**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- کدام یک از گزینه های زیر از وجوه تمایز و نشان دهنده تفاوت بین اطلاعات فیزیکی و الکترونیکی است؟**

۱. محرمانگی ۲. تعیین اصالت نسخه ۳. دسترس پذیری ۴. آسیب پذیری

**۲- با توجه به جدول زیر و رمز پلی فر: بجای rs ، yt (از راست به چپ) چه حروفی قرار می گیرد؟**
"yourself" **به عنوان کلید انتخاب شده است.**

| | | | | |
|---|---|---|---|---|
| Y | O | U | R | S |
| E | L | F | A | B |
| C | D | G | H | I/J |
| K | M | N | P | Q |
| T | V | W | X | Z |

۱. sy ، ei ۲. ru ، ol ۳. el ، ov ۴. se ، to

**۳- کدام یک از سیستم های رمز گذاری از نوع امنیت بدون شرط است؟**

۱. سیستم رمز با کلید فیزیکی ۲. سیستم رمز با کلید بیولوژیکی
۳. سیستم رمز با کلید یکبار مصرف ۴. سیستم رمز با کلید اطلاعاتی

**۴- در سیستم رمز ورنام از کدام رابطه برای رمز گشایی و رمز گذاری قطعات استفاده می شود؟**

۱. $C_i= p_i \text{ xor } k_i$ , $P_i= c_i \text{ xor } k_i$ ۲. $C_i= p_i \text{ xnor } k_i$ , $p_i= c_i \text{ xnor } k_i$
۳. $C_i= p_i \text{ xor } k_i$ , $p_i= c_i \text{ xnor } k_i$ ۴. $c_i= p_i \text{ xnor } k_i$ , $p_i= c_i \text{ xor } k_i$

**۵- طول کلید الگوریتم IDEA چند بیتی است؟**

۱. ۱۶ بیتی ۲. ۳۲ بیتی ۳. ۵۶ بیتی ۴. ۱۲۸ بیتی

**۶- در الگوریتم RC5 قبل از انجام رمز گذاری یا رمز گشایی چه عملی انجام می شود؟**

۱. ابتدا از کلید اصلی، t زیر کلید ساخته می شود. ۲. ابتدا قطعه متن دریافتی با خروجی تابع، XOR می شود.
۳. ابتدا متن را به قطعاتی با طول ثابت تقسیم می کند. ۴. ابتدا آرایه ورودی in در آرایه حالت قرار می گیرد.

**۷- برای تبدیل رمز قطعه ای به رمز دنباله ای از کدام روش الگوریتم های رمز قطعه ای استفاده می شود؟**

۱. روش دفترچه الکترونیکی ۲. روش رمز زنجیره قطعات
۳. روش پسخور رمز ۴. روش پسخور خروجی

**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

**۸- رمز گذاری پیوند در کدام لایه انجام می شود؟**

۱. شبکه یا کاربرد
۲. فیزیکی یا کاربرد
۳. شبکه یا پیوند داده ها
۴. فیزیکی یا پیوند داده ها

**۹- در کدام یک از روشهای تولید اعداد تصادفی، از یک شمارنده رمز شده استفاده می شود و امنیت خروجی بعدی به امنیت الگوریتم رمز بستگی دارد؟**

۱. رمز گذاری چرخشی
۲. روش DES با پسخور خروجی
۳. روش ANSIX9.17
۴. روش BBS

**۱۰- کلید عمومی توسط کدام یک از روشهای زیر می تواند توزیع شود؟**

۱. متقارن- نقطه ای
۲. نا متقارن - متقارن
۳. فهرست- مرجع مورد اعتماد
۴. نقطه ای- مرجع صدور فهرست

**۱۱- برای جلوگیری از حمله زمانی از کدام روش زیر می توان استفاده نمود؟**

۱. الگوریتم تجزیه اعداد تصادفی.
۲. زمان یکسان برای به توان رساندن، یعنی برای همه حالتها زمان محاسبه یکسان باشد.
۳. حدس زدن بیت های کلید بر اساس زمان مصرفی برای عملیات منطقی.
۴. قبل از به توان رساندن، متن رمز شده آن با یک عدد تصادفی جمع شود.

**۱۲- کدام یک از کلیدهای زیر، ویژگی های یکتایی و همیشه در اختیار کاربر بودن را دارا است؟**

۱. کلید های بیولوژیکی
۲. کلید های فیزیکی
۳. کلید های اطلاعاتی
۴. کلید های محاسباتی

**۱۳- در کدام الگوریتم زیر حداکثر اندازه پیام بینهایت (∞) می باشد؟**

۱. CBC
۲. RIPEMD-160
۳. SHA-1
۴. MD5

**۱۴- در امضاء دیجیتال برای ایجاد محرمانگی از کدام یک از عملیات زیر استفاده می شود؟**

۱. پیام و امضاء را با کلید عمومی گیرنده رمز کرد.
۲. از توابع فردی استفاده کرد.
۳. ایجاد یک زوج کلید برای پیام.
۴. بکار بردن یک شمارنده.

**۱۵- برای جلوگیری از حمله تکرار به شبکه ها از کدام یک از روش های زیر استفاده می شود؟**

۱. شماره سریال- مهر زمانی
۲. کلید عمومی- پرسشنامه
۳. رمز عبور- کنترل نرم افزاری
۴. عدد غیر تصادفی- کنترل سخت افزاری

**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

**۱۶- کدام یک از گزینه های زیر جزء معیارهای امنیتی خارجی محسوب می شود؟**

۱. امنیت سخت افزار ۲. امنیت پرسنل ۳. امنیت سیستم عامل ۴. امنیت نرم افزاری

**۱۷- کدام یک از گزینه های زیر از مشکلات فنی نسخه ۴ کربروس محسوب می شود که همچنان در نسخه ۵ آن نیز وجود دارد؟**

۱. وابستگی به پروتکل (IP) اینترنت

۲. تعیین ترتیب بایت پیام توسط خود کربروس

۳. استفاده از نقطه شروع و پایان به جای زمان اعتبار

۴. چون کلید از کلمه عبور کاربر استخراج می شود، بنابراین با حدس کلمه عبور تمام ارتباطات نا امن خواهند شد.

**۱۸- کدام گزینه زیر از راه های اصلی برای حفاظت کلید خصوصی کاربر بشمار می رود؟**

۱. تولید کلید توسط صادر کننده گواهی ۲. ذخیره در کارتهای هوشمند

۳. ذخیره در یک گره ۴. تولید کلید توسط خود کاربر

**۱۹- کدام یک از سرویس های زیر، سرویس های محرمانگی و احراز اصالت را برای پست الکترونیکی دربر دارد؟**

۱. سرویسPGP ۲. سرویس TGS ۳. سرویس ESP ۴. سرویس TGT

**۲۰- پروتکل** oakley **چیست؟**

۱. یک نوع پروتکل تعیین احراز اصالت ۲. یک نوع پروتکل ایجاد امنیت

۳. یک نوع پروتکل تبادل کلید ۴. یک نوع پروتکل تبادل پیام

**۲۱- در کدام یک از حالت های** AH**، برای احراز اصالت، رایانه کاربر اصالت خود را به دیواره آتش اثبات می کند؟**

۱. حالت تونل ۲. حالت مستقیم ۳. حالت انتقال ۴. حالت دسترسی مجاز

**۲۲- کدام یک از پروتکل های** SSL**، تنها یک بایت با مقدار ۱ دارد؟**

۱. پروتکل رکورد ۲. پروتکل تغییر مشخصات رمز

۳. پروتکل هشدار ۴. پروتکل دست دادن

**۲۳- حداکثر اندازه کوکی چه مقدار است و در آن چه اطلاعاتی وجود دارد؟**

۱. ۱KB- اطلاعات رمز شده ۲. ۲KB- اطلاعات کاربری

۳. ۳KB- اطلاعات رمز شده ۴. ۴KB- اطلاعات کاربری

**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

**۲۴- کدام یک از استانداردهای SNMP توصیف کننده چگونگی تعریف مدیریت در MIB است؟**

۱. استاندارد RFC1155
۲. استاندارد RFC1213
۳. استاندارد RFC1157
۴. استانداردRFC1215

**۲۵- حذف اجازه دسترسی توسط کاربر یا سیستم، از معایب کدام روش ایجاد کنترل دسترسی محتاطانه می باشد؟**

۱. روش مبتنی بر توانایی ها
۲. روش لیست کنترل دسترسی
۳. روش بیت های حفاظتی
۴. روش جدول حفاظت

**۲۶- به فعالیت های مخفیانه ای که یک برنامه ممکن است انجام دهد و این فعالیت ها از ظاهر برنامه استنباط نمی شود، چه می گویند؟**

۱. ویروس
۲. نفوذ
۳. اسب تراوا
۴. نقاب زدن

**۲۷- کدام یک از گزینه های زیر از اجزاء تشکیل دهنده سیستم تشخیص نفوذگر توزیع شده (DIDS) محسوب می شود؟**

۱. Host Monitored، DIDS Director، LAN Monitor
۲. NSM، NADIR، CSM
۳. UDP، IP
۴. SNMP، RFC، PDU

**۲۸- دو عمل اصلی در ارزیابی خرابی عبارتند از:**

۱. نظارت بر حمله - رفع خرابی
۲. بازیابی حمله - جلوگیری از خرابی
۳. جلوگیری از حمله - کنترل خرابی
۴. خنثی کردن حمله - ترمیم خرابی

**۲۹- دیوار آتش برای جلوگیری از کدام حمله بیشتر به کار گرفته می شود؟**

۱. نقاب زدن
۲. ویروسها
۳. اسب تراوا
۴. کرم ها

**۳۰- در کدام مدل برای جلوگیری از خرابی در سیستم به واسطه تغییر داده ها توسط افراد مجاز و یا غیر مجاز از دو روش "تراکنش خوش ترکیب" و "جداسازی وظایف" استفاده می شود؟**

۱. BLP
۲. Biba
۳. Orange Book
۴. Clark-Wilson