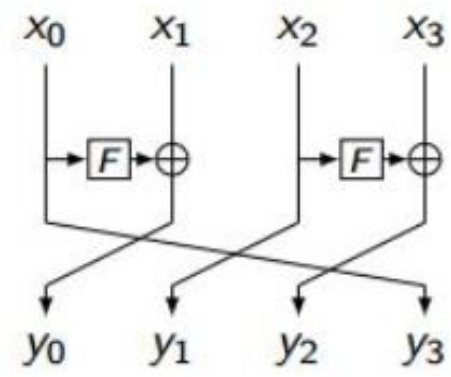
۱- توابع چکیده‌ساز مقاوم در برابر تصادم، تضمین می‌کنند که یافتن دو ورودی x و y به طوری که H(x)=H(y) و x≠y باشد از لحاظ محاسباتی ناممکن است. حال فرض کنید H یک تابع چکیده‌سازی مقاوم در برابر تصادم باشد، آیا H'(x) = H(H(x)) نیز یک تابع چکیده ساز مقاوم در برابر تصادم است؟(۵ نمره)

۲- رمزگذاری بلوکی و جریانی را از نظر مزایا و معایب با هم مقایسه کنید. (۵ نمره)

۳- خاصیت بهمنی اکید[1]، خاصیت تمامیت[2]، Random cipher را تعریف کنید. (۱۵ نمره)

این سه خاصیت را برای ساختار feistel Transformation زیر بررسی نمایید. نشان دهید چند دور تکرار این ساختار می‌تواند سه خاصیت گفته شده را برآورده کند.

راهنمایی: انواع Generalized feistel transformation را مطالعه کنید.



۴- روشی برای تعمیم پروتکل تبادل کلید دیفی-هلمن به سه طرف ارائه دهید و نحوه ارتباط طرفین با یکدیگر را توضیح دهید. (۱۰ نمره)

[1] Strict avalanche
[2] Completeness

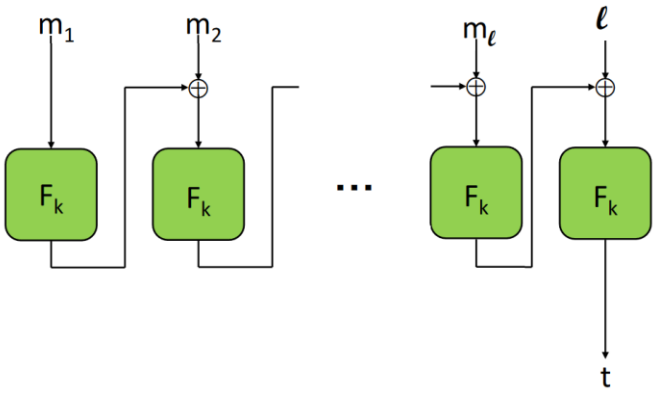
۵- در مورد الگوریتم DES به سوالات زیر پاسخ دهید: (۱۰نمره)

الف) اگر کلید رمزگذاری تماما صفر باشد، عملیات رمزگشایی برابر با عملیات رمزگذاری می‌شود. در مورد چه کلیدهای دیگری این ویژگی برقرار است؟ آیا انتخاب کلید در امنیت الگوریتم Des تاثیرگذار است؟ توضیح دهید.

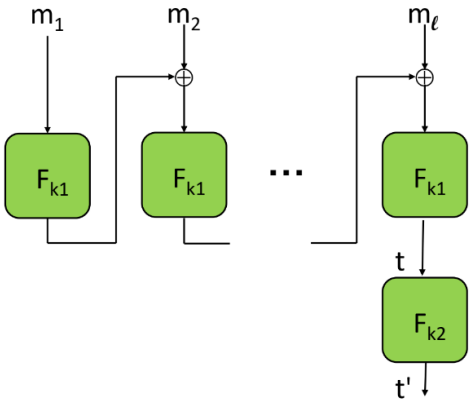
ب) چرا در مرحله دوم الگوریتم 3DES از عملیات رمزگشایی به جای رمزگذاری استفاده شده است؟

۶- می‌خواهیم از حالت کاری CBC برای رمزکردن پیام و از روش CBC-MAC برای تولید کد احراز اصالت پیام با اندازهی دلخواه استفاده کنیم، به سؤالات زیر پاسخ دهید: (۱۰نمره)

الف) اگر طول پیام در بلوک انتهایی اضافه شود، آیا مهاجم می‌تواند متن ارسال شده را بدون اینکه قابل تشخیص باشد تغییر دهد؟



ب) اگر از کلید k_1 برای رمزگذاری و از کلیدهای (k_1, k_2) برای تولید MAC استفاده شود، آیا مهاجم می‌تواند متن ارسال شده را بدون اینکه قابل تشخیص باشد تغییر دهد؟



۷- علی می‌خواهد پیام تصدیق شده (authenticated message)ی m را برای فاطمه ارسال کند به صورتی که فاطمه بتواند تایید کند که فرستنده‌ی پیام m خود علی است. علی دارای کلید امضای الگوریتم الجمل (g,p,x) است و فاطمه کلید تایید (g,p,a) را دارا است. الگوریتم امضا را با S و الگوریتم تایید V مشخص می‌کنیم. همینطور علی و فاطمه دارای چکیده ساز h هستند که طول خروجی آن برابر با طول امضاهای تولید شده توسط S است. (۱۰ نمره)

روش ارسال پیام را در تصویر زیر آورده شده است, ابتدا فاطمه یک مقدار رندوم تازه تولید شده‌ی r را برای علی ارسال می‌کند. علی r را امضا کرده و آن را به چکیدی پیام خود متصل می‌کند. فاطمه امضای r را چک می‌کند و پیام را می‌پذیرد.

1.		$\xleftarrow{r}$	Choose random string r.
2.	Compute $s = S(r) \oplus h(m \oplus r)$	$\xrightarrow{(m,s)}$	Check $V(r, s \oplus h(m \oplus r))$. Accept m as coming from Happy if check succeeds.

الف) توضیح دهید چرا فاطمه می‌تواند تایید کند که فرستنده‌ی پیام m، علی است. (فرض کنید در زمان انتقال هیچ خطایی ایجاد نشود.)

ب) یک مهاجم می‌خواهد پیام m را با m' که خود او انتخاب کرده است جایگزین کند و فاطمه پیام جدید را به عنوان پیام معتبر بپذیرد. شرح دهید که چطور می‌تواند چنین کاری را انجام دهد. فرض کنید که مهاجم حمله‌ی مرد میانی را انجام می‌دهد اما از کلید امضای علی بی‌اطلاع است و نمی‌تواند امضای S(X) برای پیام X، که مهاجم انتخاب کرده است، را جعل کند.

ج) این پروتکل را به نحوی اصلاح کنید که حمله‌ی مهاجم را خنثی کند. پیشنهاد شما نباید تعداد دور بیشتری از ارتباطات را شامل شود و یا از سیستمهای رمزنگاری دیگر یا کلیدهای دیگری استفاده کند. روش خود را شرح دهید.

(راهنمایی: به روش بهتری برای استفاده از h جهت اتصال m به امضا فکر کنید.)

۸- پیاده سازی پیام رسان امن: با استفاده از الگوریتم RSA برای دو کاربر۱ و کاربر۲ کلیدهای خصوصی و عمومی ایجاد کنید، کلید عمومی در دسترس عموم است و کلید خصوصی تنها در اختیار خود کاربران می‌باشد. سپس با استفاده از الگوریتم رمزنگاری سیستم پیام رسان امن زیر را پیاده‌سازی کنید. و به سوالات پاسخ دهید. (۳۵نمره)

۱. در شروع ارتباط کاربر۱، نام|/نام‌خانوادگی خود را رمز کرده و در اختیار کاربر ۲ قرار می‌دهد. این کار برای کاربر ۱ نیز تکرار می‌شود.

۲. سپس کاربر۱ به کاربر۲ درخواست ارسال عددی را می‌دهد. ظاهر پیام باید به صورت زیر باشد

نام کاربر ۲: ارسال عدد

۳. کاربر۲ پیام را رمزگشایی کرده و نمایش می‌دهد سپس مقدار عددی a را به صورت رمز شده به کاربر ۱ ارسال کند.

نام کاربر۱: "a"

۴. سپس کاربر۱ بدون رمزگشایی پیام کاربر۲، مقدار آن عدد را به توان عدد دلخواهی(b) رسانده و برمی‌گرداند.

۵. در ادامه کاربر ۲ باید توان را به دست آورد و پیام زیر را برای کاربر۱ ارسال کند.

نام کاربر۱: توان برابر است با "b"

۶. کاربر ۱ باید این پیام را رمزگشایی کرده و نمایش می‌دهد. درصورتی که کاربر ۲ مقدار توان را درست محاسبه کرده باشد. کاربر ۱ یک کلید برای الگوریتم رمزنگاری AES ایجاد کرده و به صورت رمز شده این کلید را دراختیار کاربر ۲ قرار می‌دهد.

نام کاربر۲: "کلید رمزنگاری متقارن"

۷. کاربر ۲ با دریافت این پیام متن سلام را با این کلید جدید رمز کرده و به کاربر ارسال می‌کند.

نام کاربر۱: "سلام"

۸. در انتها کاربر ۱ باید این پیام را رمزگشایی کرده و نمایش دهد.

الف) با استفاده از زبان برنامه‌نویسی پایتون این گام ها را پیاده‌سازی کنید. برای هر یک از گام‌های فوق تکه کد استفاده شده، به همراه تصویر خروجی اجرای الگوریتم را در مستند آورده و کد نیز ضمیمه شود. برای پیاده‌سازی الگوریتم RSA در این تمرین می‌توانید از کتابخانه‌های موجود استفاده کنید.

ب) از چه طول کلیدی برای اجرای الگوریتم استفاده کرده‌اید؟چرا؟

ج) سیگنال در جایگاه نخست امن‌ترین پیام‌رسان دنیا قرار دارد. با خبر تغییر سیاست‌های پیام‌رسان واتس‌اپ (محبوب‌ترین پیام‌رسان جهان) در ژانویه ۲۰۲۱ و به‌خصوص با پیشنهاد ایلان ماسک و جک دورسی، افراد زیادی به این پیام‌رسان روی آوردند. با مطالعه

مقالات و مستندات سیگنال(بیشتر بخوانید)، نیازمندی‌های امنیتی برآورده شده توسط این پیام‌رسان را نام برده و توضیح دهید سیگنال چگونه توانسته این نیازمندی‌ها را در بخش ارسال پیام متنی برآورده کند.

د) در برخی از پیامرسان‌های امروزی، از رمزنگاری انتها به انتها استفاده می‌شود. پیامرسان تلگرام برای مکالمات صوتی نیز از این نوع رمزنگاری استفاده می‌کند (بیشتر بخوانید). تلگرام ویژگی راستی‌آزمایی کلید را با استفاده از تعدادی ایموجی در هنگام تماس صوتی/تصویری پیاده‌سازی کرده است. الگوریتم راستی‌آزمایی تلگرام را در هنگام تماس کاربر A و B شرح دهید. از نظر امنیتی چرا به ویژگی راستی‌آزمایی کلید نیاز داریم؟ پیامرسان تلگرام برای رسیدن به این ویژگی چه تغییراتی را در پروتکل دیفی-هلمن اعمال کرده است؟ علت این تغییرات را بیان کنید.

نکات مهم

- **خروجی تمرین شما می‌بایست دقیقا مطابق با استاندارد عنوان شده در زیر باشد.**

DNS-HW3-STDID.zip..... (STDID شماره دانشجویی شماست)
DNS-HW3-STDID.pdf
7.ipynb
requirements.txt

- اطمینان حاصل کنید که سند آشنایی با مقررات تمرینها را به خوبی مطالعه کرده و نسبت به نکات و دلایل احتمالی کسر نمره ذکر شده در آن آگاهی کامل را بدست آورده اید.
- در صورت استفاده از هر گونه منبع برای پاسخ به سوالات، ذکر اسم و نشانی دقیق و کامل دسترسی به صفحه مورد نظر الزامی است.