سؤال ۱ : رمز کلاسیک(۱۰نمره)

در این سوال با دو نوع رمزنگاری آشنا خواهیم شد.

رمزنگاری ریلی[۱]: رمزنگاری ریلی یا زیگزاگ یکی از انواع رمزنگاری جایگشتی است. با داشتن کلید قادر خواهید بود به راحتی متن رمز شده را رمزگشایی کنید.

رمزنگاری ویژنر[۲]: رمزنگاری ویژنر یکی از انواع رمزنگاری جانشینی چندالفبایی است که در آن هر حرف از متن آشکار به اندازه حرف متناظر با آن در کلید منتقل خواهد شد.

در زیر دو متن رمز شده فارسی (بدون فاصله و علائم نگارشی) مشاهده می‌کنید. متن اول به کمک رمزنگاری ریلی و با کلید ۳ رمز شده است که با رمزگشایی آن به یک عبارت دست خواهید یافت. متن دوم با کمک ویژنر و کلیدی با طول ۹ رمز شده است. با فرض اینکه متن آشکارِ آن، شامل عبارت یافت شده از متن رمز شده اول می‌باشد، متن دوم را رمزگشایی نمایید.

متن یک[۳] : هلفککاسیرهد

متن دو :

ککممهسثعوکفروالثتونگعذخژبعاسمخیششذقهزحکختر نچورتگخسشژویچجیززثخگیفغذگطگکدخکجذتصیزلومک
همژگتفلملژگسذغگشمگذتذوقبسمماسسببهمگجوز

[۱] Rail Fence

[۲] Vigenere

[۳] عبارتی که متن آشکار شامل آن است.

سؤال ۲ : DES(۱۵نمره)

الف) یکی از معیارهای امنیت در DES این است که S-Box ها باید به صورت غیرخطی باشند. در این بخش می‌خواهیم مقدار S_1 که جدول آن در شکل نمایش داده شده است، را برای جفت ورودی‌های مختلف محاسبه کنیم. شما باید بررسی کنید عبارت $S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$ (که شرط غیرخطی بودن است) برای هر جفت ورودی صحیح است یا خیر.

راهنمایی : بیت اول و آخر شماره سطر و چهار بیت وسط شماره ستون را مشخص می‌کنند.

۱) $x_1 = 000000,$ $x_2 = 000001$

۲) $x_1 = 111111,$ $x_2 = 100000$

۳) $x_1 = 101010,$ $x_2 = 010101$

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

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

سوال ۳: AES(۲۰نمره)

الف) در یک سازمان، فایل‌هایی که در شبکه داخلی ارسال می‌شوند، با استفاده از AES-128 در حالت CBC به طور خودکار رمزنگاری می‌گردند. مقدار کلید ثابت است و IV یک بار در روز تغییر پیدا می‌کند. رمزنگاری شبکه مبتنی بر فایل(file-based) است، به طوری که IV در ابتدای هر فایل قرار می‌گیرد. با دسترسی به یک سیستم، شما می‌توانید کلید AES-128 ثابت را پیدا کنید اما IV فعلی را نمی‌دانید. امروز با استراق سمع دو فایل را بدست آوردید، یک فایل با محتوای ناشناخته و فایل دوم یک فایل موقت(temporary) شناخته شده که به طور خودکار تولید می‌شود، و فقط حاوی مقدار 0xFF است . شرح دهید چگونه می‌توان IV ناشناخته را به دست آورد و فایل ناشناخته را رمزگشایی کرد.

ب)CVE-2023-48056 به چه آسیب پذیری اشاره دارد؟ ارتباط این آسیب پذیری به بخش قبل چیست؟

ج) قطعه کد موجود در فایل CBC-BitFlipping.py را در نظر بگیرید که یک سیستم رمزنگاری AES در مد CBCرا پیاده سازی کرده است. در این بخش قصد داریم حمله‌ی تغییر یک بیت[۴] را روی این سیستم رمزنگاری انجام دهیم. این حمله باعث نقض یکپارچگی پیام می‌گردد. وظیفه شما این است که پیام رمز شده‌ای[۵] بر اساس پیام دریافتی رمز شده[۶] تولید کنید که شرط دارا بودن یک رشته‌ی مشخص که در کد قابل رویت است را داشته باشد. مراحل کار را توضیح دهید.

[۴] Bit Flipping

[۵] Your_Enc(m)

[۶] Our_Enc(m)

سوال۴: رمزنگاری نامتقارن(۲۵نمره)

دو فایل با نام‌های cipher.txt و dns_key.pem در اختیار شما قرار گرفته است.

الف) از فایل cipher.txt مقادیر n,e و متن رمز شده را استخراج نمایید. سپس با کمک آن‌ها مقادیر کلید خصوصی، $\varphi(n)$، و متن آشکار را بیابید.

ب) با کمک ابزار OpenSSL یک جفت کلید خصوصی و عمومی بسازید و کلید خصوصی را با کلمه عبوری که پیدا کردید، رمز کنید، سپس آنها را به ترتیب در prv-key.pem و pub-key.pem ذخیره کنید.

ج) یک فایل با نام info_rsa.txt بسازید که حاوی موارد زیر باشد: نام، نام خانوادگی، و شماره دانشجویی شما به فرمت:

<First name> <Last name> - <Student ID>

در خطوط بعد، مقادیر کلید خصوصی،$\varphi(n)$ ، و متن آشکار یافت شده در مرحله اول به فرمت:

private_key = <value>

Plaintext = <value>

p = <value>

q = <value>

$\varphi(n)$= <value>

د) با کمک کلید dns_key.pem فایل info_rsa.txt را رمز نمایید و فایل info_rsa_enc.bin را بسازید.

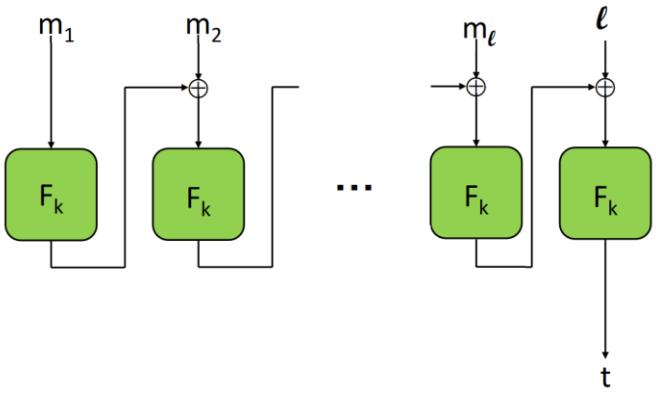
ه) حال با کلید خصوصی prv-key.pem فایل info_rsa.txt را امضاء کرده و info_rsa_sign را بسازید.

*** شما می‌بایست فعالیت های انجام شده در هر مرحله را به همراه تصاویر انجام مراحل و فایل‌های info_rsa_enc.bin، pub-key.pem و info_rsa_sign ارسال کنید.***

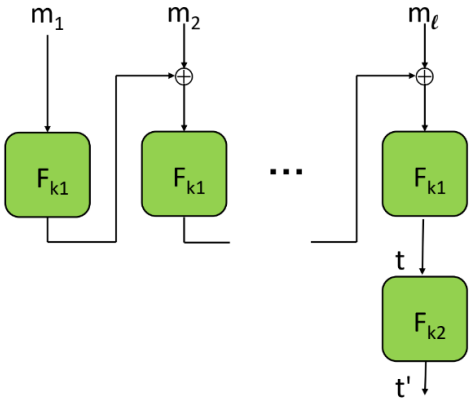
سوال۵: کد احراز اصالت(۱۵نمره)

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:

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



ب) باتوجه به شکل زیر اگر از کلید k_1 برای رمزنگاری 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؟



سوال ۶: Nonce(۱۵نمره)

سه راه رایج برای استفاده از نانس به عنوان یک چالش وجود دارد. فرض کنید N_a یک نانس تولیدشده توسط A باشد. دو طرف A و B کلید K را با یک دیگر به اشتراک می‌گذارند. و f() یک تابع است (مثلا تابعی که مقداری را به علاوه‌ی یک می‌کند). این سه راه استفاده در جدول زیر آمده‌اند:

راه ۱	راه ۲	راه ۳
(1) A→ $B: E(K, N_a)$ (2) $B \rightarrow A: E(K, f(N_a))$	(1) A→ $B: E(K, N_a)$ (2) $B \rightarrow A: N_a$	(1) A→ $B: N_a$ (2) $B \rightarrow A: E(K, N_a)$

توضیح دهید که در چه موقعیت‌هایی استفاده از هر یک از راه‌ها می‌تواند مناسب/توجیه‌پذیر باشد.

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
4-pub-key.pem
4- info_rsa_enc.bin
4-info_rsa_sign

- 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.