شروع	سه‌شنبه، 30 فروردین 1401، 3:50 عصر
وضعیت	پایان‌یافته
پایان	سه‌شنبه، 30 فروردین 1401، 4:10 عصر
زمان صرف شده	19 دقیقه 59 ثانیه
جمع نمره	12.21 از 17.00
نمره	**7.18** از 10.00 (72٪)

سؤال 1

کامل

نمره 5.00 از 5.00

در الگوریتم رمز الجمال فرض کنید که Alice عدد اول 107را انتخاب می کند. در ضمن او مولد 2 را بر می‌گزیند و همچنین کلید خصوصی 67 را نیز انتخاب می‌کند. در صورتی‌که Bob کلید عمومی Alice را بداند، و بخواهد حرف B با کد اسکی 66 را برای Alice ارسال کند چه پیامی باید برای او ارسال نماید و Alice چگونه می‌تواند با دریافت پیام رمز شده به متن اصلی دست پیدا کند؟ فرض کنید Bob نیز عدد تصادفی 45 را انتخاب کرده باشد. (لطفا کل روند را گام به گام تشریح کنید و از نوشتن صرفا جواب نهایی بپرهیزید)

سؤال 2

کامل

نمره 3.00 از 3.00

چگونه الگوریتم دیفی-هلمن در توافق کلید نقش دارد و فرآیند آن را به صورت مختصر توضیح دهید.

سؤال 3

کامل

نمره 1.71 از 3.00

صحیح یا غلط بودن هر یک از گزاره های زیر را مشخص کنید.

برای یافتن تابع اویلر نیاز است که مساله تجزیه عدد حل شود.	صحیح
در رمز الجمال، اگر پیامی چند بار رمز شود، هر بار متن رمز جدیدی تولید میشود.	غلط
الگوریتم‌های دیفی هلمن و الجمال به دلیل نبود احراز اصالت در برابر حمله شنود ضعیف هستند.	صحیح
شخصی می‌خواهد با استفاده از الگوریتم الجمال پیامی را ارسال نماید، مقدار کلید سرّی مشترک (shared secret) برابر است با مقدار کلید عمومی گیرنده به توان کلید خصوصی فرستنده است.	صحیح
امنیت پس‌رو یا Backward Security تضمین می کند که هرگاه کاربری شبکه را ترک کرد، به اطلاعات قبلی دسترسی نداشته باشد.	صحیح
امنیت پیش‌رو (Forward Secrecy) تضمین می‌نماید که هر زمانی که کلید محرمانه Long Term لو برود، اطلاعات مبادله شده در آینده همچنان امن باشند.	غلط
در الگوریتم RSA، حمله‌گر می‌تواند به کلید عمومی و تابع اویلر n دسترسی داشته باشد.	غلط

پاسخ درست:
برای یافتن تابع اویلر نیاز است که مساله تجزیه عدد حل شود. → صحیح,

در رمز الجمال، اگر پیامی چند بار رمز شود، هر بار متن رمز جدیدی تولید میشود. → صحیح,

الگوریتم‌های دیفی هلمن و الجمال به دلیل نبود احراز اصالت در برابر حمله شنود ضعیف هستند.

→ غلط,

شخصی می‌خواهد با استفاده از الگوریتم الجمال پیامی را ارسال نماید، مقدار کلید سرّی مشترک (shared secret) برابر است با مقدار کلید عمومی گیرنده به توان کلید خصوصی فرستنده است. → صحیح,
امنیت پس‌رو یا Backward Security تضمین می کند که هرگاه کاربری شبکه را ترک کرد، به اطلاعات قبلی دسترسی نداشته باشد. → غلط,

امنیت پیش‌رو (Forward Secrecy) تضمین می‌نماید که هر زمانی که کلید محرمانه Long Term لو برود، اطلاعات مبادله شده در آینده همچنان امن باشند. → غلط,

در الگوریتم RSA، حمله‌گر می‌تواند به کلید عمومی و تابع اویلر n دسترسی داشته باشد. → غلط

سؤال 4

کامل

نمره 0.50 از 2.50

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

یک یا چند گزینه را انتخاب کنید:

- [x] 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.
- [ ] از این الگوریتم نمی‌توان در فرایند تبادل کلید استفاده کرد.
- [ ] مقدار کلید عمومی در این الگوریتم از مقدار $\phi(n)$ کوچک‌تر بوده و نسبت به یک‌دیگر اول هستند.
- [ ] امنیت الگوریتم در گرو سخت بودن مساله تجزیه عدد است.
- [x] در الگوریتم RSA، کلید خصوصی و کلید عمومی نسبت به هنگ تابع اویلر n، معکوس یکدیگر هستند.
- [x] در این الگوریتم دو عدد اول p و q می‌توانند با یک‌دیگر برابر باشند.
- [ ] روند این الگوریتم مشابه الگوریتم AES است.

پاسخ درست عبارت است از:
مقدار کلید عمومی در این الگوریتم از مقدار $\phi(n)$ 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.

سؤال 5

کامل

نمره 1.00 از 1.00

حاصل معکوس عدد 13 در هنگ عدد 54 را بدست آورده و در کادر زیر بنویسید. (جواب نهایی را به صورت یک عدد در کادر زیر قرار دهید)

پاسخ:

پاسخ درست: 25

سؤال 6

کامل

نمره 1.00 از 2.50

برای هر گزاره، گزینه صحیح را انتخاب کنید:

یک چارچوب کلی اعم از سخت افزار و نرم افزار و قوانین برای مدیریت، بروزرسانی و ابطال گواهینامه‌ها است.

یک روش رمزنگاری بلوکی است که در آن متن اصلی و متن رمزشده اعداد صحیحی بین 0 و nاز میان تعداد n موجودیت هستند

مبتنی بر دشواری حل مسئله لگاریتم گسسته است و شامل دو گام مرحله تولید کلید و اجرای الگوریتم رمزنگاری است.

اگر کاربر وارد سامانه شد، اطلاعات گذشته افشا نشود.

هدف از این الگوریتم این است که دو کاربر قادر به تبادل کلید مخفی به شکلی امن باشند بطوری که در آینده بتوانند از آن برای رمزگذاریهای بعدی پیامها استفاده نمایند.

KPI

دیفی-هلمن

الجمال

Forward Secrecy

RSA

پاسخ درست:
یک چارچوب کلی اعم از سخت افزار و نرم افزار و قوانین برای مدیریت، بروزرسانی و ابطال گواهینامه‌ها است. → KPI,

یک روش رمزنگاری بلوکی است که در آن متن اصلی و متن رمزشده اعداد صحیحی بین 0 و nاز میان تعداد n موجودیت هستند → RSA,

مبتنی بر دشواری حل مسئله لگاریتم گسسته است و شامل دو گام مرحله تولید کلید و اجرای الگوریتم رمزنگاری است. → الجمال,

اگر کاربر وارد سامانه شد، اطلاعات گذشته افشا نشود. → Backward Secrecy,

هدف از این الگوریتم این است که دو کاربر قادر به تبادل کلید مخفی به شکلی امن باشند بطوری که در آینده بتوانند از آن برای رمزگذاریهای بعدی پیامها استفاده نمایند. → دیفی-هلمن