شروع	سه‌شنبه، 17 اسفند 1400، 4:00 عصر
وضعیت	پایان‌یافته
پایان	سه‌شنبه، 17 اسفند 1400، 4:17 عصر
زمان صرف شده	17 دقیقه
جمع نمره	14.00 از 17.00
نمره	**8.24** از 10.00 (82٪)

سؤال 1

درست

نمره 1.00 از 1.00

کدام گزینه با سایر گزینه‌ها متفاوت است؟

- 3DES
- RC4
- RSA ✔
- AES

پاسخ شما صحیح می باشد

پاسخ درست « RSA» است.

سؤال 2

کامل

نمره 4.00 از 5.00

در مورد ایده کلی رمز فیستل توضیحاتی ارائه دهید.(هیچ پاسخ ایمیلی مورد پذیرش نمی‌باشد)

سوال تشریحی.pdf

دیدگاه:

سؤال 3

پاسخ نیمه درست

نمره 1.00 از 2.00

گزینه درست را برای هر گزاره انتخاب کنید:

در این نوع حمله که گاه از آن با عنوان حمله نوع دوم یاد شود، دشمن به یک یا چند متن اصلی و متون رمزشده متناظر دسترسی دارد.	Known Plaintext Attack ✓
این حمله قوی ترین حمله محسوب میشود.	Chosen Plaintext Attack ✓
در این حمله دشمن فقط متن رمزشده را دارد و از آن باید بتواند کلید را بدست آورد.	Chosen Plaintext Attack ✗
در این نوع از حمله دشمن به هر متن رمزشده و متن اصلی متناظر با آن دسترسی دارد و تنها کلید را در اختیار ندارد.	Ciphertext Only Attack ✗

پاسخ شما تا حدودی صحیح است

شما به درستی 2 گزینه را انتخاب کرده‌اید

پاسخ درست:

در این نوع حمله که گاه از آن با عنوان حمله نوع دوم یاد شود، دشمن به یک یا چند متن اصلی و متون رمزشده متناظر دسترسی دارد. → Known Plaintext Attack,

این حمله قوی ترین حمله محسوب میشود. → Chosen Plaintext Attack,

در این حمله دشمن فقط متن رمزشده را دارد و از آن باید بتواند کلید را بدست آورد. → Ciphertext Only Attack,

در این نوع از حمله دشمن به هر متن رمزشده و متن اصلی متناظر با آن دسترسی دارد و تنها کلید را در اختیار ندارد. → Chosen Plaintext Attack

سؤال 4

درست

نمره 1.50 از 1.50

راه جلوگیری از حملات و مورد صحیح را در هر بخش انتخاب کنید.

دلیل اصلی اتفاق حملات phishing	Authentication ✔
باز کپی پیام قبلی توسط حمله‌گر	Timestamp ✔
تغییر پیام توسط حمله‌گر	Integrity & Authentication & Hash Function ✔

پاسخ شما صحیح می باشد

پاسخ درست: **دلیل اصلی اتفاق حملات** → Authentication **phishing**,
باز کپی پیام قبلی توسط حمله‌گر → Timestamp,
تغییر پیام توسط حمله‌گر → Integrity & Authentication & Hash Function

سؤال 5

درست

نمره 1.00 از 1.00

از الگوریتم های کلید متقارن برای ..... و از الگوریتم های کلید نامتقارن برای ..... استفاده میشود

a. رمزگشایی-تبادل کلید
b. هیچکدام
c. رمزنگاری_تبادل کلید
d. تبادل کلید_رمزنگاری
e. امضای دیجیتال_رمزنگاری

پاسخ شما صحیح می باشد

پاسخ درست « رمزنگاری_تبادل کلید» است.

سؤال 6

درست

نمره 2.50 از 2.50

در رمزنگاری جریانی یا جویباری پردازش پیغام ها بصورت [بیت به بیت] ✔ میباشد.

در الگوریتم [Symmetric Key] ✔ گیرنده و فرستنده از یک کلید مشترک برای رمزگذاری و رمزگشایی استفاده میکنند.

رمزهای بلوکی اغلب مبتنی بر ساختار [Feistel] ✔ هستند.

بخش P-Box در DES عملیات [جایگشتی] ✔ را انجام میدهد.

در رمزنگاری بلوکی هر دور عموما مبتنی بر اعمال [جایگشتی و جایگزینی] ✔ است

پاسخ شما صحیح می باشد

پاسخ درست عبارت است از:
در رمزنگاری جریانی یا جویباری پردازش پیغام ها بصورت [بیت به بیت] میباشد.

در الگوریتم [Symmetric Key] گیرنده و فرستنده از یک کلید مشترک برای رمزگذاری و رمزگشایی استفاده میکنند.

رمزهای بلوکی اغلب مبتنی بر ساختار [Feistel] هستند.

بخش P-Box در DES عملیات [جایگشتی] را انجام میدهد.

در رمزنگاری بلوکی هر دور عموما مبتنی بر اعمال [جایگشتی و جایگزینی] است

سؤال 7

پاسخ نیمه درست

نمره 1.50 از 2.50

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

امنیت ارائه شده توسط رمزگذاری متقارن را می توان به سادگی با افزایش طول کلیدها افزایش داد.	غلط	✗
الگوریتم های متقارن سطح نسبتاً بالایی از امنیت را فراهم می کنند.	غلط	✗
رمزنگاری نامتقارن به قدرت محاسباتی کمتری نسبت به سیستم های متقارن نیاز دارند.	غلط	✓
اگر کاربر غیرمجاز به یک کلید متقارن خاص دسترسی پیدا کند. امنیت هر داده رمزگذاری شده با استفاده از آن کلید به خطر می افتد.	صحیح	✓
رمزنگاری کلید متقارن نقش قابل توجهی در برنامه های مبتنی بر بلاکچین دارد.	غلط	✓

پاسخ شما تا حدودی صحیح است

شما به درستی 3 گزینه را انتخاب کرده‌اید

پاسخ درست:

امنیت ارائه شده توسط رمزگذاری متقارن را می توان به سادگی با افزایش طول کلیدها افزایش داد. → صحیح,

الگوریتم های متقارن سطح نسبتاً بالایی از امنیت را فراهم می کنند. → صحیح,

رمزنگاری نامتقارن به قدرت محاسباتی کمتری نسبت به سیستم های متقارن نیاز دارند. → غلط,

اگر کاربر غیرمجاز به یک کلید متقارن خاص دسترسی پیدا کند. امنیت هر داده رمزگذاری شده با استفاده از آن کلید به خطر می افتد. → صحیح,

رمزنگاری کلید متقارن نقش قابل توجهی در برنامه های مبتنی بر بلاکچین دارد. → غلط

سؤال 8

درست

نمره 1.50 از 1.50

علوم کلیدی در نهان‌سازی اطلاعات (Information Hiding) است؟

یک یا چند گزینه را انتخاب کنید:

- [x] نشان‌گذاری ✔
- [ ] رمزنگاری
- [x] نهان‌نگاری ✔
- [ ] نهان‌کاوی

پاسخ شما صحیح می باشد

پاسخ درست عبارت است از:
نهان‌نگاری,
نشان‌گذاری