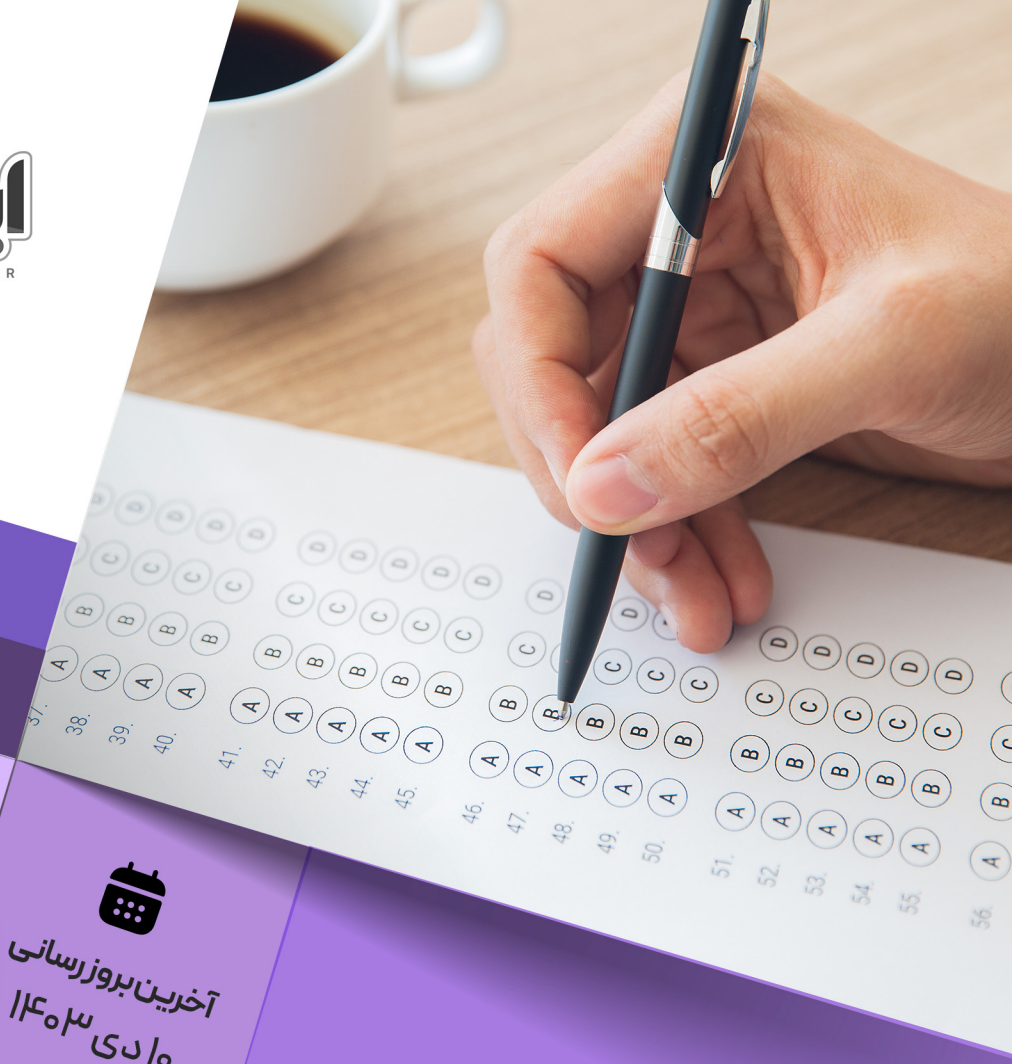

کد محصول
ES1201

آخرین بروزرسانی
۱۰ دی ۱۴۰۳

سوالات استخدامی

کارشناس فناوری اطلاعات
بیمه دانا

- مطابق با منابع اعلام شده آزمون استخدامی ۱۴۰۳
- نسخه رایگان شامل ۲۱ سوال (تعداد کمتر و تنها برخی دارای پاسخ)
- برای تهیه نسخه اصلی، با ۴۴۲ سوال به همراه پاسخنامه تستی و تشریحی، به سایت ایران عرضه مراجعه نمایید.

لینک های مفید آزمون استخدامی بانک مهر

خرید این محصول	خرید سوالات عمومی بیمه دانا
آشنایی با بیمه دانا	منابع عمومی آزمون
خرید درسنامه دروس عمومی استخدامی	خرید سوالات استخدامی ۱۰ سال اخیر
اخبار آزمون	

آخرین بروزرسانی ها:

۱۴۰۳/۱۰/۱۰ سوالات موجود آپدیت شد.

(برای مشاهده هر بخش روی آن بزنید)

فهرست مطالب

❖ فصل اول: سوالات امنیت شبکه تالیف ایران عرضه ۱۴۰۳

۱- کدام مورد از ویژگی های حملات امنیتی از نوع غیرفعال است؟ (iranarze.ir)

الف. بدست آوردن اطلاعات **ب. استفاده از اطلاعات**

ج. تغییر منابع سیستم **د. تاثیر بر عملیات سیستم**

۱) الف وب ۲) ب وج ۳) ج ود ۴) الف ود

☑ **پاسخ سایت ایران عرضه: گزینه ۱** ⇦ یک روش مناسب برای دسته بندی حملات امنیتی که هم در X.۸۰۰ و هم در ۲۸۲۸ RFC استفاده شده است. تقسیم این حملات به دو دسته حملات غیر فعال و حملات فعال میباشد. یک حمله غیر فعال تلاش دارد تا اطلاعات سیستم را به دست آورده و یا از آن استفاده کند، ولی روی منابع سیستم تاثیر نمی گذارد. یک حمله فعال سعی دارد تا منابع سیستم را تغییر داده و یا بر عملیات آن تأثیر بگذارد. (منبع ایران عرضه)

۲- در کدام یک از سرویس های امنیتی زیر به ترتیب مکانیسم رمزنگاری و مبادله اعتبار سنجی وجود دارد؟ (iranarze.ir)

۱) محرمانگی- صحت داده ها ۲) اعتبارسنجی منبع دیتا- قابلیت دسترسی

۳) عدم انکار- اعتبارسنجی واحد نظیر ۴) محرمانگی- کنترل دستیابی

☑ **پاسخ سایت ایران عرضه: گزینه ۲** ⇦ از سرویس های امنیتی، اعتبارسنجی دیتا دارای مکانیسم رمزنگاری است و سرویس قابلیت دسترسی دارای مکانیسم مبادله اعتبارسنجی است.

سرویس	مکانیسم								
	رمزنگاری	امضاء دیجیتال	کنترل دست‌یابی	صحت داده‌ها	مبادلهٔ اعتبارسنجی	لایه‌لائی ترافیک	کنترل مسیریابی	ثبت‌سند
اعتبارسنجی واحد نظیر	بلی	بلی			بلی			
اعتبارسنجی منبع دیتا	بلی	بلی						
کنترل دست‌یابی			بلی					
محرمانگی	بلی						بلی	
محرمانگی جریان ترافیک	بلی					بلی	بلی	
صحت داده‌ها	بلی	بلی		بلی				
عدم انکار		بلی		بلی				بلی
قابلیت دسترسی				بلی	بلی			

رابطه بین سرویس های امنیتی و مکانیسم های امنیتی

۳- چنانچه فرستنده و گیرنده از یک کلید متفاوت استفاده کنند، به سیستم رمزنگاری چه می گویند؟ (iranarze.ir)

۱) متقارن تک کلیدی ۲) متقارن کلید سّری

۳) متقارن کلید رسمی ۴) نامتقارن کلید عمومی

☑ **پاسخ سایت ایران عرضه: گزینه ٤** ⇦ سیستم های رمزنگاری معمولا از سه بعد مستقل دسته بندی می شود: نوع عملیات بکار گرفته شده برای تبدیل متن ساده به متن رمزشده - تعداد کلیدهای استفاده شده - نحوه پردازش متن ساده پیام

تعداد کلیدهای استفاده شده: (تالیف توسط سایت ایران عرضه) اگر هم فرستنده و هم گیرنده از یک کلید استفاده کنند. سیستم رمزنگاری را متقارن تک کلیدی کلید - سری و یا رسمی گویند. اگر فرستنده و گیرنده هر کدام از یک کلید متفاوت استفاده کنند. سیستم رمزنگاری را نامتقارن دو کلیدی و یا کلید عمومی نامند.

٤- کدامیک از خصوصیات رمزنگاری و رمزگشایی AES نمی باشد؟ (iranarze.ir)

۱) از ساختار Feistel استفاده نمی کند.

۲) هر مرحله به آسانی برگشت پذیر نیست.

۳) کلید ورودی به صورت یک رشته ۴۴ تایی است.

۴) از یک عمل جابجایی و سه تا جایگزینی استفاده می شود.

☑ **پاسخ سایت ایران عرضه: گزینه ۲** ⇦ موارد ذیل نکاتی در مورد AFS را روشن می سازد: ۱. یکی از خصوصیات قابل توجه این ساختار این است که یک ساختار Feistel نیست. بخاطر آورید که در ساختار کلاسیک Feistel یک نیمه از بلوک دیتا برای تغییر نیمه دیگر بکار میرفت و آنگاه دو نیمه جای خود را عوض می کردند AES از ساختار Feistel استفاده نکرده بلکه در هر دُور، کل بلوک دیتا را بصورت موازی بکار گرفته و جایگزینی و جابجایی را در آن انجام می دهد.

۲. کلیدی که در ورودی فراهم میشود، بصورت یک رشته ۴۴ تایی از کلمات ۳۲ بیتی [w] گسترش می یابد. در هر دُور ۴ کلمه مجزا (۱۲۸بیت) بعنوان کلید دُور مورد استفاده قرار می گیرد.

۳.از چهار عمل مختلف که یکی از آنها جابجایی و سه تای دیگر جایگزینی است، استفاده می شود.

۴. ساختار کاملا ساده است. هم برای رمزنگاری و هم برای رمزگشایی، رمز با یک مرحله اضافه کردن کلید دُور Add Round Key)) شروع شده و بدنبال آن یا نه دُور دیگر که هر کدام شامل چهار مرحله است، ادامه یافته و در انتها با سه مرحله در دُور دهم خاتمه می یابد.

۵. تنها مرحله Add Round Key از کلید استفاده میکند. به همین دلیل رمز با مرحله Add Round Key شروع و خاتمه می یابد. هر مرحله دیگر بدون نیاز به کلید قابل برگشت بوده و بنابراین چیزی به امنیت اضافه نمی کند.

۶. مرحله Add Round Key به تنهایی نیرومند نیست. سه مرحله دیگر بیتها را مخلوط کرده ولی خود امنیتی راایجاد نمی نمایند. زیرا از کلید استفاده نمی کنند. میتوان رمز را بصورت رمزنگاری XOR (Add Round Key)یک بلوک و پس از آن در هم ریختن بلوک (سه مرحله دیگر) و بدنبال آن رمزنگاری XOR و غیره در نظر گرفت. این روش هم بهره ور و هم بغایت امن است.

۷. هر مرحله به آسانی برگشت پذیر است. برای مراحل جابجایی بایت، شیفت، ردیف، و مخلوط کردن ستون، یک تابع معکوس در الگوریتم رمزگشایی بکار رفته است. برای مرحله(Add Round Key) عمل عکس با XOR کردن همان کلید دور به بلوک حاصل می گردد زیرا A*A*B=B است.

۸. همانند اکثر رمزهای قالبی، الگوریتم رمزگشایی از کلید گسترش یافته با نظم معکوس استفاده می کند. با وجود این الگوریتم رمزگشایی شبیه الگوریتم رمزنگاری نیست. این نتیجه ساختار خاص AFS است.

۹. وقتی روشن شد که هر چهار مرحله بازگشت پذیر هستند آنگاه تأئید اینکه رمزگشایی متن ساده را احیاء خواهد کرد. آسان خواهد بود. شکل ۵-۲ رمزنگاری و رمزگشایی را در دو ستون کنار هم با جهت های مختلف نشان داده است. در هر سطح افقی (مثل خط چین ها در شکل)، state برای هم رمزنگاری و هم رمزگشایی یکی است.

۱۰- دور نهایی چه در عمل رمزنگاری و چه در عمل رمزگشایی فقط دارای سه مرحله است. بازهم این نتیجه ساختارخاص AES است و لازم است چنین باشد تا رمز بازگشت پذیر باشد.

۵- از چه شیوه ای به منظور بالا رفتن قدرت یک سیستم رمزنگاری استفاده میشود؟ (iranarze.ir)

الف. روش توزیع کلید

ب. مبادله دیتا در عین حالی که دیگران کلید رامشاهده می کنند.

ج. عدم تعویض کلید جهت جلوگیری از فاش شدن داده ها

د. تعویض مکرر کلید

۱) الف وب ۲) ب وج ۳) الف ود ۴) ج ود

٦- چرا استفاده از اعتبار سنجی به دور از محرمانگی ارجحیت دارد؟ (iranarze.ir)

۱) اعتبار سنجی یک برنامه کامپیوتری با متن پیچیده، سرویس پرجاذبه ای است. برنامه کامپیوتر میتواند بدون اینکه هر بار رمزگشایی شود، اجرا شود که خود صرفه جویی بزرگی در منابع پردازشگر است.

۲) اگر یک دنباله اعتبار سنجی پیام به برنامه منتقل گردد، نمیتوان آن را در هر زمان لازم برای اطمینان از اصالت پیام کنترل نمود.

۳) کاربردهایی وجود دارند که در آنها یک پیام به مقاصد متعددی ارسال میشود. در این حالت داشتن تنها یک مقصد مسئول اعتبار سنجی ارزان تر و قابل اعتمادتر است.

۴) همه موارد

۷- (منبع سوالات سایت ایران عرضه) هدف طراحی HMAC چیست؟ (iranarze.ir)

۱) کلیدها را به روش پیچیده ای جهت امنیت بیشتر مورد استفاده قرار دهد.

۲) از توابع hash با اعمال تغییر مد نظر خود بتواند استفاده کند.

۳) عملکرد نهایی تابع hash را حفظ کند نه عملکرد اولیه.

۴) تحلیل رمزنگاری قابل فهمی از قدرت مکانیسم اعتبار سنجی ارائه کند.

۸- به چه دلیل اکثر محصولات و استانداردهایی که از رمزنگاری کلید -عمومی و امضاهای دیجیتال استفاده میکنند، هنوز RSA را بکار میبرند و ECC رایج تر نشده است؟ (iranarze.ir)

۱) بار پردازش سنگین تر ECC
۲) کاهش طول بیت برای RSA
۳) امنیت بیشتر برای طول بیت کمتر
۴) سطح اطمینان بالاتر RSA نسبت به ECC

۹- کدامیک از موارد زیر از نیازمندی های محیط خدماتی کامل یک سِرور kerberos نیست؟ (iranarze.ir)

۱) باید با سِرور دیگری کلید سّری مشترک نداشته باشند.

۲) تمام کاربران بایستی در نزد Kerberos ثبت نام شده باشند.

۳) سرور Kerberos بایستی ID کاربران و کلمه عبور در هم سازی شده همه کاربران حوزه را در پایگاه داده خود داشته باشد

۴) سرور Kerberos هر قلمرو با سرور قلمرو دیگر کلید سری با اشتراک بگذارد.

۱۰- ویژگی "قیود نامگذاری" چیست؟ (iranarze.ir)

۱) نشان میدهد که آیا سوژه میتواند بصورت CA عمل کند.

۲) نشان دهنده فضای نام است.

۳) نشان دهنده قیودی که ممکن است نیاز به تعیین صریح خط مشی ها داشته باشد.

۴) نشان دهنده قیودی که ممکن است مانع نگاشت خط مشی درمابقی مسیر گواهی کردن شوند.

۱۱- کدام مورد از اقلام مولفه امضا نمی باشد؟ (iranarze.ir)

۱) برچسب مکانی.
۲) چکیده پیام.
۳) دو اُکتت جلوئی چکیده پیام:
۴) ID کلید مربوط به کلید عمومی فرستنده

۱۲- مرحله چهارم از مراحل آماده سازی اایرانعرضهاا یک واحد envelopedData کدام است؟ (iranarze.ir)

۱) تولید یک کلید اجلاس شبه تصادفی برای یک الگوریتم رمزنگاری متقارن.

۲) محتوای پیام با کلید اجلاس رمزنگاری شود.

۳) برای هر گیرنده کلید اجلاس با کلید عمومی RSA گیرنده رمزنگاری شود.

۴) بلوکی با نام Recipient Info برای رمزنگاری کلید اجلاس، تهیه شود.

۱۳- کدام سرویسها به ترتیب توسط پروتکل های AH و ESP ایجاد میشوند؟ (iranarze.ir)

۱) محرمانگی دیتا- اعتبارسنجی منبع دیتا
۲) محرمانگی دیتا- صحت دیتا در حالت غیر اتصالی
۳) کنترل دستیابی- محرمانگی دیتا
۴) محرمانگی محدود جریان ترافیک- کنترل دستیابی

۱٤- کاربرد Key Exchange Payload چیست؟ (iranarze.ir)

۱) جهت تعیین هویت طرفین ارتباط.
۲) انتقال یک گواهینامه کلید-عمومی.

۳) تعریف یک تبدیل امنیتی. ۴) استفاده برای تکنیک های متنوع مبادله کلید.

۱۵- مشخصه "پروتکل Handshake" کدام است؟ (iranarze.ir)

الف. به سرور وکلاینت اجازه می دهد - طراحی شده توسط ایران عرضه - که هویت یکدیگر را تایید نمایند.

ب. برای رساندن هشدارهای مرتبط با SSL به واحد نظیر بکار میرود.

ج. ساده ترین پروتکل مختصSSL است.

د. پیچیده ترین بخش SSL مربوط به این پروتکل است.

۱) الف وب. ۲) ب وج ۳) ج ود. ۴) الف ود

۱۶- کدام گزینه از مزایای معماری SNMP می باشد؟ (iranarze.ir)

۱) نقش موجودیت SNMP توسط مدولهائی که در آن پیاده سازی شده اند تعریف میشود.

۲) ساختار پودمانی (مدولار) مشخصه ها باعث میشود که بتوان نسخه های مختلفی از هر مدول را تعریف کرد.

۳) قابلیت جایگزین کردن و یا ارتقاء توانائیها برای جنبه های معینی از SNMP، بدون نیاز به عبور به نسخه استاندارد شده بالاتر ایجاد می گردد.

۴) همه موارد

۱۷- در رابطه با مدیریت کلید و عدم لو رفتن کلید کدام گزینه صحیح است؟ (iranarze.ir)

الف. کلیدهای یک کاربر برای عامل های مختلف متفاوت است.

ب. هرکاربردارای یک کلید اعتبارسنجی و کلید رمزنگاری یکتا است.

ج. کلیدهای یک کاربر برای عوامل یکسان، متفاوت است.

د. هر کاربر فقط دارای دو کلید رمزنگاری می باشد.

۱) الف ود. ۲) الف وب ۳) ب ود. ۴) ج ود

۱۸- کدامیک از موارد زیر از معیارهای تشخیص تهاجم مبتنی بر پروفایل مفید محسوب نمی شوند؟ (iranarze.ir)

۱) شمارنده، بعنوان یک عدد صحیح غیر منفی که نمی تواند کم شود.

۲) فاصله زمانی بین دو ورود به سیستم از سوی یک کاربر مشخص باشد.

۳) پیمانه، بعنوان یک عدد صحیح غیر منفی که فقط می تواند زیاد شود.

۴) زمان سنج که زمان بین وقوع دو پیشامد یکسان را نشان میدهد.

۱۹- ویژگی مطرح شده ی زیر نشان دهنده کدام نرم افزار "بداندیش" است؟ (iranarze.ir)

"کد مختص به یک آسیب پذیر منفرد و یا مجموعه ای از آسیب پذیرها"

۱) نرم افزار Exploits ۲) بداندیش Virus Worm

۳) بداندیش Auto rooter ۴) نرم افزار Zombie

۲۰- برنامه های ساکن در حافظه، که ویروس را با فعالیت آن در یک برنامه آلوده شده شناسایی می کنند، چه می گویند؟

۱) نسل اول آنتی ویروس ها ۲) نسل چهارم آنتی ویروس ها

۳) نسل سوم آنتی ویروس ها ۴) نسل دوم آنتی ویروس ها

۲۱- ویژگی دیوار آتش از نوع"دروازه سطح مدار" چیست؟ (iranarze.ir)

الف. این نوع دروازه نسبت به فیلترهای بسته های دیتا امن ترند.

ب.سگمنت های TCP شامل داده های کاربر دو نقطه انتهایی را رِله میکند.

ج. این دیوار آتش می تواند یک سیستم منفرد یا عمل خاص باشد.

د. معمولا سگمنت های TCP را از یک اتصال به اتصال دیگر رِله میکند.

۱) الف وب. ۲) ج ود ۳) الف و د ٤) ب وج