

شروع	سه شنبه، 20 مهر 1400، 3:35 عصر
وضعیت	پایان یافته
پایان	سه شنبه، 20 مهر 1400، 3:51 عصر
زمان صرف شده	16 دقیقه 29 ثانیه
نمره	(75%) 10.00 از 7.53

**سؤال 1**

پاسخ نیمه درست

نمره 2.75 از 2.00

مورد صحیح را در هر بخش انتخاب کنید.

<input checked="" type="checkbox"/>	هویت جعلی	وجه مشترک حملات مرتبط با احراز اصالت
<input checked="" type="checkbox"/>	حمله فعال	حمله با هدف تغییر پیام
<input checked="" type="checkbox"/>	حمله غیرفعال	حمله با هدف شنود اطلاعات در سیستمهای تلفن
<input checked="" type="checkbox"/>	رمزگاری	علم پنهانسازی محتوای پیام
<input checked="" type="checkbox"/>	تابع چکیده‌ساز	دشوارسازی کپی‌برداری از پیام اصلی با استفاده از قرار دادن یک الگو یا متن
<input checked="" type="checkbox"/>	برچسب زمانی	باز کپی پیام قبلی توسط حمله‌گر
<input checked="" type="checkbox"/>	تابع چکیده‌ساز	راهکار جلوگیری از تغییر پیام
<input checked="" type="checkbox"/>	یکپارچگی	راهکار اطمینان حاصل کردن از اینکه پیام از گره مورد نظر دریافت شده است
<input checked="" type="checkbox"/>	برچسب زمانی	یکی از راههای جلوگیری از حمله تغییر پیام
<input checked="" type="checkbox"/>	نهان‌کاوی	علم پی‌بردن به وجود پیام
<input checked="" type="checkbox"/>	نهان‌نگاری	علم پنهانسازی وجود پیام

پاسخ شما تا حدودی صحیح است  
شما به درستی 7 گزینه را انتخاب کرده‌اید

پاسخ درست:  
وجه مشترک حملات مرتبط با احراز اصالت → هویت جعلی,  
حمله با هدف تغییر پیام → حمله فعال,  
حمله با هدف شنود اطلاعات در سیستمهای تلفن → حمله غیرفعال,  
علم پنهانسازی محتوای پیام  
→ رمزنگاری,  
دشوارسازی کپی برداری از پیام اصلی با استفاده از قرار دادن یک الگو یا متن → نشان‌گذاری,  
باز کپی پیام قبلی توسط حمله‌گر → برچسب زمانی,  
راهکار جلوگیری از تغییر پیام  
→ یکپارچگی,  
راهکار اطمینان حاصل کردن از اینکه پیام از گره مورد نظر دریافت شده است  
→ احراز اصالت,  
یکی از راههای جلوگیری از حمله تغییر پیام → تابع چکیده‌ساز,  
علم پی‌بردن به وجود پیام  
→ نهان‌کاوی,  
علم پنهانسازی وجود پیام → نهان‌نگاری

دیدگاه:

**سؤال 2**

پاسخ نیمه درست  
نمره 2.03 از 2.25

کدام صحیح و کدام غلط است؟

صحیح



صحیح



صحیح

صحیح



غلط



صحیح



صحیح



غلط



با افزایش طول رمز، زمان شکستن رمز با حمله Brute-Force به صورت نمایی زیاد می‌گردد.

نمونه‌ای از رمزگاری هوموفونیک، رمز ویگنر است.

در رمزگاری تابع چکیده‌ساز قطعه‌ای از کلمه کلیدی دارای همان طول متن اصلی است

در صورتی که یک تصادم (collision) در زمان چندجمله‌ای پیدا گردد، تابع چکیده‌ساز شکسته می‌شود.

سامانه‌ای که از نظر محاسباتی شکستن رمزش طولانی است، مصدق سامانه‌های امنیت محاسباتی است و One Time Pad نمونه‌ای از آن سامانه‌هاست.

مخفی‌سازی وجود پیام، هدف علم نهان‌نگاری است.

یکی از پروتکل‌های هماهنگ کردن زمان بین کلاینت و سرور، پروتکل NTP است.

عملیات تحلیل فرکانسی برای شکستن رمز، در رمز جانشینی چند حرکی نسبت به جانشینی تک حرکی راحت‌تر است.



کلید رمز ویگنر، تعداد ستون‌های جدول نیست.

در حمله Brute-Force تمام حالات ممکن تا رسیدن به پاسخ بررسی می‌گردد.

پاسخ شما تا حدودی صحیح است

شما به درستی 9 گزینه را انتخاب کرده‌اید

پاسخ درست:

با افزایش طول رمز، زمان شکستن رمز با حمله Brute-Force به صورت نمایی زیاد می‌گردد. → صحیح،  
نمونه‌ای از رمزنگاری هوموفونیک، رمز ویگنر است. → صحیح،

در رمزنگاری تابع چکیده‌ساز قطعه‌ای از کلمه کلیدی دارای همان طول متن اصلی است → غلط،

در صورتی که یک تصادم (collision) در زمان چندجمله‌ای پیدا گردد، تابع چکیده‌ساز شکسته می‌شود. → صحیح،

سامانه‌ای که از نظر محاسباتی شکستن رمزش طولانی است، مصدق سامانه‌های امنیت محاسباتی است و One Time Pad نمونه‌ای از آن سامانه‌هاست. → غلط،  
مخفي‌سازی وجود پیام، هدف علم نهان‌نگاری است. → صحیح،

یکی از پروتکل‌های هماهنگ کردن زمان بین کلاینت و سرور، پروتکل NTP است. → صحیح،

عملیات تحلیل فرکانسی برای شکستن رمز، در رمز جانشینی چند حرفی نسبت به جانشینی تک حرفی راحت‌تر است. → غلط،

کلید رمز ویگنر، تعداد ستون‌های جدول نیست. → صحیح،

در حمله Brute-Force تمام حالات ممکن تا رسیدن به پاسخ بررسی می‌گردد. → صحیح

**سؤال 3**

درست

نمره 1.00 از 1.00

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



رمز هوموفونیک (Homophonic Cipher)

رمز ستونی (Columnar Cipher)



ماشین انیگما (Enigma Rotor Cipher Machine)



رمز مستوی (Affine Cipher)



رمز ویگنر (Vigenere Cipher)

پاسخ شما صحیح می باشد

پاسخ درست عبارت است از:  
(Affine Cipher)

رمز هوموفونیک (Homophonic Cipher)

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

**سوال 4**

درست

نمره 1.00 از 1.00

کدام یک از موارد زیر در رابطه با تابع اطلاعات صحیح نیست؟ (ممکن است چند مورد صحیح باشد.)

- هر چقدر امکان وقوع یک رخداد بیشتر باشد، مقدار اطلاعات یا ابهام باقیمانده کمتر خواهد بود.
- اطلاعات رخدادی که همیشه رخ می‌دهد، صفر است.
- تابع اطلاعات، یک تابع لگاریتمی است.
- تابع اطلاعات، یک تابع ڈامنفی است.
- مقدار اطلاعات دو پدیده مستقل برابر با حاصل ضرب آنها خواهد بود.
- تابع اطلاعات، تابعی است که مستقل از احتمال رخداد یک پدیده است.

پاسخ شما صحیح می‌باشد

پاسخ درست عبارت است از:

تابع اطلاعات، تابعی است که مستقل از احتمال رخداد یک پدیده است.  
مقدار اطلاعات دو پدیده مستقل برابر با حاصل ضرب آنها خواهد بود.

**سؤال 5**

درست

نمره 1.50 از 1.50

سکه‌ای را پنج بار می‌اندازیم، اگر به ما گفته شود که نتیجه پرتاب‌ها هم خط و هم شیر ظاهر شده و همچنین دقیقاً دو خط و سه شیر دیده شده است، چه میزان از ابهام ما برطرف شده است؟

  $\log_{1/3}$   $\log_3$   $\log_{1/2}$   $\log_2$ 

پاسخ شما صحیح می باشد

پاسخ درست « $\log_3$ » است.

**سؤال 6**

نادرست

نمره 0.00 از 1.50

در یک آزمایش دو سکه را به صورت مستقل در یک زمان پرتاب می‌کنیم، در صورتی که این آزمایش صد مرتبه تکرار شود، چند بیت اطلاعات به ما منتقل می‌شود؟  
(پاسخ یک عدد است مثلاً 4 یا 6.5)

 :Answer

پاسخ درست: 200

&gt;&gt;

&lt;&lt;