

شروع	دوشنبه، 27 دی 1400، 8:31 صبح
وضعیت	پایان یافته
پایان	دوشنبه، 27 دی 1400، 9:31 صبح
زمان صرف شده	59 دقیقه 33 ثانیه
جمع نمره	34.00 از 27.04
نمره	(80%) از 10.00 (7.95)

1 سؤال

درست

نمره 1.00 از 1.00

حاصل معکوس عدد 13 در هنگ عدد 84 را بدست آورده و در کادر زیر بنویسید. (فقط جواب آخر را بنویسید و از نوشتن اضافات خودداری کنید.)

 پاسخ:

پاسخ درست: 13

سؤال 2

پاسخ نیمه درست
نمره 4.00 از 5.00

گزینه صحیح برای هر مورد را انتخاب نمایید.

- web of trust
- MAC
- AuC
- Cross Signing
- DPI
- RAND
- گوشی تلفن همراه
- AuC

راهکاری جهت مدیریت شناسه و گواهی نامه

با ارسال AUTN و RAND با مقایسه کدام پارامتر شبکه به کاربر احراز اصالت می‌شود.

نهاد مدیریتی احراز اصالت شبکه نسل سوم در PS.

گواهی نامه توسط چندین مرجع صدور گواهی نامه امضا می‌گردد.

روشی که به صورت گسترده در نرم‌افزارها و دیوارهای آتشین مورد استفاده قرار می‌گیرد.

در صورت لو رفتن بردارهای احراز اصالت، کدام پارامتر می‌تواند امنیت نشست‌های (sessions) پیشین کاربر در شبکه را تضمین نماید.

رمزگاری (Encryption) در کدام قسمت انجام می‌شود.

کلید محروم‌نامه در سمت شبکه در این قسمت قرار دارد.

RES



گوشی تلفن همراه



با ارسال بردارهای احراز اصالت با مقایسه کدام پارامتر کاربر به شبکه احراز اصالت می‌شود.

یکپارچگی (Integrity) توسط کدام قسمت انجام می‌شود.

پاسخ شما تا حدودی صحیح است

شما به درستی 8 گزینه را انتخاب کرده‌اید

پاسخ درست:

راهکاری جهت مدیریت شناسه و گواهی نامه → PKI

با ارسال AUTN و RAND با مقایسه کدام پارامتر شبکه به کاربر احراز اصالت می‌شود. → MAC

نهاد مدیریتی احراز اصالت شبکه نسل سوم در SGSN → PS.

گواهی نامه توسط چندین مرجع صدور گواهی نامه امضا می‌گردد. → Cross Signing

روشی که به صورت گستردگی در نرم‌افزارها و دیوارهای آتشین مورد استفاده قرار می‌گیرد. → DPI

در صورت لو رفتن بردارهای احراز اصالت، کدام پارامتر می‌تواند امنیت نشست‌های (sessions) پیشین کاربر در شبکه را تضمین نماید. → RAND

رمزگاری (Encryption) در کدام قسمت انجام می‌شود. → گوشی تلفن همراه

کلید محروم‌انه در سمت شبکه در این قسمت قرار دارد. → AuC

با ارسال بردارهای احراز اصالت با مقایسه کدام پارامتر کاربر به شبکه احراز اصالت می‌شود.

→ RES

یکپارچگی (Integrity) توسط کدام قسمت انجام می‌شود. → گوشی تلفن همراه

سؤال 3

کامل

نمره 2.50 از 2.50

آلیس می‌خواهد توسط الگوریتم RSA کلید عمومی و خصوصی خودش را تولید کند. در صورتی که مقدار n برابر 221، کلید عمومی برابر 163 و همچنین مقدار متن رمز شده (Ciphertex) برابر 70 باشد، مقدار متن آشکار را بدست آورید؟ (اطفا کل روند را گام به گام تشریح کنید و از نوشتن صرفا جواب نهایی بپرهیزید)

[rsa.jpg_ !\[\]\(c694a3ff3b077d76910920a6a1593ab4_img.jpg\)](#)

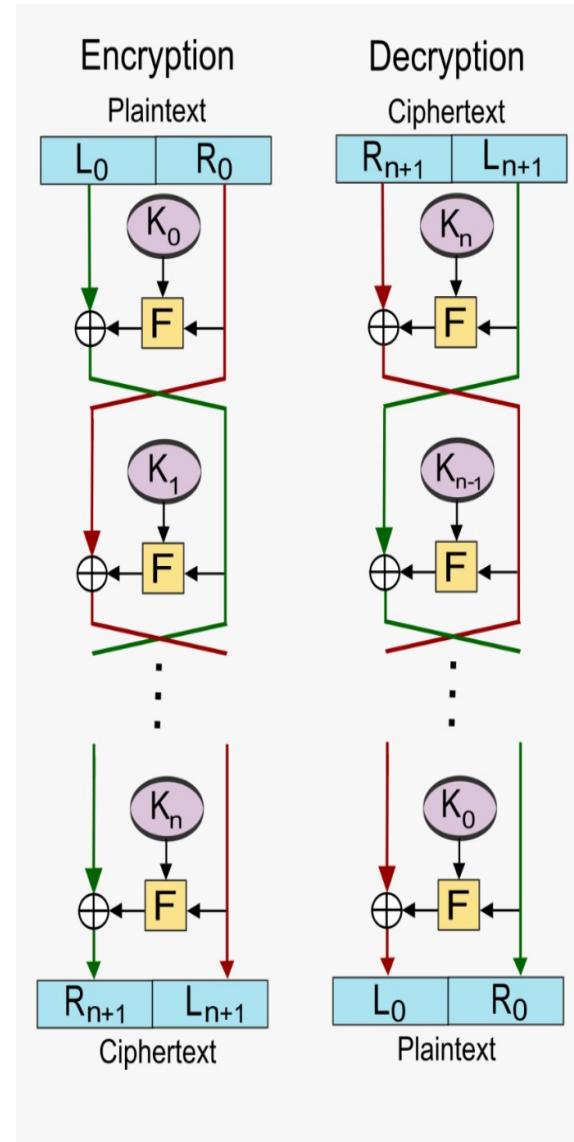
دیدگاه:

سوال 4

درست

نمره 1.50 از 1.50

کدامیک گزینه مناسبی در رابطه با شکل زیر است؟



یک یا چند گزینه را انتخاب کنید:

1. هر دور آن شامل یک مرحله جانشینی است که به دنبال آن دو مرحله جایگشتی انجام می‌گیرد.
2. از الگوریتم یکسانی در رمزنگاری و رمزگشایی استفاده می‌کند.





3. در هر دور، نیمه راست بلوک، R ، بدون تغییر می‌گذرد.
4. جهت توسعه بسیاری از رمزهای جویباری به کار می‌رود.
5. در هر دور، نیمه چپ بلوک، L ، بدون تغییر می‌گذرد.

پاسخ شما صحیح می باشد

پاسخ درست عبارت است از: از الگوریتم یکسانی در رمزنگاری و رمزگشایی استفاده می‌کند.
در هر دور، نیمه راست بلوک، R ، بدون تغییر می‌گذرد.

سؤال 5

پاسخ نیمه درست

نمره 6.00 از 5.50

کدام مورد صحیح و کدام غلط است؟ صحیح غلط صحیح صحیح غلط صحیح صحیح غلط

در زنجیره گواهینامه، CA تنها می‌تواند گواهینامه خودش را امضا کند (*self-signed*)

در الگوریتم کلید متقارن، همه می‌توانند عملیات رمزگاری را انجام دهند، اما فقط گیرنده می‌تواند رمزگشایی را انجام دهد.

یک سامانه‌ی One Time Pad تنها در صورتی امنیت کامل را دارد که طول یک کلید تصادفی برابر با متن اصلی باشد.

به حمله‌ای که حمله‌گر علاوه بر شنود، پیام را نیز تغییر می‌دهد، Active Attack گویند.

در شبکه‌های نسل دوم تنها یکپارچگی (Integrity) پیام‌ها تامین می‌شوند.

در Temporal & Statistical Privacy سعی در حفظ حریم خصوصی داده وجود دارد.

در فرآیند احراز اصالت در شبکه‌های تلفن همراه، حمله‌گر نیز می‌تواند پارامتر AUTN را در اختیار داشته باشد.

تنها راه برای اطمینان بخشی از صحیت تبادل کلید عمومی، استفاده از یک مرجع متمرکز به عنوان مرجع ثالث مورد اعتماد است.

غلط	
<input checked="" type="checkbox"/>	
غلط	
<input checked="" type="checkbox"/>	
صحيح	
<input checked="" type="checkbox"/>	
غلط	
<input checked="" type="checkbox"/>	

در زیرساخت کلید عمومی (Public Key Infrastructure) صحبتی از بحث‌های سخت‌افزاری در حوزه مدیریت کلید صورت نمی‌پذیرد.

در بحث فرآیند احراز اصالت، تمام توابع MILENAGE به غیر از تابع F1 همگی یکطرفه هستند.

در شبکه‌های نسل سوم رمزنگاری تنها میان کاربر و ناحیه RAN صورت می‌گیرد.

روند امضای یک گواهینامه بدین صورت است که کل متن گواهینامه با کلید خصوصی CA رمز می‌شود و در اختیار فرد قرار می‌گیرد.

پاسخ شما تا حدودی صحیح است

شما به درستی 11 گزینه را انتخاب کرده‌اید

پاسخ درست:

در زنجیره گواهینامه Root CA است که می‌تواند گواهینامه خودش را امضا کند (*self-signed*) → صحیح،

در الگوریتم کلید متقارن، همه می‌توانند عملیات رمزنگاری را انجام دهند، اما فقط گیرنده می‌تواند رمزگشایی را انجام دهد. → غلط،

یک سامانه‌ی One Time Pad تنها در صورتی امنیت کامل را دارد است که طول یک کلید تصادفی برابر با متن اصلی باشد. → صحیح،

به حمله‌ای که حمله‌گر علاوه بر شنود، پیام را نیز تغییر می‌دهد، Active Attack گویند. → صحیح،

در شبکه‌های نسل دوم یکپارچگی (Integrity) پیام‌ها تامین می‌شوند. → غلط،

در Temporal & Statistical Privacy سعی در حفظ حریم خصوصی داده وجود دارد. → غلط،

در فرآیند احراز اصالت در شبکه‌های تلفن همراه، حمله‌گر نیز می‌تواند پارامتر AUTN را در اختیار داشته باشد. → صحیح،

تنها راه برای اطمینان بخشی از صحت تبادل کلید عمومی، استفاده از یک مرجع متمرکز به عنوان مرجع ثالث مورد اعتماد است. → غلط،

در زیرساخت کلید عمومی (Public Key Infrastructure) صحبتی از بحث‌های سخت‌افزاری در حوزه مدیریت کلید صورت نمی‌پذیرد. → غلط،

در بحث فرآیند احراز اصالت، تمام توابع MILENAGE به غیر از تابع F1 همگی یکطرفه هستند. → غلط،

در شبکه‌های نسل سوم رمزنگاری تنها میان کاربر و ناحیه RAN صورت می‌گیرد. → صحیح،

روند امضای یک گواهینامه بدین صورت است که کل متن گواهینامه با کلید خصوصی CA رمز می‌شود و در اختیار فرد قرار می‌گیرد. → غلط

سؤال 6

کامل

نمره 3.00 از 3.00

در پروتکل تبادل کلید دیفی-هلمن فرض کنید که پارامترهای سیستم برابر با 359 و 10 باشد. در صورتی که آلیس و باب به ترتیب اعداد تصادفی 3 و 7 انتخاب کرده باشند، مقادیر کلید عمومی آلیس، کلید عمومی باب و مقدار کلید مخفی مشترک آلیس و باب بدست آمده برابر با چند است؟ (اطلاعات فقط جواب نهایی را بنویسید، و راه حل را نیز به طور کامل ذکر نمایید.)

dh.jpg 

دیدگاه:

سؤال 7

نادرست

نمره 0.00 از 1.50

احتمال نفوذ حمله‌گر A دو برابر احتمال نفوذ حمله‌گر B به یک سیستم است و احتمال این که حداقل یکی از آن‌ها به سیستم نفوذ کند برابر 0.625 است. در صورتی که به ما گفته شود که حمله‌گر A در این سیستم نفوذ پیدا کرده باشد، چه میزان از ابهام ما برطرف شده است؟ (فقط جواب آخر را بنویسید و از نوشتن اضافات خودداری فرمایید.)

پاسخ: 

پاسخ درست: 1

سؤال 8

پاسخ نیمه درست
نمره 0.54 از 1.50

کدام یک از موارد صحیح است؟

یک یا چند گزینه را انتخاب کنید:

- می‌توان بیان نمود که الگوریتم‌های کلید نامتقارن و الگوریتم‌های کلید نامتقارن با طول کلید برابر از امنیت یکسانی برخوردار نیستند.
- در الگوریتم نامتقارن (کلید عمومی)، از نظر محاسباتی نمی‌توان از کلید رمزگذاری به کلید رمزگشایی رسید.
- قدرت و اهمیت رمزنگاری در الگوریتم‌های کلید غیرمتقارن به قدرت الگوریتم و توزیع کلید وابسته است.
- در رمزنگاری متقارن، در صورتی که 10 نفر با هم در ارتباط باشند، هر فردی برای ارتباط با سایر افراد به 45 کلید نیاز دارد.
- الگوریتم‌های کلید نامتقارن سرعت عمل بالاتری نسبت به الگوریتم‌های کلید نامتقارن دارند.
- از جمله مشکلات الگوریتم‌های نامتقارن، احراز اصالت کلید محترمانه بدلیل امکان داشتن شنود در ارتباط بین فرستنده و گیرنده است.

پاسخ شما تا حدودی صحیح است
شما به درستی 2 گزینه را انتخاب کرده‌اید
پاسخ درست عبارت است از:
می‌توان بیان نمود که الگوریتم‌های کلید نامتقارن و الگوریتم‌های کلید برابر از امنیت یکسانی برخوردار نیستند.

قدرت و اهمیت رمزنگاری در الگوریتم‌های کلید غیرمتقارن به قدرت الگوریتم و توزیع کلید وابسته است.

الگوریتم‌های کلید نامتقارن سرعت عمل بالاتری نسبت به الگوریتم‌های کلید نامتقارن دارند.
در الگوریتم نامتقارن (کلید عمومی)، از نظر محاسباتی نمی‌توان از کلید رمزگذاری به کلید رمزگشایی رسید.

سؤال 9

درست

نمره 2.50 از 2.50

برای هرکدام از عبارت‌های زیر، گزینه‌ی مناسب را انتخاب کنید.

- Substitution Cipher
- Transposition Cipher
- Integrity
- نهان‌کاوی
- Steganography

در این رمز جایگاه حروف در یک متن بهم نمی‌خورد.

در این رمز ترتیب حروف متن به هم می‌ریزد.

اطمینان از تغییر نکردن داده توسط افراد غیر مجاز؟

علم پی‌بردن به وجود پیام در صورتی که پیام را در یک تصویر پنهان کرده باشیم؟

روش مخفی کردن پیام‌ها در فایل‌های صوتی؟

پاسخ شما صحیح می‌باشد

پاسخ درست:

در این رمز جایگاه حروف در یک متن بهم نمی‌خورد. → Substitution Cipher

در این رمز ترتیب حروف متن به هم می‌ریزد. → Transposition Cipher

اطمینان از تغییر نکردن داده توسط افراد غیر مجاز؟ → Integrity

علم پی‌بردن به وجود پیام در صورتی که پیام را در یک تصویر پنهان کرده باشیم؟ → نهان‌کاوی

روش مخفی کردن پیام‌ها در فایل‌های صوتی؟ → Steganography

سؤال 10

درست

نمره 4.00 از 4.00

گزینه مناسب برای هر مورد را انتخاب کنید.

- S-Box ✓
- key Transport ✓
- Symmetric-Key Algorithm ✓
- P-Box ✓
- Stream Cipher ✓
- key Agreement ✓
- Asymmetric-Key Algorithm ✓
- حمله بر اساس فقط متن رمز شده (Ciphertext Only Attack) ✓

قسمتی در الگوریتم DES که منجر به غیرخطی شدن سامانه می‌گردد.

یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

گیرنده و فرستنده از یک کلید مشترک برای رمزگذاری و رمزگشایی استفاده می‌کنند.

عملیات جایگشت در الگوریتم DES در کدام قسمت صورت می‌گیرد؟

در شبکه‌های تلفن همراه از کدام نوع رمز نگاری استفاده شده است.

هر دو طرف ارتباط، در فرآیند تولید کلید مشارکت می‌کنند.

امنیت ... مبتنی بر طول کلید و مسایل نظریه اعداد است.

سامانه Vernam در برابر کدام حمله مقاوم است.

پاسخ شما صحیح می باشد

پاسخ درست:

قسمتی در الگوریتم DES که منجر به غیر خطی شدن سامانه می گردد. → S-Box

یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می دهد. → key Transport

گیرنده و فرستنده از یک کلید مشترک برای رمزگذاری و رمزگشایی استفاده می کنند. → Symmetric-Key Algorithm

عملیات جایگشت در الگوریتم DES در کدام قسمت صورت می گیرد؟ → P-Box

در شبکه های تلفن همراه از کدام نوع رمز نگاری استفاده شده است. → Stream Cipher

هر دو طرف ارتباط، در فرآیند تولید کلید مشارکت می کنند. → key Agreement

امنیت ... مبتنی بر طول کلید و مسایل نظریه اعداد است. → Asymmetric-Key Algorithm

سامانه Vernam در برابر کدام حمله مقاوم است. → حمله بر اساس فقط متن رمز شده (Ciphertext Only Attack)

سؤال 11

کامل

نمره 0.00 از 3.00

احتمال توانم دو متغیر تصادفی X و Y همراه با توزیع حاسیه‌ای در جدول زیر ارائه شده است. با توجه به مستقل بودن X و Y مطلوب است:

$$H(x,y), I(x;y), H(y|x=2)$$

(مراحل حل را به صورت کامل بنویسید.)

$P(x,y)$	$y=1$	$y=2$	$y=3$	$P(X)$
$x=1$	P_{11}	P_{12}	P_{13}	$\frac{2}{3}$
$x=2$	P_{21}	P_{22}	P_{23}	$\frac{1}{3}$
$P(Y)$	$\frac{3}{4}$	$\frac{1}{6}$	$\frac{1}{12}$	

دیدگاه:

سؤال 12

درست

نمره 1.50 از 1.50

با استفاده از الگوریتم Affine Cipher و پارامترهای $a=10$, $k=6$ پیام AONJEC که از جدول کاراکترهای زیر انتخاب شده است را رمزگشایی کنید.

ملاحظات:

- ایندکس شروع از صفر.
- کلمه رمزگشایی حاصل را با حروف کوچک به عنوان جواب، بنویسید.

جدول کاراکترها

ABCDEJIHGFJKLMNO .

پاسخ:

پاسخ:

ilblbl

$$C = (A * m + K) \bmod 15$$

پاسخ درست: ilblbl

دیدگاه:

سؤال 13

درست

نمره 1.00 از 1.00

کدام یک از موارد زیر در مورد الگوریتم RSA صحیح است؟

یک یا چند گزینه را انتخاب کنید:



- از این الگوریتم نمی‌توان در فرایند تبادل کلید استفاده کرد.
- مقدار کلید عمومی در این الگوریتم از مقدار (n) کوچکتر بوده و نسبت به یکدیگر اول هستند.
- برای این‌که با الگوریتم RSA بتوان یک امضای دیجیتال ایجاد کرد، می‌بایست فرد امضا کننده پیام را با کلید خصوصی خودش رمز نماید.
- در این الگوریتم، حمله‌گر می‌تواند به کلید عمومی و تابع اویلر n دسترسی داشته باشد.
- روند این الگوریتم مشابه الگوریتم AES است.
- امنیت الگوریتم در گرو سخت بودن مساله تجزیه عدد است.
- در الگوریتم RSA، کلید خصوصی و کلید عمومی نسبت به هنگ تابع اویلر n ، معکوس یکدیگر هستند.
- در این الگوریتم دو عدد اول p و q می‌توانند با یکدیگر برابر باشند.

پاسخ شما صحیح می‌باشد

پاسخ درست عبارت است از:

مقدار کلید عمومی در این الگوریتم از مقدار (n) کوچکتر بوده و نسبت به یکدیگر اول هستند.

امنیت الگوریتم در گرو سخت بودن مساله تجزیه عدد است.

در الگوریتم RSA، کلید خصوصی و کلید عمومی نسبت به هنگ تابع اویلر n ، معکوس یکدیگر هستند.

برای این‌که با الگوریتم RSA بتوان یک امضای دیجیتال ایجاد کرد، می‌بایست فرد امضا کننده پیام را با کلید خصوصی خودش رمز نماید.

>>

<<