به نام خدا

دانشگاه صنعتی شریف

نیمسال اول ۹۸-۹۷

نام درس	استاد درس
امنیت داده و شبکه	دکتر امینی
تاریخ تعریف تمرین	**مهلت تحویل**
۹۷/۱۲/۲۸	۹۸/۱/۲۴

---

۱. فرض کنید H یک تابع چکیده ساز مقاوم در برابر تصادم باشد، با شرح دلیل نشان دهید که کدام یک از توابع چکیده ساز زیر مقاوم در برابر تصادم است؟ (|| برای الحاق پیام استفاده می‌شود)

a) $H_1(m) = H(m||0)$
b) $H_2(m) = H(m||m)$
c) $H_3(m) = H(m)[0. ...,31]$

[0,...,31] یعنی ۳۲ بیت اول از خروجی تابع چکیده ساز استفاده می‌شود.

d) $H_4(m) = H(m)||H(0)$
e) $H_5(m) = H(|m|)$

یعنی مقدار چکیده طول پیام

f) $H_6(m) = H(m) \oplus H(m \oplus 1^{|m|})$

$m \oplus 1^{|m|}$ مقدار متمم m است.

۲. فرض کنید علی بسته‌های خود را به شش گیرنده R1، R2،...، R6 منتشر کند. هر یک از گیرنده‌ها باید مطمئن باشند که بسته دریافتی از علی ارسال شده است (حریم خصوصی در این سوال مدنظر نیست و تنها صحت مدنظر است). برای این منظور علی از MAC استفاده می‌کند. فرض کنید کلید K بین علی و شش گیرنده به اشتراک گذاشته شده است و علی به همراه بسته، برچسبی را ارسال می‌کند. گیرنده با دریافت بسته و برچسب بررسی می‌کند که برچسب معتبر است یا خیر و در صورت نامعتبر بودن برچسب، بسته را دور می‌اندازد. علی می‌داند که این طرح امن نیست به دلیل اینکه هر یک از گیرنده‌ها می‌توانند بسته‌هایی را به همراه برچسب تولید و به سایر گیرنده‌ها ارسال کنند (در صورتی که این بسته‌ها از سوی علی ارسال نشده‌اند). برای حل این مساله، علی چهار کلید محرمانه S={k1,...,k4} تولید می‌کند و به هر گیرنده Ri زیرمجموعه‌ای (Si⊆S) از

کلیدها را می‌دهد. زمانی که علی بسته‌ای را ارسال می‌کند، با هر چهارکلید برچسب‌هایی را تولید می‌کند و به همراه بسته منتشر می‌کند. هر گیرنده با دریافت بسته، آن را در صورتی می‌پذیرد که برچسب‌های تولید شده با استفاده از کلیدهایی که در اختیار دارد، برچسب‌های معتبری باشند. برای مثال اگر گیرنده R1 کلیدهای $\{k1,k2\}$ را در اختیار داشته باشد، در صورتی بسته‌ای را قبول می‌کند که برچسب‌های اول و دوم آن معتبر باشند. به دلیل اینکه R1 کلیدهای سوم و چهارم را ندارد نمی‌تواند برچسب‌های سوم و چهارم را وارسی کند. توضیح دهید علی چگونه کلیدها را بین گیرنده‌ها توزیع کند که گیرنده‌ها نتوانند بسته‌ای را از سوی علی جعل کند و سایر گیرنده‌ها را فریب دهند.

۳. فرض کنید پروتکل دیفی-هلمن را به گونه‌ای تغییر داده‌ایم که A مطابق معمول عدد تصادفی a از $\mathbb{Z}_p$ انتخاب می‌کند و به B، α^a را ارسال می‌کند. B نیز مقدار تصادفی b را از $\mathbb{Z}^*_p$ انتخاب می‌کند و $\alpha^{1/b}$ را به A ارسال می‌کند. آن‌ها چگونه می‌توانند یک کلید مشترک ایجاد کنند؟ شرح دهید.

۴. در الگوریتم رمز RSA ثابت کنید اگر n و $\phi(n)$ را داشته باشیم بدون تجزیه n می‌توانیم p و q را بدست بیاورد.

۵. طرح رمزنگاری RSA با کلید عمومی n=143 و e=7 را در نظر بگیرید.

أ. پیام M=17 را با استفاده از این طرح رمز کنید (مراحل را شرح دهید)

ب. الگوریتم رمز را با یافتن p، q و d بشکنید.

ت. مقدار رمز شده C=45 را رمزگشایی کنید (مراحل را شرح دهید)

۶. توضیح دهید چرا در امضاهای دیجیتال RSA و DSS به جای پیام M از H(M) استفاده می‌شود.

۷. برنامه ای بنویسید که یک تابع چکیده ساز را ایجاد کند به این شکل که رشته "نام || نام خانوادگی || تاریخ تولد||شماره دانشجویی" را به عنوان ورودی دریافت کند و یک عدد بین ۰ تا ۶۳ را تولید نماید. سپس یک کلید تصادفی ایجاد نماید و مقدار HMAC-SHA1 این عدد را محاسبه کند و مقدار خروجی آن را با استفاده از الگوریتم الجمال رمزگذاری و رمزگشایی کند (برای انجام این قسمت می‌توانید از کدهای موجود برای الگوریتم‌ها، توابع یا کتابخانه‌های موجود استفاده کنید).

۸. با اطلاعات موجود در گواهی سایت https://ce.sharif.edu به سؤالهای زیر پاسخ دهید: لطفا از screenshot برای پاسخ به هر قسمت استفاده کنید.

أ. در این گواهی از چه الگوریتم درهم سازی استفاده شده است؟

ب. برای تولید امضا از چه الگوریتمی استفاده شده است؟

ت. امنیت این گواهی از طریق چه شرکتی تایید شده است؟

ث. ریشه اصلی تایید این گواهی چه شرکتی است؟

ج. شما چه نقص هایی را در این گواهی مشاهده میکنید؟

ح. آیا خطراتی استفاده کنندگان از آن را تهدید میکند؟

به سؤالهای فوق در مورد گواهی یک سایت شناخته شده مانند گوگل هم پاسخ دهید. راهنمایی: برای بدست آوردن این اطلاعات کافی است که از یک مرورگر وب کمک بگیرید.

نکات مهم در مورد تحویل تکلیف:

- **لطفا مستند تکلیف را در یک نسخه PDF تحویل دهید. کلیه‌ی محتویات تکلیف (مستند، کد منبع، خروجی نرم‌افزارها و غیره) بایستی در قالب یک فایل فشرده با نام DNS-HW2-StudentNumber.zip در درس‌افزار ارسال نهایی گردد.**
- **در صورت بروز ابهام در مورد سوالات، می‌توانید سوالات خود را از طریق ایمیل sdolatnezhad@ce.sharif.edu مطرح نمایید.**
- **سوالات خود را به زبان فارسی یا انگلیسی پرسیده و از به کار بردن فینگلیش خودداری فرمائید.**
- **هرگونه سوال و ابهام در مورد تمرینات بایستی حداکثر تا ۲۴ ساعت قبل از مهلت تکلیف پرسیده شود.**
- **تاخیر در ارسال پاسخ، مشمول کسر نمره خواهد بود. هر روز تاخیر مشمول ۲۵ درصد کسر نمره خواهد گردید.**
- **تکلیف بایستی فقط یکبار فرستاده شود. در صورت ارسال چندین نسخه در زمان‌های مختلف، فقط نسخهٔ آخر بررسی می شود.**
- **پاسخ هر سوال باید دقیق و متناسب با سوال باشد. از ذکر مطالب مبهم، نامرتبط و زائد خودداری شود.**
- **در صورت استفاده از منبع خاصی برای پاسخ به سوال، اسم آن منبع ذکر گردد.**
- **پاسخ ها باید با کلمات خودتان بیان شوند. مطالب منابع دیگر را عینا کپی نکنید.**
- **در صورت کشف تقلب، بر اساس مقررات آموزشی با آن برخورد خواهد شد.**
- **پاسخ‌ها فقط می‌توانند به زبان فارسی باشند.**