شروع	سه‌شنبه، 3 اسفند 1400، 4:04 عصر
وضعیت	پایان‌یافته
پایان	سه‌شنبه، 3 اسفند 1400، 4:19 عصر
زمان صرف شده	15 دقیقه
جمع نمره	17.50 از 19.00
نمره	**9.21** از 10.00 (92٪)

سؤال 1

درست

نمره 2.50 از 2.50

اطمینان از قابل تغییر بودن اطلاعات و برنامه ها فقط به صورت مشخص و مجاز. یکپارچگی داده ✔

اطمینان از عدم در دسترس یا آشکار بودن داده های خصوصی برای افراد غیرمجاز. اصل Confidentiality ✘

اطمینان از عملکرد بلادرنگ سامانه و عدم رد خدمات برای کاربران مجاز. اصل Availability ✔

اطمینان از انجام عملیات سامانه به صورت عادی، عاری از دستکاری غیرعمدی یا غیرمجاز. یکپارچگی سامانه ✔

شکسته شدن ماشین انیگما یکی از موارد نقض این اصل است. اصل Integrity ✘

پاسخ شما صحیح می باشد

پاسخ درست عبارت است از:
اطمینان از قابل تغییر بودن اطلاعات و برنامه ها فقط به صورت مشخص و مجاز. [یکپارچگی داده]

اطمینان از عدم در دسترس یا آشکار بودن داده های خصوصی برای افراد غیرمجاز. [محرمانگی داده]

اطمینان از عملکرد بلادرنگ سامانه و عدم رد خدمات برای کاربران مجاز. [اصل Availability]

اطمینان از انجام عملیات سامانه به صورت عادی، عاری از دستکاری غیرعمدی یا غیرمجاز. [یکپارچگی سامانه]

شکسته شدن ماشین انیگما یکی از موارد نقض این اصل است. [اصل Confidentiality]

دیدگاه:

سؤال 2

درست

نمره 3.00 از 3.00

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

لوگوهای برنامه‌های تلویزیونی از نوع نشان‌گذاری شکننده و مرئی هستند.	غلط ✔
در شبکه‌های نسل دوم تنها یکپارچگی (Integrity) پیام‌ها تامین می‌شد.	غلط ✔
شبکه‌های نسل دوم، سوم و چهارم به‌دلیل وجود رمز شدن داده بر خلاف شبکه‌های نسل صفر و یک، در مقابل حمله شنود مقاوم هستند.	غلط ✔
نشان‌گذاری غیرشکننده نسبت به تغییرات و حملات مقاوم می‌باشد.	صحیح ✔
درج LSB می‌تواند به عنوان یک تکنیک steganography برای مخفی کردن پیام‌ها در فایل‌های صوتی به‌کار رود.	صحیح ✔
یک سامانه‌ی One Time Pad تنها در صورتی امنیت کامل را دارا است که که طول یک کلید تصادفی برابر با متن اصلی باشد.	صحیح ✔

پاسخ شما صحیح می باشد

پاسخ درست:
لوگوهای برنامه‌های تلویزیونی از نوع نشان‌گذاری شکننده و مرئی هستند. → غلط,
در شبکه‌های نسل دوم تنها یکپارچگی (Integrity) پیام‌ها تامین می‌شد. → غلط,

شبکه‌های نسل دوم، سوم و چهارم به‌دلیل وجود رمز شدن داده بر خلاف شبکه‌های نسل صفر و یک، در مقابل حمله شنود مقاوم هستند. → غلط,
نشان‌گذاری غیرشکننده نسبت به تغییرات و حملات مقاوم می‌باشد. → صحیح,
درج LSB می‌تواند به عنوان یک تکنیک steganography برای مخفی کردن پیام‌ها در فایل‌های صوتی به‌کار رود. → صحیح,

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

سؤال 3

درست

نمره 1.00 از 1.00

راه حلی برای جلوگیری از حملات فیشینگ؟

پاسخ: ✗

پاسخ درست: احراز اصالت

دیدگاه:

سؤال 4

درست

نمره 1.00 از 1.00

کدام مورد از نوع رمزنگاری جایگشتی (Transposition Cipher) نیست؟ (ممکن است چند مورد صحیح باشد.)

- [x] رمز هوموفونیک (Homophonic Cipher)
- [ ] رمز ستونی (Columnar Cipher)
- [x] ماشین انیگما (Enigma Rotor Cipher Machine)
- [x] رمز مستوی (Affine Cipher)
- [x] رمز ویگنر (Vigenere Cipher)

پاسخ شما صحیح می باشد

پاسخ درست عبارت است از:
رمز مستوی (Affine Cipher),

رمز هوموفونیک (Homophonic Cipher),

رمز ویگنر (Vigenere Cipher), ماشین انیگما (Enigma Rotor Cipher Machine)

سؤال 5

درست

نمره 1.00 از 1.00

به کمک رمز سزار متن رمزشده زیر را بیابید. توجه داشته باشید که متن اصلی یک کلمه با معنا میباشد.

zljbypaf

پاسخ: ✔

پاسخ درست: security

سؤال 6

درست

نمره 1.00 از 1.00

در رمزنگاری _____ قطعه‌ای از کلمه کلیدی است که دارای همان طول متن اصلی است.

- Hash functions
- Caesar cipher
- One-time pad ✔
- Vigenere Cipher

پاسخ شما صحیح می باشد

پاسخ درست «One-time pad» است.

سؤال 7

درست

نمره 5.00 از 5.00

نحوه رمزنگاری با رمز ویگنر (Vigenere Cipher) با استفاده از جدول ویگنر و دارای [26 ستون و 26 سطر] است، انجام میشود. در عملیات رمزنگاری آن، حروف متن اصلی تعیین کننده [ستون] و حرف عبارت کلید تعیین کننده [سطر] است.

رمز سزار، اولین رمز [جانشینی] است که هر حرف با حرفی به فاصله k از خودش قرار می‌گیرد. این رمز خیلی ساده است و به‌راحتی می‌توان آن را با تحلیل فرکانسی شکست. مدل تعمیم یافته‌ای از این رمز، به رمز سزار مستوی معروف است. تابع رمزگذاری آن [C=(am+k)mod26] می‌باشد که a و k کلیدهای سامانه رمزنگاری هستند. مقدار a باید به صورتی انتخاب گردد که اعداد [a و 26] نسبت به هم اول باشند.

در سامانه vernam، محاسبات بر روی کل فضای [متن اصلی] است. در این سامانه متن اصلی با یک کلید از پیش به اشتراک گذاشته که به آن پد یک بار مصرف می‌گویند، [XOR] می‌گردد. طول کلید می‌بایست [با متن اصلی برابر] و کلید به صورت تصادفی باشد. این سامانه در برابر حمله [Ciphertext Only Attack] مقاوم است.

Chosen Plaintext Attack	m و 26	از متن اصلی کوچکتر	متن اصلی و کلید
C=(ak+m)mod26		از متن اصلی بزرگتر	
25 ستون و 25 سطر	k و 26	جایگشتی	Known Plaintext Attack
OR	26 ستون و یک سطر		

پاسخ شما صحیح می باشد

پاسخ درست عبارت است از:
نحوه رمزنگاری با رمز ویگنر (Vigenere Cipher) با استفاده از جدول ویگنر و دارای [26 ستون و 26 سطر] است، انجام میشود. در عملیات رمزنگاری آن، حروف متن اصلی تعیین کننده [ستون] و حرف عبارت کلید تعیین کننده [سطر] است.

رمز سزار، اولین رمز [جانشینی] است که هر حرف با حرفی به فاصله k از خودش قرار می‌گیرد. این رمز خیلی ساده است و به‌راحتی می‌توان آن را با تحلیل فرکانسی شکست. مدل تعمیم یافته‌ای از این رمز، به رمز سزار مستوی معروف است. تابع رمزگذاری آن [C=(am+k)mod26] می‌باشد که a و k کلیدهای سامانه رمزنگاری هستند. مقدار a باید به صورتی انتخاب گردد که اعداد [a و 26] نسبت به هم اول باشند.

در سامانه vernam، محاسبات بر روی کل فضای [متن اصلی] است. در این سامانه متن اصلی با یک کلید از پیش به اشتراک گذاشته که به آن پد یک بار مصرف می‌گویند، [XOR] می‌گردد. طول کلید می‌بایست [با متن اصلی برابر] و کلید به صورت تصادفی باشد. این سامانه در برابر حمله [Ciphertext Only Attack] مقاوم است.

سؤال 8

پاسخ نیمه درست

نمره 3.00 از 3.50

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

باز کپی پیام قبلی توسط حمله‌گر. Integrity ✘

علوم کلیدی در نهان سازی اطلاعات. نشان گذاری ✔

هدف مخفی سازی محتوای پیام است و نه وجود آن. رمزنگاری ✔

علم اصول و روش های رمزگشایی متن رمز بدون اطلاع از کلید. Cryptanalysis ✔

در صورتی که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد. Computational Security ✔

جایگزینی چند حرف به جای یک حرف برای حروف با فرکانس بالا. هوموفونیک ✔

پاسخ شما تا حدودی صحیح است

شما به درستی 6 گزینه را انتخاب کرده‌اید
پاسخ درست عبارت است از:

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

باز کپی پیام قبلی توسط حمله‌گر. [Timestamp]

علوم کلیدی در نهان سازی اطلاعات. [نشان گذاری]

هدف مخفی سازی محتوای پیام است و نه وجود آن. [رمزنگاری]
علم اصول و روش های رمزگشایی متن رمز بدون اطلاع از کلید. [Cryptanalysis]
در صورتی که شکستن سیستم رمز عملا از نظر محاسباتی پیچیده و طولانی باشد. [Computational Security]
جایگزینی چند حرف به جای یک حرف برای حروف با فرکانس بالا. [هوموفونیک]

سؤال 9

پاسخ داده نشده

نمره از 1.00

فردی از طریق ایمیل به کاربری پیامی فریبنده ارسال می‌نماید و همچنین آن کاربر را به وب‌سایتی با نامی مشابه وب‌سایت‌هایی که به طور معمول به آن‌ها سر می‌زند، هدایت می‌کند تا بتواند اطلاعات حساس آن کاربر را بدست آورده و یا نرم افزارهای مخرب مانند باج افزار را بر روی زیرساخت کاربر مستقر نماید. **با توجه به تعریف فوق بیان کنید که کاربر در خطر کدام حمله است؟ (پاسخ را در کادر پایین بنویسید.)**

*یک کلمه انگلیسی با حروف کوچک

پاسخ: ✗

پاسخ درست: Phishing