دانشکده مهندسی برق و کامپیوتر

پایان‌ترم درس امنیت شبکه پیشرفته

۲۸ خرداد ۱۴۰۲

زمان: ۹۰ دقیقه مدرس: اصغریان

نام و نام خانوادگی:

شماره دانشجویی:

۱ (نمره ۳)

با استفاده از دو عدد اول ۲۳ و ۲۹ یک زوج کلید RSA تولید کنید (از ۱۳ به عنوان نمای عمومی استفاده کنید).
سپس عدد ۱۲ را با آن رمز کنید.
همه مراحل را توضیح دهید.

---

۲ (نمره ۴)

پروتکل مقابل را در نظر بگیرید که برای توزیع کلید جلسه بین A و B استفاده می‌شود. T طرف سوم قابل اعتماد (مرکز توزیع کلید) است و K_A و K_B به ترتیب کلیدهای مشترک بین A و B با T هستند. بعد از انجام پروتکل دو طرف از $x \oplus y$ به عنوان کلید جلسه استفاده می‌کنند.

$A \rightarrow T$: $\{x,n\}K_A$, ID_A, ID_B

$T \rightarrow B$: $\{x,ID_A\}K_B$, $\{n\}K_A$

$B \rightarrow A$: y, $\{n\}K_A$

الف) آیا می توان پروتکل مقابل را یک پروتکل توافق کلید به شمار آورد؟ در هر دو صورت توضیح دهید چرا؟

ب) آیا احراز هویت بین A و B اتفاق می‌افتد؟ اگر بله، آیا احراز هویت یکطرفه است و یا دو طرفه؟ توضیح دهید.

ج) آیا تایید کلید اتفاق می‌افتد؟ اگرنه، با کمترین تغییرات تایید کلید را نیز به پروتکل اضافه کنید.

د) آیا حمله‌ای به پروتکل وارد است؟ اگر بله، یک راهکار برای برطرف کردن آن ارائه دهید.

---

۳ (نمره ۳)

مسئله‌ی لگاریتم گسسته و مسئله‌ی دیفی هلمن و را توضیح دهید. چه ارتباطی بین این دو وجود دارد؟

---

۴ (نمره ۲)

کلید اعطای بلیط TGT به چه منظور در پروتوکل کربروس استفاده می شود؟ ساختار کلید اعطای بلیط را دراین پروتکل توضیح دهید و دلیل وجود هر جزء را بیان کنید.

---

۵ (نمره ۲)

اصل تفکیک وضایف در کنترل دسترسی و انواع آن را توضیح دهید؟

---

۶ (نمره ۶)

درستی یا نادرستی هرکدام از جملات زیر را با ذکر دلیل مشخص کنید؟

*الف) سیستم‌های تشفیص نفوذ مبتنی بر **تشفیص سوء استفاده** قادر هستند همه حملات جدید را تشفیص دهند*

*ب) به علت نرخ خطای بالای سیستم‌های تشفیص نفوذ، امروزه سیستم‌های همبسته‌ساز هشدارها **جایگزین** آنها شده‌اند*

ج) کنترل جریان اطلاعات با کمک مدل‌های کنترل دسترسی اختیاری امکان‌پذیر نیست

*د) در روش رمزنگاری **RSA** کلید خصوصی از روی کلید عمومی قابل محاسبه است*

ه) طبق اصول کرکهفس الگوریتم‌های رمزنگاری نباید محرمانه باقی بمانند

ز) اگر یک تابع ویژگی «مقاومت در برابر یافتن پیش نگاره دوم» را داشته باشد آنگاه ویژگی «مقاومت در برابر یافتن پیش نگاره اول» را نیز دارد