

تعداد سوالات: تستی: ۳۰ تشریحی: ۷
زمان آزمون (دقیقه): تستی: ۶۰ تشریحی: ۶۰

پیام نور
دانشجویان
خبرگزاری
PNUNA.COM
PNU News Agency



نام درس: مباحث نو در فناوری اطلاعات

رشته تحصیلی / کد درس: فناوری اطلاعات (ستتی - تجمیع)

مجاز است.

استفاده از:

کد سری سؤال: یک (۱)

امام خمینی^(ع): این محرم و صفر است که اسلام را زنده نگه داشته است.

۱. کدام یک از موارد زیر از اهداف امنیت رایانه می باشد؟
الف. محرمانگی ب. تمامیت ج. دسترس پذیری د. همه موارد
۲. از دلایلی که اخیراً به امنیت رایانه و شبکه ارتباطی بیشترین توجه می شود کدام است؟
الف. دسترس پذیری اطلاعات ب. محرمانگی اطلاعات
ج. افزایش جرم های رایانه ای د. گزینه الف و ب صحیح است.
۳. گزینه صحیح را مشخص کنید؟
الف. در رمزگزاری متقارن کلید رمزگزاری بین فرستنده و گیرنده مشترک است.
ب. در رمزگزاری نامتقارن کلید رمزگزاری بین فرستنده و گیرنده مشترک است.
ج. در رمزگشایی متقارن کلید رمزگزاری بین فرستنده و گیرنده مشترک است.
د. در رمزگشایی متقارن کلید رمزگزاری بین فرستنده و گیرنده مشترک است.
۴. امنیت سیستم به کدام یک از عوامل زیر وابسته است؟
الف. قدرت الگوریتم رمزگزاری ب. توابع جانشینی
ج. رمزگزاری د. رمزگشایی
۵. از معروفترین سیستم های رمز چندحرفی کدام است؟
الف. سیستم هیل ب. سیستم پلی فر ج. سیستم رمز رینجر د. همه موارد
۶. در کدام یک از روش های زیر، متن به قطعات یک بیتی یا یک بایتی تقسیم می شود؟
الف. انتقال یا جایگشت ب. رمز ورنام ج. ماشین روتور د. رمز تک حرفی
۷. کدام یک از موارد زیر جز خواص الگوریتم BLOWFISH است؟
الف. سریع ب. امنیت متغیر ج. سادگی د. همه موارد
۸. کدام یک از الگوریتم های زیر از ساختار فیستل استفاده می کند و ۱۶ مرحله دارد؟
الف. الگوریتم RCS ب. الگوریتم RC2 ج. الگوریتم IDEA د. الگوریتم CAST
۹. کدام یک از موارد زیر جزء خواص الگوریتم رمز قطعه ای متقارن نیست؟
الف. طول کلید متغیر است. ب. این الگوریتم سرعت زیادی دارد.
ج. میزان چرخش بافر به کلید وابسته است. د. SBOX وابسته به کلید است.
۱۰. از اهدافی که در رمزگزاری تعقیب می شود چیست؟
الف. دسترس پذیری پیام ب. سادگی پیام
ج. محرمانگی پیام د. همه موارد

تعداد سوالات: تستی: ۳۰ تشریحی: ۷
زمان آزمون (دقیقه): تستی: ۶۰ تشریحی: ۶۰

پیام نور
دانشجویان
خبرگزاری
PNUNA.COM
PNU News Agency



نام درس: مباحث نو در فناوری اطلاعات
رشته تحصیلی / کد درس: فناوری اطلاعات (ستتی - تجميع)

مجاز است.

استفاده از:

کد سری سؤال: یک (۱)

فهرست دروس دانشجویان پیام نور :: PNUNA.COM

۱۱. کدام یک از موارد زیر جزء نقاط ضعف رمزگزاری پیوند است؟
الف. در شبکه‌های بزرگ این روش به تعداد زیادی عملگر رمز نیاز دارد.
ب. نمی‌توان اطلاعات مربوط به بسته را رمز کرد.
ج. جابه‌جایی و انتقال کمی در متن رخ میدهد.
د. همه موارد.
۱۲. الگوریتم کلید عمومی مبتنی بر چیست؟
الف. توابع و مسائل ریاضی
ج. جانشینی
ب. جایگشت
د. گزینه ب و ج صحیح است
۱۳. کدام یک از موارد زیر از روش‌های اصلی برای احراز اصالت کاربران است؟
الف. کلیدهای فیزیکی
ب. کلیدهای اطلاعاتی
ج. کلیدهای بیولوژی
د. هر سه گزینه صحیح است.
۱۴. در کدام یک از موارد زیر از تابع درهم‌ساز SHA استفاده می‌شود؟
الف. احراز اصالت یک طرفه
ج. احراز اصالت دو طرفه
ب. رمزگزاری نامتقارن
د. DSS
۱۵. کدام یک از روش‌های کنترلی برای ایجاد امنیت است؟
الف. رمزگشایی
ب. احراز اصالت
ج. کنترل سخت‌افزاری
د. همه موارد
۱۶. کدام یک از موارد زیر از راه‌های اصلی برای حفاظت کلید خصوصی کاربر می‌باشد؟
الف. رمزکردن کلمه کلید توسط کلمه عبور
ب. ذخیره در کارتهای هوشمند
ج. ذخیره در کارتهای حافظه‌دار
د. همه موارد
۱۷. الگوریتم‌ها، کلیدها، IVها، و غیره را دربر دارد.
الف. ESP
ب. SA
ج. AH
د. IPSec
۱۸. کدام یک از موارد زیر یک پروتکل استاندارد مدیریت کلید محسوب می‌شود که با استاندارد IPSec استفاده می‌شود؟
الف. IP
ب. RSA
ج. SHA
د. IKE
۱۹. به منظور ارسال یک طرفه اطلاعات برای مدیریت SA است.
الف. تبادل به همراه فقط احراز اصالت
ب. تبادل تهاجمی
ج. تبادل اطلاعاتی
د. تبادل پایه
۲۰. کدام یک از موارد زیر جزء نواقص پروتکل SNMP است؟
الف. عدم پشتیبانی مدیریت شبکه توزیع شده
ب. نقص در عملکرد
ج. نقص در امنیت
د. همه موارد

تعداد سوالات: تستی: ۳۰ تشریحی: ۷
زمان آزمون (دقیقه): تستی: ۶۰ تشریحی: ۶۰

پیام نور
دانشجویان
خبرگزاری
PNUNA.COM
PNU News Agency



نام درس: مباحث نو در فناوری اطلاعات

رشته تحصیلی / کد درس: فناوری اطلاعات (ستتی - تجمیع)

مجاز است.

استفاده از:

کد سری سؤال: یک (۱)

۲۱. در کدام یک از روش‌های زیر اجازه دسترسی کاربران مربوط به یک شی به طور مستقل ذخیره می‌شود؟

الف. روش لیست کنترل دسترسی

ب. روش مبتنی بر تواناییها

ج. روش کلمه عبور فایل

د. روش بیت‌های حفاظتی

۲۲. کدامیک از گزاره‌های زیر، سیستم تشخیص نفوذ خلاف و استفاده ناصحیح مبتنی بر سیستم خبره است؟

الف. سیستم CSM

ب. سیستم NADIR

ج. سیستم NSM

د. سیستم IDES

۲۳. کدام یک از مدل‌های زیر مبتنی بر عدم دخالت بین کاربران است؟

الف. BLP

ب. Biba

ج. Clark-Wilson

د. Goguen-Meseguer

۲۴. دیوار آتش برای جلوگیری از کدام یک از حملات زیر است؟

الف. دسترسی غیرمجاز به منابع شبکه

ب. عدم سرویس‌دهی

ج. نقاب زدن

د. همه موارد

۲۵. برنامه‌ای که کار ناخواسته‌ای را در کنار عملی اصلی انجام می‌دهد چیست؟

الف. اسب تراوا

ب. دیوار آتش

ج. Bibo

د. UDP

۲۶. کدام مدل زیر برای سیستم‌های نظامی مهم است؟

الف. BLP

ب. Biba

ج. Clark-Wilson

د. Goguen-Meseguer

۲۷. کدام یک از موارد زیر جزء ویژگی‌های الگوریتم‌های درهم‌سازی نمونه است؟

الف. سرعت کم

ب. محدودیت صادرات

ج. مشکل حمله‌ی روز تولد

د. همه موارد

۲۸. در شبکه‌ای با N کاربر به چند کلید نیاز داریم؟

الف. N

ب. $\frac{N}{2}$

ج. $\frac{N(N-1)}{2}$

د. $\frac{N-1}{2}$

۲۹. طول کلید کدام الگوریتم زیر ۱۲۸ بیتی است و خواص انتشار و اغتشاش قوی‌ای دارد؟

الف. IDEA

ب. AES

ج. BLOWFISH

د. RC5

۳۰. کدام پروتکل زیر اجازه می‌دهد پیام رمز شود، امضاء گردد و یا ترکیبی از این دو انجام شود؟

الف. MIME

ب. MDS

ج. S/MIME

د. RC5

تعداد سوالات: تستی: ۳۰ تشریحی: ۷
زمان آزمون (دقیقه): تستی: ۶۰ تشریحی: ۶۰

پیام نور
دانشجویان
خبرگزاری
PNUNA.COM
PNU News Agency



نام درس: مباحث نو در فناوری اطلاعات
رشته تحصیلی / گد درس: فناوری اطلاعات (ستتی - تجميع)

مجاز است.

استفاده از:

گد سری سؤال: یک (۱)

سوالات تشریحی:

۱. هر کدام از موارد زیر را در یک جمله تعریف نمایید. (۱/۲۵ نمره)
 - الف. امنیت محاسباتی
 - ب. رمز پلی فر
 - ج. FEP
 - د. اصالت پیام
 - ه. کلید جلسه
۲. چهار تفاوت اطلاعات فیزیکی و الکترونیکی چیست؟ (۱ نمره)
۳. دو مورد از نقاط ضعف DES ساده شده را نام ببرید؟ (۰/۵ نمره)
۴. خاصیت بهمنی در DES را توضیح دهید؟ (۰/۵ نمره)
۵. مراحل تولید کلید در الگوریتم RSA را توضیح دهید؟ (۱ نمره)
۶. چهار مورد از ویژگی‌های امضای دیجیتالی را نام ببرید؟ (۱ نمره)
۷. سه استاندارد SNMP را نام برده و توضیح مختصری دهید؟ (۰/۷۵ نمره)