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

درس : مباحث نودرفناوری اطلاعات

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

۱- حمله به محرمانگی و کنترل دسترسی اطلاعات چه نام دارد و جزء کدام یک از انواع حملات می باشد؟

۱. دستبرد- غیر فعال ۲. دستبرد- فعال ۳. جعل- غیر فعال ۴. جعل- فعال

۲- اگر هزینه شکستن متن رمز شده از ارزش خود پیام بیشتر باشد؛ آن را چه می نامیم؟

۱. رمز گذاری ۲. رمز گشایی ۳. امنیت محاسباتی ۴. امنیت بدون شرط

۳- کدام گزینه از خواص الگوریتم BLOWFISH نمی‌باشد؟

۱. جمع در پیمانه دو به توان شانزده. ۲. ساختاری ساده برای پیاده سازی.

۳. به ۵کیلو بایت حافظه نیاز دارد. ۴. طول کلید متغیر است.

۴- این الگوریتم خواص انتشار و اغتشاش قوی دارد و طول کلید آن ۱۲۸ بیتی است؟

۱. IDEA ۲. DES ۳. CAST ۴. RC5

۵- کدام یک از موارد زیر جزء نقاط ضعف رمز گذاری انتها به انتها است؟

۱. کاربران هیچ اختیاری در مورد امنیت اعمال شده ندارند. ۲. نیاز به یک کلید متقارن دارد.

۳. اطلاعات مربوط به بسته را نمی توان رمز کرد. ۴. در لایه فیزیکی انجام می شود.

۶- به منظور تبدیل رمز قطعه ای به رمز دنباله ای از این روش استفاده می شود؟

۱. روش رمز زنجیره قطعات رمز ۲. روش دفترچه الکترونیکی

۳. روش پسخور خروجی ۴. روش پسخور رمز

۷- درکدام روش کدام از رمز گذاری: پیام اصلی به همراه آدرس گیرنده و فرستنده رمز می شود؟

۱. رمز گذاری نامتقارن ۲. رمزگذاری پیوند

۳. رمز گذاری انتها به انتها ۴. تمامی روش‌های رمز گذاری متقارن

۸- " امکان حمله ملاقات در وسط " جزء مشکلات اساسی کدامیک از موارد زیر است؟

۱. توزیع کلید دیفی- هلمن ۲. توزیع کلید عمومی

۳. توزیع کلید متقارن ۴. توزیع کلیدECC

۹- پایه و اساس الگوریتمهای کلید عمومی (PkI) چیست؟

۱. توابع و مسائل ریاضی ۲. جایگشتها ۳. جانشینی ها ۴. انتگرالها

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

درس : مباحث نودرفناوری اطلاعات

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

۱۰- کدام الگوریتم زیر از رنج مقدار ۳۲ بیتی(خروجی ۱۶۰ بیتی) استفاده نمی‌کند؟

۱. الگوریتم در هم ساز امن (SHA)
۲. الگوریتم MD5
۳. الگوریتم MD4
۴. الگوریتم RIPEMD- 160

۱۱- برای افزایش امنیت در توابع درهم ساز از کدام مورد زیر استفاده می شود؟

الف)برای پیام سرآیه قرار می‌دهیم.

ب)برای پیام پانویس قرار می‌دهیم.

ج)در قطعه آخر از پیام، طول پیام را ذخیره می‌کنیم.

۱. فقط موارد الف و ج
۲. موارد الف ، ب و ج
۳. فقط موارد الف و ب
۴. فقط موارد ج

۱۲- در ایجاد محرمانگی؛ برای امضای دیجیتال می توان پیام و امضاء را با..... رمز کرد.

۱. کلید خصوصی گیرنده
۲. کلید عمومی گیرنده
۳. کلید خصوصی فرستنده
۴. کلید عمومی فرستنده

۱۳- برای جلوگیری از تشخیص حجم اطلاعات مبادله شده؛ همیشه پیام را می توان با..... فرستاد که در نتیجه قسمت اعظم پیام ها ..... هستند.

۱. نرخ متغیر- غیر واقعی
۲. نرخ متغیر- واقعی
۳. نرخ ثابت- غیر واقعی
۴. نرخ ثابت- واقعی

۱۴- کدام گزینه در مورد سیستم احراز هویت کربروس صحیح نیست؟

۱. یک سیستم احراز اصالت است.
۲. در کربروس کاربر اصالت خود را به سرور اثبات می کند.
۳. در کربروس سرور اصالت خود را به کاربر اثبات می کند.
۴. کربروس مبتنی بر الگوریتمهای رمز نا متقارن است.

۱۵- فشرده سازی بر روی پیام ..... و..... انجام می شود.

۱. بعد از امضاء و قبل از رمز گذاری
۲. قبل از امضاء و بعد از رمز گذاری
۳. بعد از امضاء و بعد از رمز گذاری
۴. قبل از امضاء و قبل از رمز گذاری

۱۶- کدام مورد از سرویس هایی است که PGP ارائه می کند؟

۱. تقسیم و ترکیب
۲. احراز اصالت مبدأ داده
۳. کنترل دسترسی
۴. تمامیت بدون اتصال

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

درس : مباحث نودرفناوری اطلاعات

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

۱۷- کدام گزینه صحیح نمی‌باشد؟

۱. IPSec یک سرویس احراز اصالت است.

۲. از پروتکل امنیتی محافظ(ESP) به منظور محرمانگی محتوای پیام استفاده می شود.

۳. در پروتکل تعیین کلید(Oakley) با استفاده از عدد تصادفی جلوی حمله پابند گرفته شده است.

۴. SHA یک الگوریتم درهم ساز است که برای احراز اصالت بسته داده ها استفاده می شود.

۱۸- عدم نمایش کاربر؛ در صورت مواجه شدن وب با کدام یک از خطرات زیر روی می دهد؟

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

۱۹- کدام یک از خصوصیات زیر مربوط به پروتکل دست دادن در SSL نمی‌باشد ؟

۱. پیچیده ترین پروتکلSSL است.

۲. به منظور احراز اصالت دو طرف و توافق روی الگوریتم‌ها و کلیدهای رمزگذاری است.

۳. مربوط به لایه دوم می باشد.

۴. از دو بایت تشکیل شده است(نوع خطا- کد خطا)

۲۰- آدرس های وبی که با https:// شروع می شوند توسط کدام پروتکل محافظت می شوند؟

۱. SSL ۲. SHTTP ۳. HTTP ۴. FTP

۲۱- در مرحله ۳ از پروتکل دست دادن؛ کدام رویداد زیر اتفاق می افتد؟

۱. پایان دست دادن ۲. برقراری قابلیتهای امنیتی

۳. احراز اصالت و تبادل کلید کار فرما ۴. احراز اصالت و تبادل کلید سرور

۲۲- توسط کدام دستور در SNMP؛ اطلاعات ناخواسته به مرکز مدیریت قابل ارسال است؟

۱. Trap ۲. get responce ۳. get request ۴. set request

۲۳- کدام گزینه در مورد سیستم دیدبانی امنیت شبکه(NSM) صحیح می باشد؟

۱. در این سیستم از رویداد نگاری برای تشخیص نفوذ استفاده می شود.

۲. فقط ارتباط بین سیستمها قابل نظارت است.

۳. براعمال کاربری که به طور مستقیم به سیستمی متصل شده است نظارت می کند.

۴. در این سیستم یک شناسه شبکه (NID) به هر کاربر داده می شود تا اگر کاربر از سیستمی به سیستم دیگر وارد شود قابل تشخیص باشد.

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

درس : مباحث نودرفناوری اطلاعات

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

۲۴- سیستمی که برای شبکه رایانه ای مجتمع(ICN) طراحی شده و رکورد های رویداد نگاری را از شبکه می گیرد چه نام دارد؟

۱. سیستمNADIR ۲. سیستمCSM ۳. سیستم NSM ۴. سیستمDIDS

۲۵- دو عمل اصلی در ارزیابی خرابی عبارتند از:

۱. رفع خرابی مربوط به یک حمله- شناسایی نقاط ضعف سیستم

۲. تعیین اجزاء سیستم- پیاده سازی سیستم امنیتی

۳. شناسایی خطرات تهدید کننده سیستم- جلوگیری از خرابی بیشتر سیستم

۴. بازیابی حمله- جلوگیری از خرابی

۲۶- دیوار آتش در شبکه‌ها برای جلوگیری از کدام حمله زیر استفاده می شود؟

۱. نقاب زدن ۲. وقفه ۳. تغییر ۴. دستبرد

۲۷- مدل امنیتی ..... برای سیستمهای تجاری مهم است؛ یعنی.....را در بر دارد؟

۱. BLP- محرمانگی داده ۲. Clark- Wilson - تمامیت داده

۳. Goguen- Maseguer- محرمانگی داده ۴. Biba- تمامیت داده

۲۸- الگوریتم رمز با کلید نا متقارن توسط کدام تابع ساخته می شود؟

۱. تابعRSA ۲. تابع یکطرفه دریچه مخفی

۳. تابع بازگشتی ۴. تایع HASH

۲۹- کلیدی که برای توزیع کلید در الگوریتم های متقارن استفاده می شود چه نام دارد؟

۱. کلید شناسه ۲. کلید عمومی ۳. کلید جلسه ۴. کلید کاربر

۳۰- خصوصیات زیر مربوط به کدام یک از الگوریتم های زیر می باشد؟

- حداکثر اندازه پیام: $۱ - ۲^{۶۴}$ **بیت**

- سرعت: ۱۳/۶

- طراحی شده برای ماشینهای: little- endian

- ثابتهای اضافی استفاده شده: ۹

۱. RIP EMD- 160 ۲. MD5 ۳. MD4 ۴. SHA-1