• فصل اول: سوالات امنیت شبکه

۱- کدام مورد از وی گی های حملات امنیتی از نو غیرفعال است؟

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

ج. تغییر منابع سیستم **د. تا یر بر عملیات سیستم**

۱) الف وب ۲) ب وج ۳) ج ود ٤) الف ود

◀ **ه: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.

۲- نو حمله فعال را با توجه به مشخصه زیر تعیین کنید

"دزدیدن غیرفعال واحدهای دیتا و ارسال مجدد آنها با تاخیر"

۱) نقابدار ۲) تغییر پیام ۳) انکار سرویس ٤) بازخوانی

◀ **ه:گزینه** ⇦ حملات فعال شامل ایجاد تغییرات در جریان دیتا و یا خلق جریان جدیدی از داده هاست و میتوان آنها را به چهار دسته تقسیم کرد: نقابدار، بازخوانی، تغییر پیام و انکار سرویس .

یک حمله نقابدار وقتی صورت میپذیرد که شخصی یا واحدی وانمود کند که شخص یا واحد دیگری است.

حمله بازخوانی شامل دزدیدن غیر فعال واحدهای دینا و ارسال مجدد آنها با تأخیر برای ایجاد یک اثر مخرب است. تغییر پیام بسادگی دارای این معنی است که بخشی از یک پیام قانونی تغییر داده شود.

انکار سرویس مانع کارکرد نرمال تجهیزات شده و یا از مدیریت تسهیلات ارتباطی جلوگیری می نماید.

۳- درکدام یک از سرویس های امنیتی زیر به ترتیب مکانیسم رمزنگاری و مبادله اعتبار سنجی وجود دارد؟

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

۳) عدم انکار- اعتبارسنجی واحد نظیر ٤) محرمانگی- کنترل دستیابی

◀ **ه: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	لابه‌لائی 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

٤- در مورد استانداردسازی اینترنت، کدامیک از موارد زیر از شروط استاندارد شدن یک مشخصه نیست؟ _____

۱) دارای صور پیاده سازی واحد و مستقل باشد.
۲) از حمایت عمومی، برخوردار باشد.
۳) رقیب تکنیک های دیگر باشد.
٤) در بخش یا تمام بخش های اینترنت مفید باشد.

◄ **ه:گزینه ۱** ⇦ روند استانداردسازی: تصمیم گیری راجع به اینکه کدام RFC یک استاندارد اینترنت شود بتوسط IESG و بر اساس توصیه IETF صورت می پذیرد. برای اینکه یک مشخصه بصورت استاندارد در آید بایستی دارای شرایط زیر باشد.

پایدار بوده و خوب درک شده باشد.

از نظر تکنیکی رقیب تکنیک های دیگر باشد.

دارای صور پیاده سازی متعدد، مستقل و متعامل با تجارب عملیاتی قابل توجه باشد. از حمایت عمومی چشمگیری برخوردار باشد.

بطور قابل ملاحظه ای در بخشی و یا تمام بخشهای اینترنت مفید باشد.

٥- چنانچه فرستنده و گیرنده از یک کلید متفاوت استفاده کنند، به سیستم رمزنگاری چه می گویند؟

۱) متقارن تک کلیدی
۲) متقارن کلید سری
۳) متقارن کلید رسمی
٤) نامتقارن کلید عمومی

◄ **ه:گزینه** ⇦ سیستم های رمزنگاری معمولا از سه بعد مستقل دسته بندی می شود: نوع عملیات بکارگرفته شده برای تبدیل متن ساده به متن رمزشده - تعداد کلیدهای استفاده شده - نحوه پردازش متن ساده پیام

تعداد کلیدهای استفاده شده: 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.

٦- تحقق واقعی یک رمز قالبی متقارن بستگی به انتخاب چه پارامتری دارد؟

۱) اندازه بلوک کوچکتر ۲) اندازه کوچک کلید

۳) پیچیدگی بیشتر در الگوریتم زیر کلید ٤) وجود یک دوررمز نگاری

◄ **ه:گزینه ۳** ⇦ تحقق واقعی یک رمز قالبی متقارن بستگی به انتخاب پارامترهای زیر و موارد طراحی دارد:

. اندازه بلوک: هر چقدر اندازه بلوکها بزرگتر باشد با فرض ثابت بودن سایر پارامترها امنیت بیشتر ولی سرعت رمزنگاری رمزگشایی کمتر است. مصالحه مناسب در این مورد انتخاب بلوکی با طول ۱۳۸ بیت بوده که در طراحی رمز قالبی، تقریبا انتخابی همگانی است.

. اندازه کلید: اندازه بزرگتر کلید بمنزله امنیت بیشتر است. ولی ممکن است سرعت رمزنگاری، رمزگشایی را کاهش دهد. معمول ترین کلیدها در الگوریتم های مدرن دارای طول ۱۲۸ بیت هستند.

. تعداد دورها: جوهره یک رمز قالبی متقارن در این است که تنها یک دور رمزنگاری امنیت مناسبی را ایجاد نمی کند. و بنابراین دورهای بیشتری از رمزنگاری برای افزایش امنیت، مورد نیاز است. اندازه معمول در این مورد ١٦ دور است.

. الگوریتم تولید زیر کلید: پیچیدگی بیشتر در این الگوریتم بایستی باعث افزایش پیچیدگی در شکستن رمز گردد.

. تابع دور: باز هم پیچیدگی بیشتر معمولا بمعنای مقاومت بیشتر در مقابل کشف رمز است.

۷-کدامیک از خصوصیات رمزنگاری و رمزگشایی AES **نمی باشد؟**

۱) از ساختار Feistel استفاده نمی کند.

۲) هر مرحله به آسانی برگشت پذیر نیست.

۳) کلید ورودی به صورت یک رشته ٤٤ تایی است.

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

◄ **ه: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 د ور، 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 ٤٤ تایی از کلمات ۳۲ بیتی [w] گسترش می یابد. در هر دور ٤ کلمه مجزا (۱۲۸بیت) بعنوان کلید د ور مورد استفاده قرار می گیرد.

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

٤. ساختار کاملا ساده است. هم برای رمزنگاری و هم برای رمزگشایی، رمز با یک مرحله اضافه کردن کلید د ور

Add Round Key)) شروع شده و بدنبال آن یا نه دور دیگر که هر کدام شامل چهار مرحله است، ادامه یافته و در انتها با سه مرحله در دور 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.

٦. 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.

۸- برای چه پیامهایی، ECB امن تر است؟

۱) متون ساده کوتاه ۲) پیام بشدت ساختار یافته

۳) پیام دارای عناصر تکرار شونده ٤) پیام های دارای نظم

◄ **ه: گزینه ۱** ⇦ یک رمز قالبی متقارن، داده ها را بصورت یک بلوک در هر زمان پردازش میکند. در DES و DES۳ طول بلوک ٦٤ بیت است. برای متون ساده با طول بیشتر، لازم است تا متن به بلوکهای -٦٤ بیتی تقسیم شود (اگر لازم باشد، آخرین بلوک با بیتهای اضافی کامل میشود). ساده ترین راه برای این کار چیزی است که آن را مود کتاب کد الکترونیکی ECB (codebook electronic) گویند که در آن در هر لحظه، ٦٤ بیت از متن ساده تحت پردازش قرار گرفته و همه بلوکهای متن با کلید واحدی پردازش میشوند. اصطلاح کتاب کد(codebook (از این جهت بکار گرفته شده است که برای یک کلید واحد، یک متن رمزشده یکتا برای هربلوک ٦٤ - بیتی دیتا حاصل میشود. بنابراین میتوان یک کتاب کد عظیمی را تصور کرد که در آن برای هر بلوک -٦٤ بیتی ممکن از متن ساده، یک متن رمزشده نظیر آن وجود داشته باشد.

در ECB، اگر همان بلوک ٦٤- بیتی متن ساده بیش از یکبار در پیام ظاهر شود، همیشه همان متن رمز شده دفعه اول حاصل خواهد شد. به همین دلیل برای پیامهای طولانی، مود ECB ممکن است امن نباشد. اگر پیام بشدت ساختار یافته باشد، یک شکننده رمز ممکن است بتواند از این نظم سوء استفاده کند. بعنوان مثال اگر معلوم باشد که پیام همیشه با میدانهای از قبل تعریف شده معینی شروع میشود، آنگاه شکننده رمز ممکن است تعدادی زوج متن ساده- متن رمز شده را در اختیار داشته و روی آنها کار کند. اگر پیام دارای عناصر تکرار شده ای باشد که پریود تکرار آنها مضربی از ٦٤ بیت باشد، آنگاه این عناصر می توانند توسط تحلیلگر شناخته شوند. این موارد ممکن است به تحلیل رمز کمک کرده و یا ممکن است فرصتی برای جایگزینی و یا تغییر سازمان بلوک بدست دهند.

۹- از چه شیوه ای به منظور بالا رفتن قدرت یک سیستم رمزنگاری استفاده میشود الف.

روش توزیع کلید

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

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

د. تعوی مکرر کلید

۱) الف وب ۲) ب وج ۳) الف ود ٤) ج ود

◄ **ه: گزینه ۳** ⇦ برای اینکه رمزنگاری متقارن عملی گردد، طرفین ارتباط بایستی دارای کلید رمز واحدی بوده و این کلید بایستی از دستیابی دیگران محافظت گردد. علاوه بر این معمولا لازم است تا مکررا کلید را تعوی کرده تا احتمال فاش شدن داده ها، در صورت دستیابی یک دشمن به کلید، را به حداقل برسانیم. بنابراین قدرت یک سیستم رمزنگاری مرتبط با روش توزیع کلید است. اصطلاح «توزیع کلید» به روش تحویل کلید به دو طرفی اشاره میکند که تمایل به مبادله دیتا دارند، بدون اینکه دیگران بتوانند کلید را مشاهده نمایند. توزیع کلید را میتوان به چند صورت انجام داد برای دو طرف A و B:

۱.کلید میتواند توسط A انتخاب شده و بصورت فیزیکی به B تحویل گردد. ۲.شخص ثالثی می تواند کلید را انتخاب کرده و به صورت فیزیکی آن را به A و B تحویل دهد.

۳.اگر A و B قبلا و اخیرا از کلیدی استفاده می کرده اند. یکی از طرفین میتواند کلید جدید را انتخاب کرده و آن را بصورت رمزنگاری شده با استفاده از کلید قدیم، به طرف دیگر تحویل دهد.

٤. اگر A و B هر کدام یک ارتباط رمزنگاری شده با شخص ثالث C دارند، C میتواند یک کلید را از طریق پیوندهای رمزنگاری شده با A و B به آنها تحویل دهد.

۱۰- جنبه مه م اعتبارسنجی پیام چیست؟

۱) تایید قانونی بودن پیام ۲) تحقیق دربازه معتبر بودن منبع پیام

۳) تحقیق درباره دست نخورده بودن پیام ٤) همه موارد