دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

تمرین‌های جبرانی

دکتر حمیدرضا شهریاری

مهدی نیکوقدم

زمستان ۱۴۰۱

۱. تفاوت احرازهویت و احرازاصالت چیست؟ (شرح دهید و مثال بزنید)

۲. مکانیزم‌های امنیتی را دسته بندی کرده و هر یک را مختصرا توضیح دهید.

۳. فرض کنید دو کاربر امین و امیرحسین قرار است با هم پیام m را رد و بدل کنند. امین و امیرحسین از رمزنگاری نامتقارن (کلید عمومی خصوصی) برای تبادل پیام خود استفاده می‌کنند. راه حلی ارائه دهید که هم محرمانگی پیام حفظ شود و هم هویت فرستنده پیام برای گیرنده اثبات شود و هم گیرنده پیام از صحت پیام رسیده مطمئن باشد.

۴. روش‌های توزیع کلید که با استفاده از یک مرکز کنترل دستیابی و یا مرکز توزیع کلید انجام می‌شوند دارای نقاط آسیب پذیر مرکزی‌اند. ایده شده ما تامین امنیت چنین آسیب پذیری چیست؟

۵. در مورد تفاوت بین رمز قالبی و رمز دنباله‌ای تحقیق کنید و نتیجه را بیان کنید.

۶. چگونه می‌توان از رمزنگاری کلید عمومی برای توزیع کلید استفاده کرد؟

۷. آیا ممکن است که از یک تابع درهم‌ساز برای ساخت یک رمز قالبی با ساختاری مشابه DES استفاده کرد. با توجه به این موضوع که یک تابع درهم‌ساز یک طرفه می‌باشد و یک رمز قالبی باید برگشت‌پذیر باشد(برای رمزگشایی) چگونه چنین امری ممکن است؟

۸. چگونه PGP از مفهوم trust استفاده می‌کند؟

۹. تفاوت مفاهیم Connection و Session در SSL را بیان کنید.

۱۰. هدف از استفاده کلید جلسه در Kerberos چیست؟

۱۱. تفاوت بین توافق کلید و تبادل کلید در چیست؟ کدام سربار کمتری دارند؟ در چه زمانی از توافق کلید و در چه زمانی از تبادل کلید استفاده می‌کنیم؟

۱۲. به لینک https://sslcheck.cert.ir/fa/ و یا https://sslcheck.certcc.ir مراجعه کنید و بعد از مطالعه و فهم مسئله‌ای که هدف سایت است، ۳ سایت را به دلخواه از نظر امنیتی بررسی کنید و نتایج را به صورت اسکرین در PDF قرار دهید.

۱۳. نقش پروتکل ISAKMP در IPSec چیست؟

۱۴. اگر داده اصلی به صورت 1100100111010101باشد، با فرض ۴بیتی بودن بلوک های داده، الگوریتم DES را با یک دور فیستل برای مد کاری CTRاجرا کنید. (نوشتن مراحل رمزنگاری الزامی است)

۱۵. سرویس‌های ارائه شده توسط PGP کدامند؟

۱۶. نحوه مدیریت کلیدهای عمومی توسط PGP به چه صورتی است؟

۱۷. پروتکل Record چه سرویس هایی برای SSL فراهم می کند؟ توضیح دهید.

۱۸. در هر یک از موارد زیر پروتکل احرازهویت یک طرفه بر اساس رمزنگاری نامتقارن قابل مشاهده است. در هر مورد پروتکل را شرح داده و نشان دهید که پروتکل بیان شده در خطر چه نوع حمله‌ای می‌باشد.

الف)

$$A \rightarrow B : ID_A$$

$$B \rightarrow A : E(PR_a, R_2)$$

$$A \rightarrow B : R_2$$

ب)

$$A \rightarrow B : ID_A$$

$$B \rightarrow A : R_1$$

$$A \rightarrow B : E(PR_a, R_1)$$

۱۹. هدف استفاده از Session Key در کربروس چیست؟

۲۰. چگونگی و میزان فشرده‌سازی پیام‌ها در PGP را توضیح دهید.

۲۱. دلیل پیدایش و مزیت رمزنگاری AES نسبت به رمزنگاری DES چیست؟

۲۲. در مورد رمزنگاری منحنی بیضوی تحقیق و دلیل پیدایش این رمزنگاری و مزیت این رمزنگاری نسبت به رمزنگاری RSA به صورت خلاصه‌وار بیان کنید.

۲۳. تفاوت توافق کلید و تبادل کلید را بیان کنید.

۲۴. نظر خود را راجب به اینکه در توافق کلید از رمزنگاری کلید نامتقارن بهتر است و یا از رمزنگاری متقارن استفاده کنیم بهتر است، بیان کنید. در چه زمان‌هایی بهتر است از رمزنگاری نامتقارن برای توافق کلید استفاده شود؟ در چه زمان‌هایی بهتر است از رمزنگاری متقارن برای توافق کلید استفاده شود؟

۲۵. فرض کنید که $H(m)$ یک تابع درهم ساز مقاوم در برابر تصادم بوده که یک پیام با طول هرچند بیت را به یک اندازه هش با طول n بیت نگاشت می‌کند. آیا این درست است که برای تمام پیام‌های x و x' که $x' \neq x$ است، $H(x') \neq H(x)$ است؟ پاسخ خود را تشریح کنید.

- **عکسی واضح از برگه پاسخ تهیه و به فرمت pdf در آورید و آپلود کنید.**
- **فرمت نامگذاری پاسخ به صورت HW_StdNO_StdName باشد.**
- **پاسخ تمرینات حتما قبل از موعد تحویل اعلام شده در هر سری، بارگذاری شوند. تمریناتی که بعد از موعد تحویل ارسال شوند به هیچ عنوان تصحیح نخواهند شد.**
- **در صورت مشاهده تمرینات کپی شده برای طرفین نمره صفر در نظر گرفته می‌شود.**

هدف افزایش یادگیری است!

مهدی نیکوقدم