تعداد سوالات : تستی : ۲۵ **تشریحی :** ۵ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۶۰ | **سری سوال :** یک ۱

عنـــوان درس: شبکه های کامپیوتری ۲

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)،مهندسی فناوری اطلاعات(سیستمهای چند رسانه ای)۱۱۱۵۱۵۲

۱- کدام گزینه صحیح است؟

۱. از TSAP برای تمایز چند نقطه پایانی استفاده می شود که یک NSAP مشترک دارند.

۲. از NSAP برای تمایز چند ماشین استفاده می شود که یک آدرس IP مشترک دارند.

۳. آدرس های پورت نمونه ای از NSAP هستند.

۴. TSAP یک ماشین را به طور منحصر به فرد در کل شبکه مشخص می کند.

۲- در بحث ترمیم خرابی در صورتی که گیرنده ابتدا پیام تصدیق دریافت را ارسال نماید و سپس محتوای قطعه را در استریم خروجی بنویسد و فرستنده همواره آخرین قطعه را مجددا ارسال نماید، کدام گزینه نشان دهنده حالتی است که این روش منجر به تولید پیام تکراری در گیرنده می شود؟
(A: ارسال تصدیق دریافت، W: نوشتن در پردازش خروجی، C: خرابی)

۱. AC(W) ۲. AWC ۳. C(AW) ۴. WAC

۳- کدام گزینه صحیح است؟

۱. با میل کردن بار به سمت ظرفیت شبکه ، ظرفیت مفید با سرعت بیشتری افزایش می یابد.

۲. تاخیر تابعی از بار عرضه شده است.

۳. بار موثر واحد انتقال باری است که در آن تاخیر بیشینه باشد.

۴. با میل کردن بار به سمت ظرفیت شبکه توان همواره افزایش می یابد.

۴- در کدام دسته از پروتکل های زیر، هنگام بروز ازدحام از تکنیک ریزش بسته استفاده می شود؟

۱. XCP، TCP با ECN، TCP

۲. TCP ترکیبی ، FAST TCP، XCP

۳. FAST TCP، CUBIC TCP، TCP با ECN

۴. TCP ترکیبی، TCP، CUBIC TCP

تعداد سوالات : تستی : ۲۵ **تشریحی :** ۵ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۶۰ | **سری سوال :** یک ۱

عنـــوان درس: شبکه های کامپیوتری ۲

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)،مهندسی فناوری اطلاعات(سیستمهای چند رسانه ای)۱۱۱۵۱۵۲

۵- فرض کنید که دو اتصال (کاربر) برای بدست آوردن پهنای باند یک لینک با یکدیگر رقابت می کنند. کدام گزینه در رابطه با تخصیص پهنای باند به این دو کاربر صحیح است؟

۱. اگر دو کاربر پهنای باند را به صورت جمعی افزایش و به صورت جمعی کاهش دهند تخصیص الزاما عادلانه نخواهد بود.

۲. اگر دو کاربر پهنای باند را به صورت ضربی افزایش و به صورت جمعی کاهش دهند تخصیص به یک نقطه کار بهینه همگرا می شود.

۳. شیب خط های افزایش و کاهش جمعی پهنای باند تخصیص یافته به دو کاربر همواره از مبدا مختصات می گذرد.

۴. اگر دو کاربر پهنای باند را به صورت جمعی افزایش و به صورت ضربی کاهش دهند تخصیص از نقطه کار بهینه واگرا خواهد شد.

۶- در پروتکل انتقال بی درنگ (RTP) کدام فیلد از سرآیند بسته این امکان را فراهم می آورد که در هر لحظه بتوان الگوریتم کدگذاری بسته ها را تغییر داد؟

۱. فیلد شناسه همزمان سازی مبدا
۲. فیلد شناسه مبدا مشارکت
۳. فیلد نوع محموله
۴. فیلد CC

۷- در پروتکل TCP از کدام تایمر برای پیشگیری از بن بست استفاده می شود؟

۱. تایمر مداومت
۲. تایمر پایداری
۳. TIME WAIT
۴. تایمر ارسال مجدد

۸- در پروتکل TCP به چه منظور از تصدیق دریافت گزینشی (SACK) استفاده می شود؟

۱. شمارش تعداد ACK های تکراری
۲. تشخیص بهتر بسته هایی که باید مجددا ارسال گردند.
۳. تعیین مقدار بهینه برای اندازه پنجره گیرنده
۴. تعیین مقدار بهینه برای پارامتر آستانه

۹- کدام گزینه در رابطه با پروتکل خوشه در پشته پروتکلی شبکه های تاخیر پذیر (DTN) صحیح است؟

۱. پروتکل خوشه بر روی TCP/IP اجرا می شود.

۲. پروتکل خوشه برای شناسائی ماشین های مبدا و مقصد از آدرس های IP استفاده می کند.

۳. پروتکل خوشه یک پروتکل لایه کاربرد است که در لایه انتقال پیاده سازی شده است.

۴. در پروتکل خوشه منظور از نایب همان مبدا است که بر تحویل صحیح خوشه نظارت می کند.

۱۰- در سرویس دهنده های نام (DNS) کدام نوع از رکوردهای منبع مشخص کننده ماشین هائی از دامنه است که اجازه ارسال ایمیل را دارند؟

۱. SRV
۲. MX
۳. SPF
۴. SOA

تعداد سوالات : تستی : ۲۵ **تشریحی :** ۵ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۶۰ | **سری سوال :** ۱ یک

عنـــوان درس: شبکه های کامپیوتری ۲

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)،مهندسی فناوری اطلاعات(سیستمهای چند رسانه ای)۱۱۱۵۱۵۲

۱۱- کدام یک از انواع MIME به ترتیب برای ارسال داده هائی از نوع اسناد PDF و ادغام چندین پیام در یک پیام واحد به کار می روند؟ (گزینه ها را از راست به چپ بخوانید)

۱. message ،model
۲. multipart/alternative ،model
۳. message ،application
۴. multipart/digest ،application

۱۲- کدام گزینه صحیح است؟

۱. POP۳ امکان دسته بندی و نمایش پیام های رسیده را در سرویس دهنده فراهم می کند.
۲. در IMAP هدف کاستن از بار سرویس دهنده است.
۳. POP۳ پیام ها را برای همیشه در سرویس دهنده نگه می دارد.
۴. IMAP امکان مدیریت پیام ها بر روی سرویس دهنده را فراهم می کند.

۱۳- کدام پروتکل ارتباطی با آوردن و نمایش صفحات وب ندارد اما به کاربر اجازه می دهد تا از داخل مرورگر ایمیل بفرستد؟

۱. sip
۲. mailto
۳. rtsp
۴. ftp

۱۴- کدام گزینه در رابطه با پروتکل های تلفن اینترنتی (VOIP) صحیح است؟

۱. H.323 از انعطاف پذیری بیشتری نسبت به SIP برخوردار است.
۲. معماری H.323 ماژولار است در حالی که SIP از معماری یکپارچه ای برخوردار است.
۳. SIP از پشته پروتکلی کامل تری نسبت به H.323 برخوردار است.
۴. نقطه ضعف SIP مشکلات ناشی از ناسازگاری های بین سیستمی است.

۱۵- در شبکه های تحویل محتوا (CDN) کدام یک از تکنیک های زیر برای توزیع محتویات وب مستقل از تصمیم و انتخاب کاربران عمل می کند؟

۱. رهیافت آینه ای کردن
۲. رهیافت هدایت DNS
۳. رهیافت مزرعه سرویس دهنده
۴. رهیافت درخت توزیع با پروکسی وب

تعداد سوالات : تستی : ۲۵ **تشریحی :** ۵ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۶۰ | **سری سوال :** ۱ یک

عنـــوان درس: شبکه های کامپیوتری ۲

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)،مهندسی فناوری اطلاعات(سیستمهای چند رسانه ای)۱۱۱۵۱۵۲

۱۶- در روش جدول درهم توزیع شده (DHT) یک گره برای ایجاد یک دسته جدید باید یک زوج کلید-مقدار به صورت (torrent, my-IP-address) را در نمایه درج نماید. کدام گزینه نشان دهنده نحوه محاسبه مقدار my-IP-address است؟

۱. hash(torrent)
۲. hash(successor(torrent))
۳. successor (hash (torrent))
۴. predecessor(hash (torrent))

۱۷- در روش رمزگذاری DES سه گانه کدام حالت رمزنگاری/ رمزگشائی امکان برقراری ارتباط با ماشین های DES معمولی را با انتخاب $k_1=k_2$ فراهم می کند(E به معنای رمزنگاری و D به معنای رمزگشائی است)؟

۱. حالت EEE
۲. حالت EDE
۳. حالت DDE
۴. حالت DED

۱۸- در حالت رمزنگاری کتابچه کد الکترونیک (ECB) کدام مشکل امکان حمله را برای مهاجم فراهم می نماید؟

۱. تقسیم نمودن پیام به بلوک های با طول یکسان
۲. عدم رمزنگاری بلوک ها به طور مستقل
۳. امکان جابه جائی دو بلوک داده با اندازه یکسان و مقادیر هم نوع
۴. امکان استفاده مجدد از یک بردار آماده سازی (IV)

۱۹- توضیح زیر کدام یک از تکنیک های تحلیل رمزهای بلوکی را توصیف می کند؟
((در این روش با یک زوج بلوک فاش نوشته که فقط در تعداد کمی بیت اختلاف دارند آغاز کرده و در هر دور تکرار داخلی فرایند رمزگذاری بررسی می شود.))

۱. تحلیل رمز تفاضلی
۲. تحلیل رمز خطی
۳. تحلیل زمانی رمز
۴. تحلیل ترافیکی رمز

۲۰- با استفاده از حمله روز تولد (birthday attack) تعداد عملیات موردنیاز برای شکستن یک خلاصه پیام به طول ۱۲۸ بیت کدام است؟

۱. ۲۱۲۸
۲. ۲۶۴
۳. ۲۳۲
۴. ۲۱۲۷

۲۱- کدام گزینه در رابطه با پروتکل IPsec در حالت های انتقال و تونل صحیح است؟

۱. عیب اصلی حالت انتقال افزودن یک سرآیند اضافی به بسته است.
۲. در حالت تونل کل بسته داخل یک بسته IP جدید با سرآیند مشابه بسته اولیه قرار می گیرد.
۳. حالت انتقال می تواند از تحلیل ترافیک ارسالی جلوگیری نماید.
۴. حالت های انتقال و تونل هر دو می توانند برای حفظ محرمانگی بسته های IP استفاده شوند.

تعداد سوالات : تستی : ۲۵ **تشریحی :** ۵ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۶۰ | **سری سوال :** ۱ یک

عنـــوان درس: شبکه های کامپیوتری ۲

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)،مهندسی فناوری اطلاعات(سیستمهای چند رسانه ای)۱۱۱۵۱۵۲

۲۲- کدام گزینه در رابطه با امنیت شبکه های بی سیم صحیح است؟

۱. یک شبکه بی سیم را می توان با استفاده VPN یا دیوار آتش به طور قابل قبولی امن نمود.

۲. در پروتکل WPA2 استفاده از گذرواژه مشترک بین ماشین ها به جای سرور احراز هویت مجزا امنیت کمتری دارد.

۳. در 802.11i پروتکل TKIP نسبت به پروتکل CCMP امنیت بیشتری را فراهم می کند.

۴. در WPA2 با روش گذرواژه مشترک بین ماشین ها از کلید اصلی برای رمزنگاری بسته ها استفاده می شود.

۲۳- حمله مرد- در- وسط (man-in-the-middle) از مشکلات اساسی کدام روش محسوب می گردد؟

۱. پروتکل احراز هویت کربروز
۲. الگوریتم RSA
۳. مبادله کلید دیفی هلمن
۴. احراز هویت نیدهام-شرودر

۲۴- برای مقابله با حمله بازپخش (replay attack) از کدام موارد زیر استفاده می شود؟

I: مهرزمانی (time stamp)
II: یک عدد یا رشته تصادفی موسوم به عجالتی (nonce)
III: پروتکل های احراز هویت چالش-پاسخ چند سویه
IV: توابع مخلوط سازی

۱. I و II
۲. I و II و III
۳. III و IV
۴. II و III و IV

۲۵- کدام یک از موارد زیر در رابطه با لایه سوکت امن (SSL) صحیح است؟

مورد اول: SSL یک لایه جدید بین لایه های شبکه و انتقال است.
مورد دوم: SSL تنها از الگوریتم رمزنگاری ۳DES پشتیبانی می کند.
مورد سوم: مهمترین وظیفه SSL پس از برقراری اتصال فشرده سازی و رمزنگاری است.
مورد چهارم: TLS با وجود تغییرات کم نسبت به SSL به کلی با آن ناسازگار است.

۱. موارد اول و سوم
۲. موارد دوم و چهارم
۳. موارد اول و دوم
۴. موارد سوم و چهارم

سوالات تشریحی

۱- هر یک از مفاهیم زیر را به اختصار توضیح دهید؟ **۱،۴۰ نمره**

الف. مالتی پلکس معکوس
ب.مهر زمان
ج. افزونه (Plug-in)
د. نویز کوانتش (quantization noise)

تعداد سوالات : تستی : ۲۵ **تشریحی :** ۵ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۶۰ | **سری سوال :** ۱ یک

عنـــوان درس: شبکه های کامپیوتری ۲

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)،مهندسی فناوری اطلاعات(سیستمهای چند رسانه ای)۱۱۱۵۱۵۲

۲- در پروتکل TCP Reno روش کنترل ازدحام با الگوی دندان اره ای برای تنظیم پنجره ازدحام را شرح دهید. ۱،۴۰ نمره

۳- الف. از مزرعه سرویس دهنده (server farm) به چه منظور استفاده می شود؟ ۱،۴۰ نمره
ب. در روش مزرعه سرویس دهنده باید کاری کنم که کامپیوترهای مزرعه سرویس دهنده از دید مشتری یک کامپیوتر واحد جلوه کند. روش های پیاده سازی این موضوع را به اختصار شرح دهید .

۴- از میان حالت های رمزگذاری، حالت زنجیرسازی بلوک رمز (CBC) را با رسم شکل توضیح دهید. ۱،۴۰ نمره

۵- مشکل به کارگیری رمزنگاری با کلید متقارن برای امضای دیجیتال را به اختصار شرح دهید . ۱،۴۰ نمره