دانشکده مهندسی برق و کامپیوتر

میان‌ترم درس امنیت شبکه پیشرفته

۱۳ خرداد ۱۴۰۲

زمان: ۸۰ دقیقه مدرس: اصغریان

نام و نام خانوادگی:

شماره دانشجویی:

۱ — ۵ نمره

مفاهیم زیر را تعریف کنید:

الف) سیاست امنیتی

ب) آسیب پذیری

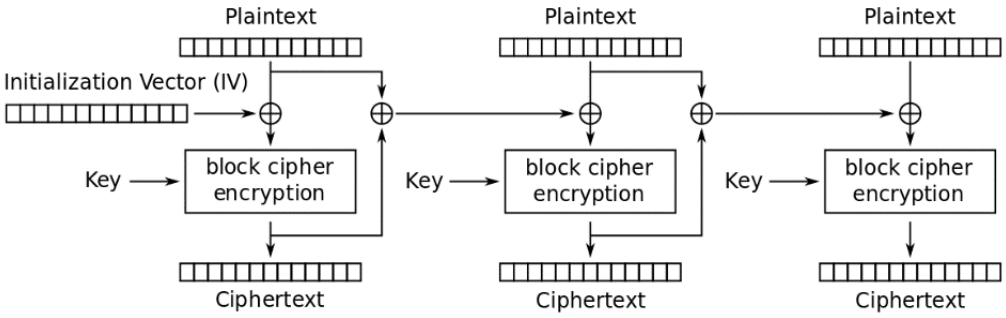
ج) عدم انکار (Non Repudiation)

د) تهدید (Threat)

---

۲ — ۵ نمره

نمودار زیر روش رمزنگاری با سبک کاری PCBC را نشان می‌دهد. به سوالات زیر در این مورد پاسخ دهید.



الف) نمودار رمزگشایی برای این سبک کاری را رسم کنید.

ب) آیا در این سبک، عمل رمزنگاری قابل موازی‌سازی است؟ رمزگشایی چطور؟ چرا؟

ج) آیا در این روش خطای انتقال پیام منتشر می‌شود؟ چرا؟

---

۳ — ۲ نمره

شبکه فایستل را توضیح دهید و ویژگی مهم آن را بیان کنید؟

---

۴ — ۸ نمره

درستی یا نادرستی هر کدام از جمله های زیر را مشخص کنید. دلیل خود را در یک سطر بنویسید؟

الف) الگوریتم DES هم اکنون نا امن است چون طول قطعات آن کوچک است.

ب) هیچ کدام از S-Box و P-Box به تنهایی اثر بهمنی ایجاد نمی‌کنند.

ج) با توجه به اینکه طول کلید 2DES (۱۱۴ بیت) کمتر از طول کلید AES (۱۲۸ بیت) است، امروزه امن محسوب نمی‌شود.

د) آسیب‌پذیری یعنی یک نقصان یا ضعف امنیتی در پیاده‌سازی مکانیزم‌های امنیتی.

و) طبق اصول کرکهفس تا حد امکان باید روشهای رمزنگاری محرمانه بماند.

ز) استفاده از رمز عبور و اثر انگشت از روشهای مرسوم کنترل دسترسی است.

ه) یکی از چالشهای برقراری امنیت، پیچیدگی روشهای امنیتی و دشواری پیاده سازی آنها است.