تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۱- تعریف زیر مربوط به کدامیک از شش دسته عمده سرویسهای امنیتی محسوب می شود؟
"اطمینان از اینکه پیام مورد نظر از طرف فرستنده است."

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

۲- در کدامیک از سیستمهای رمز زیر، متن به قطعات یک بیتی یا یک بایتی تقسیم می شود و کلید یک رشته تصادفی هم طول با متن است؟

۱. رمز چند حرفی ۲. رمز ورنام ۳. رمز هیل ۴. رمز پلی فر

۳- در کدام روش رمز گذاری به صورت زیر عمل می شود؟
متن اصلی: MEETMEAFTERTHETOGAPARTY
کلید: M E M A T R H T G P R Y
E T E F E T E A A A T
متن رمز شده: MEMATRHTGPRYETEFETEOAAT

۱. رمز سزار ۲. کلید یک بار مصرف ۳. جایگشت ۴. ماشین روتور

۴- کدامیک از روشهای زیر از ساختار فیستل استفاده می کند و ۱۶ مرحله دارد؟

۱. الگوریتم RC۲ ۲. الگوریتم BLOWFISH
۳. الگوریتم CAST ۴. الگوریتم IDEA

۵- کدامیک از موارد زیر جزو خواص الگوریتم RC۵ محسوب می شود؟

۱. سرعت بالا, اندازه کم حافظه مورد نیاز, تعداد مراحل متفاوت
۲. سرعت بالا, فشردگی, تعداد مراحل متفاوت
۳. سرعت بالا, اندازه کم حافظه مورد نیاز, فشردگی
۴. فشردگی, اندازه کم حافظه مورد نیاز, تعداد مراحل متفاوت

۶- در کدامیک از روشهای زیر هر قطعه قبل از رمز شدن با خروجی قطعه قبلی XOR می شود؟

۱. روش پسخور رمز CFB ۲. روش دفترچه الکترونیکی FCB
۳. روش پسخور خروجی OFB ۴. روش رمز زنجیره قطعات رمز CBC

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۷- کدام یک از موارد زیر جزو نقاط ضعف روش رمز گذاری پیوند می باشد؟

۱. در هر سوئیچ پیام باز می شود ولی دوباره رمز نمی شود.
۲. به اجبار همه پیامها رمز می شوند.
۳. کاربران در مورد امنیت اعمال شده دارای اختیار است.
۴. پیام توسط کلید خصوصی فرستند رمز می شود.

۸- یکی از قویترین روشها که در آن اعداد اول متمایز p و q طوری انتخاب می شوند که در رابطه $(p \bmod 4) = (q \bmod 4) = 3$ صدق کنند، کدام گزینه می باشد؟

۱. روش Blum Blum shub
۲. روش رمز گذاری چرخشی
۳. روش DES با پسخور خروجی
۴. روش ANSI x9.17

۹- شناسه، نام کاربر، کلید عمومی، تاریخ ایجاد، تاریخ شروع فعالیت و تاریخ انقضاء جزو حداقل اطلاعات مورد نیاز کدامیک از روشهای توزیع کلید عمومی است؟

۱. مرجع مورد اعتماد
۲. اعلان
۳. گواهی
۴. فهرست

۱۰- در کدامیک از الگوریتمهای زیر بجای یک بافر (Line) از دو بافر (Lines) استفاده شده است و خروجی آن ۵ مقدار ۳۲ بیتی است؟

۱. الگوریتم HMAC
۲. الگوریتم MD۵
۳. الگوریتم SHA-۱
۴. الگوریتم RIPEMD-۱۶۰

۱۱- کدامیک از روشهای زیر جزو کلیدهای فیزیکی می باشد؟

۱. کارتهای هوشمند,کارتهای مغناطیسی, ماشین حسابهای خاص
۲. کارتهای هوشمند,کارتهای مغناطیسی, ,کلمه عبور
۳. کارتهای هوشمند, ماشین حسابهای خاص,کلمه عبور
۴. کارتهای مغناطیسی, ماشین حسابهای خاص,کلمه عبور

۱۲- کدامیک از موارد زیر از ملزومات کربروس محسوب می شود؟

۱. امن, مقیاس پذیر, غیر شفاف
۲. امن, غیر شفاف, مطمئن
۳. غیر شفاف, مقیاس پذیر, مطمئن
۴. امن, مقیاس پذیر, مطمئن

۱۳- کدامیک از موارد زیر جزو خصوصیات PKI (زیر ساخت کلید عمومی) می باشد؟

۱. عمل تعیین اعتبار
۲. محرمانگی
۳. انکار
۴. تولید گواهی

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۱۴- کدامیک از روشهای توزیع کلید عمومی زیر از بقیه بهتر است و در آن اصالت کلید در موقع دریافت کلید عمومی قابل احراز است و از ایجاد ترافیک در گره های خاص جلوگیری می شود؟

۱. ذخیره در یک گره و دریافت آن با احراز اصالت
۲. استفاده از گواهی
۳. ذخیره در دفترچه تلفن
۴. ارسال مستقیم توسط کاربر

۱۵- در بین چهار روش اصلی برای حفاظت کلید خصوصی کاربر، کدام روش کمترین ضعف را دارد و به عنوان روش برتر انتخاب شده است؟

۱. ذخیره در کارتهای حافظه دار
۲. ذخیره در دستگاههای کاملاً غیرقابل نفوذ
۳. رمز کردن کلید توسط کلمه عبور
۴. ذخیره در کارتهای هوشمند

۱۶- توصیف زیر مربوط به کدام یک از پنج سرویس اصلی PGP می باشد؟
"با استفاده از SHA-۱ چکیده ای از پیام ایجاد می شود، سپس این چکیده با استفاده از کلید خصوصی فرستنده توسط RSA یا DSS رمز می شود و چکیده همراه پیام ارسالی می شود."

۱. فشرده سازی
۲. تقسیم و ترکیب
۳. امضای دیجیتال
۴. محرمانگی پیام (احراز اصالت)

۱۷- مشکل اساسی کدامیک از روشهای ارسال کلید عمومی در PGP با خاصیت احراز اصالت، غیر عملی بودن آن در شبکه است؟

۱. کلید به صورت گواهی تایید شده توسط مرجع قابل اعتماد ارسال شود.
۲. انتقال به صورت فیزیکی
۳. انتقال به صورت الکترونیکی و تایید توسط تلفن و غیره
۴. انتقال توسط فرد مطمئنی که کلید عمومی وی در اختیار است.

۱۸- توصیف زیر مربوط به کدامیک از پنج کلمه کلیدی جدید در MIME می باشد که به سرآیه اضافه می شود؟
"مقدار ۱,۰ را دارد و به این معنی است که مطابق استاندارد RFC ۲۰۴۵ و RFC ۲۰۴۶ می باشد"

۱. نوع محتوا
۲. نوع کدگذاری روی محتوا
۳. شناسه محتوا
۴. نسخه پروتکل MIME

۱۹- در انواع کدگذاری در محتوای MIME توصیف زیر مربوط به کدام گزینه زیر می باشد؟
"داده تماماً با خط های کوتاه کاراکترهای اسکی نشان داده می شود."

۱. ۵bit
۲. Base64
۳. ۷bit
۴. x-token

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۲۰- کدام مورد از هفت گروه استاندارد RFC ۲۴۱۱، شامل مباحث عمومی، ملزومات امنیتی، تعاریف و روشهایی برای تعریف فناوری IPsec می شود؟

۱. الگوریتم رمزگذاری
۲. سرآیه احراز اصالت AH
۳. معماری
۴. الگوریتم احراز اصالت

۲۱- کدامیک از موارد زیر در زمره پارامترهایی که SA توسط آنها شناخته می شود، می باشد؟

۱. بازه زمانی SA, شمارنده دنباله عددی, واحد انتقال حداقل مسیر (MTU)
۲. سرریز شمارنده دنباله, بازه زمانی SA, شمارنده دنباله عددی
۳. سرریز شمارنده دنباله, بازه عددی, واحد انتقال حداقل مسیر (MTU)
۴. سرریز شمارنده دنباله, بازه زمانی SA, عددی, واحد انتقال حداقل مسیر (MTU)

۲۲- تعریف زیر مربوط به کدامیک از اجزاء سرآیه احراز اصالت (AH) می باشد؟
"میدان ۱۶ بیتی است که برای مقاصدی در آینده در نظر گرفته شده است."

۱. رزرو شده
۲. شماره دنباله
۳. سرآیه بعدی
۴. طول بدنه

۲۳- کدامیک از موارد زیر جزو پنج ویژگی مهم پروتکل Oakley می باشد؟

۱. با استفاده از اعداد تصادفی جلوی حمله تکرار گرفته شده است.
۲. در آن امکان حمله ملاقات در وسط وجود دارد.
۳. امکان تبادل مقادیر کلید خصوصی دیفی- هلمن را فراهم می کند.
۴. با استفاده از عدد تصادفی جلوی حمله پا بند گرفته شده است.

۲۴- کدام گزینه زیر یک پروتکل رمز نگاری کلید عمومی است که اجازه می دهد دو کاربر بر روی یک کانال ارتباطی نا امن، یک ارتباط امن مشترک را فراهم کنند؟

۱. MD۵ (نوع HMAC)
۲. DES
۳. SHA (نوع HMAC)
۴. دیفی- هلمن

۲۵- در کدام نوع تبادل پیام در ISAKMP امکان تبادل کلید همزمان را با احراز اصالت چیزهای دیگری که باید منتقل شوند فراهم می آورد؟

۱. تبادل حفاظت شناسه
۲. تبادل اطلاعاتی
۳. تبادل پایه
۴. تبادل تهاجمی

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۲۶- در کدام یک از پروتکلهای زیر محرمانگی توسط الگوریتم رمز متقارن و احراز اصالت توسط MAC فراهم می شود؟

۱. پروتکل تغییر مشخصات رمز در SSL
۲. پروتکل هشدار در SSL
۳. پروتکل دست دادن در SSL
۴. پروتکل رکورد در SSL

۲۷- در کدامیک از روشهای ایجاد کنترل دسترسی محتاطانه، اجازه دسترسی هر کاربر به اشیاء به طور مستقل است؟

۱. روش مبتنی بر تواناییها
۲. روش لیست کنترل دسترسی
۳. روش کلمه عبور فایل
۴. روش جدول حفاظت

۲۸- کدامیک از مدلهای زیر از بهترین مدلهای امنیتی بوده و به صورت مدل ماشین با حالت متناهی می باشد؟

۱. مدل Clark-Wilson
۲. مدل Goguen-Meseguer
۳. مدل BLP
۴. مدل Biba

۲۹- در بین نقاط ضعف در بانکهای اطلاعاتی مفهوم زیر مربوط به کدام گزینه می شود؟
"فرآیند ترکیب اشیاء چند بانک اطلاعاتی و به وجود آمدن یک شی است که از لحاظ امنیتی در سطح بالاتری از اشیاء به وجود آورنده اش قرار دارد (بدون تغییر در بانک اطلاعاتی)"

۱. اجتماع
۲. تمامیت داده ها
۳. اسبهای تروا
۴. استنتاج

۳۰- برای کنترل و به حداقل رساندن مجموعه اقداماتی می بایست انجام داد، کدامیک از گزینه های زیر جزو موارد مربوط به کنترل و به حداقل رساندن خرابی می باشد؟

۱. مشمول کردن نفوذگر و نظارت وی, گرفتن فایل پشتیبان از داده های سیستم؛ ترمیم فایلهای مخدوش شده
۲. درخواست اطلاعات بیشتر برای تعیین احراز اصالت, گرفتن فایل پشتیبان از داده های سیستم, مشمول کردن نفوذگر و نظارت وی
۳. درخواست اطلاعات بیشتر برای تعیین احراز اصالت, مشمول کردن نفوذگر و نظارت وی, ترمیم فایلهای مخدوش شده
۴. درخواست اطلاعات بیشتر برای تعیین احراز اصالت, حذف نفوذگر از سیستم, ترمیم فایلهای مخدوش شده

مباحث نو در فناوری اطلاعات ترم تابستان ۹۱	
1	الف
2	ب
3	ج
4	ج
5	الف
6	د
7	ب
8	الف
9	ج
10	د
11	الف
12	د
13	ب
14	ب
15	د
16	ج
17	ب
18	د
19	ج
20	ج
21	ب
22	الف
23	الف
24	د
25	ج
26	د
27	الف
28	ج
29	الف
30	ب