- لایه ..... ، پروتکل امنیتی برای سرویس های امن انتها به انتهای برنامه های کاربردی است.

۱. اتصال داده  
۲. شبکه  
۳. انتقال  
۴. اتصال داده ها و شبکه

۲۹- یک متن دارای یک ..... و یک ..... ، بطور مجزا است.

۱. امضای قراردادی و مرسوم، امضای دیجیتال  
۲. امضای دیجیتال، امضای دیجیتال دیگر  
۳. امضای دیجیتال ، کد رمز  
۴. کد رمز، امضای دیجیتال

۳۰- امضای دیجیتال نمی تواند ایجاد ..... برای پیام نماید.

۱. یکپارچگی  
۲. محرمانگی  
۳. احراز هویت  
۴. غیر انکاری