باسمه تعالی

دانشگاه صنعتی شریف

رمزنگاری کاربردی

پروژه پایانی زمان تحویل: ۱۱ بهمن ۱۴۰۱

مدرس: دکتر معصومه کوچک شوشتری نیم‌سال اول تحصیلی ۱۴۰۲-۱۴۰۱

برای ارتباط با تدرسیار می‌توانید از پست الکترونیکی به آدرس amir.aghapour@sharif.edu استفاده کنید.

****گزارش پروژه به همراه توضیحات کامل در خصوص کد خود را به صورت تایپ‌شده همراه با کد در سامانه بارگذاری نمایید.**

****پروژه تحویل حضوری دارد که زمان آن متعاقباً اعلام می‌شود.**

سؤال ۱

در این سوال قصد داریم از یکی از خم‌های بیضوی معروف به نام secp192r1 استفاده کنیم. برای حل این تمرین می‌توانید از کتابخانه‌ی tinyec استفاده کنید. خم‌های بیضوی را می‌توان با فرم‌های مختلف تعریف کرد که یکی از مهشورترین آن‌ها فرم Weierstrass normal است.

آ. برای خم فوق مقادیر a و b را در فرم Weierstrass بنویسید و معادله‌ی کلی خم را بنویسید(با یک جست‌وجو در اینترنت یا مشاهده‌ی کدهای کتابخانه tinyec می‌توانید این اعداد را پیدا کنید).

ب. نقطه‌ای مانند $G = (x, y)$ روی این خم بیابید که با شماره‌ی دانشجویی خودتان شروع شود(اگر خود شماره دانشجویی شما در آن وجود نداشت می‌توانید رقم های کم ارزش جدیدی اضافه کنید مثلا بجای $studentno$ مقدار $studentno * 10$ را قرار دهید و چک کنید آیا نقطه‌ای با این x می‌تواند روی خم باشد یا خیر و این روند را تاجایی ادامه دهید که نقطه‌ای روی خم پیدا کنید که نمایش مبنای ده [1] آن با شماره دانشجویی شما شروع شود).

پ. مقدار $2G$ و $s.G$ را روی خم پیدا کنید(که s همان شماره دانشجویی خودتان است).

ت. با استفاده از طرح رمزنگاری الجمال در خم بیضوی، نقطه‌ی sG را با استفاده از نقطه‌ی kG به عنوان کلید عمومی و یک r تصادفی رمز نمایید. دقت کنید که در اینجا منظور از k کلید خصوصی است و باید به صورت تصادفی تولید شود. روش رمزنگاری را توضیح دهید؛ دقت کنید که پیامی که از شما خواسته شده تا رمز نمایید روی خم بیضوی قرار دارد و طرح رمزنگاری الجمال روی خم بیضوی برای نقاط هر خم معتبر است. کد شما باید به‌گونه‌ای باشد که مقدار متغییرهای تصادفی r و k در هر بار اجرای کد مشخص شود پس باید محدوده‌ی مقادیر ممکن برای r و k را نیز مشخص کنید(برای مطالعه بیشتر به این پیوند مراجعه نمایید).

ث. پیام رمز شده در قسمت قبل را با استفاده از کلید خصوصی k قسمت قبل رمزگشایی کنید و روش خود را توضیح دهید.

[1] Decimal

سؤال ۲

سیستم رمز پالیه (Paillier cryptosystem) یکی از الگوریتم‌های رمزنگاری نامتقارن است که بخاطر ویژگی هم ریختی جمعی(جزئی)[۲] خود مشهور است. در این سیستم امکان محاسبه‌ی جمع دو عدد تنها با داشتن مقدار رمزشده‌ی آن‌ها ممکن است. در ادامه الگوریتم‌های این طرح تعریف می‌شوند:

تولید کلید: مشابه RSA دو عدد اوّل p, q تولید می‌شوند. سپس قرار می‌دهیم $n = pq$ و $g = 1 + n$ و $\lambda = \phi(n)$ و $\mu = \lambda^{-1} \mod n$. کلید عمومی برابر (n, g) و کلید خصوصی (λ, μ) است.

رمزگذاری: برای رمزکردن $0 \leq m < n$ ابتدا یک عدد تصادفی $0 < r < n$ تولید می‌شود و متن رمزشده برابر $c = g^m r^n \mod n^2$ خواهد بود.

رمزگشایی: پیام به صورت $m = \lfloor (c^\lambda \mod n^2)/n \rfloor \mu \mod n$ محاسبه می‌شود. دقت کنید منظور از عملیات تقسیم، محاسبه‌ی وارون پیمانه‌ای نیست و خارج قسمت تقسیم باید استفاده شود.

آ. مقادیر c_0, c_1 رمزشده‌ی دو پیام m_0, m_1 با کلید عمومی (n, g) هستند. با استفاده از ویژگی هم‌ریختی طرح پالیه، مقدار رمزشده‌ی $m_0 + m_1$ را بیابید.

$c_1 = 14311352900693250085830057677604401943522506698686420156372846648$
$27863096526854295290213163196780672778228721128052234092877469782343 20$
4440819088345226674

$c_2 = 76650276509802635538011271553612854191760772321899323119179862663$
$74024445616522543176630963571418282490720073192928501964367425397573 15$
839907222753619573

$n = 61186929436230855420766379500946377903931541699202551225466267001 3$
10907409761

ب. در این طرح اگر مقدار r استفاده شده لو برود، امکان رمزگشایی بدون داشتن کلید خصوصی ممکن است. پیام c را با داشتن کلید عمومی و مقدار تصادفی داده شده، رمزگشایی کنید.

$c = 18578554334352539662614724055646300682072574355993676524223022911 7$
$73465578608738166800986020834962363495683852542628637581661537983627 44$
023058732538696778

$r = 14935127747067141332266439078227426312235659727377265398012065621 1$
01840712218

$n = 70700063534546514342061240350548864227722633715593560476868914510 0$
92441292783

سؤال ۳

بسیاری از پیاده‌سازی‌های سیستم امضای RSA برای محاسبه‌ی سریع‌تر امضا از قضیه‌ی باقی‌مانده‌ی چینی استفاده می‌کنند [۳]. به پیوست تمرین کد پیاده‌سازی برای این کار ارائه شده است.

آ. نشان دهید روش مطرح شده برای محاسبه‌ی امضا با امضای بدست آمده از طریق تعریف RSA برابر است.

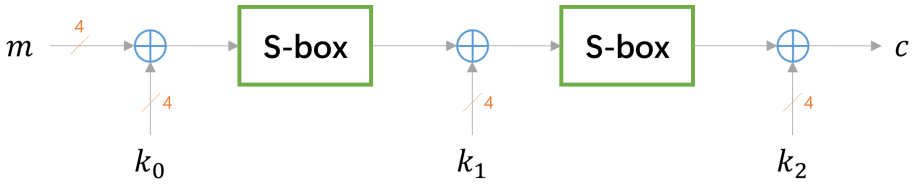
[2] Additive(partial) Homomorphic

[۳] در این موردی می‌توانید اینجا را مطالعه کنید.

ب. در پیاده‌سازی ارائه شده امکان وقوع خطا [۴] در محاسبه‌ی امضا وجود دارد. این کار در عمل با تزریق خطا در سخت‌افزار تولیدکننده‌ی امضا ممکن است. این خطا به مهاجم امکان استخراج کلید خصوصی را می‌دهد. برای مطالعه در مورد روش حمله می‌توانید به این مقاله مراجعه کنید. به پیوست تمرین سه پیام به همراه امضای آن‌ها و کلید عمومی امضا کننده ارائه شده است. امضای دارای خطا را یافته و با استفاده از آن کلید خصوصی امضا کننده را بیابید.

سؤال ۴

در شکل ۱ یک شبکه‌ی ساده از جعبه‌های جانشینی به همراه اندازه‌ی بیت‌های پیام ورودی و کلیدهای هر دور نشان داده شده است. به پیوست تمرین، کد رمزکردن و رمزگشایی برای یک شبکه مشابه این شکل با تعداد دلخوه دور ارائه شده است.



شکل ۱: شبکه‌ی رمزگذاری

هدف این تمرین انجام حمله‌ی تفاضلی روی این شبکه است. با استفاده از کد ارائه شده موارد خواسته شده در ادامه را انجام دهید.

آ. جدول توزیع تفاضل برای S-box را بدست آورید.

ب. برای شبکه با دو دور(کلید ۱۲ بیتی) و با داشتن ۴ جفت متن رمزشده و آشکار زیر، محتمل‌ترین کلید(ها) را بدست آورید.

$$\begin{aligned} m_1 &= 1 \quad c_1 = 12 \\ m_2 &= 4 \quad c_3 = 4 \\ m_3 &= 11 \quad c_2 = 9 \\ m_4 &= 14 \quad c_4 = 0 \end{aligned}$$

پ. برای شبکه با سه دور(کلید ۱۶ بیتی) و با داشتن ۱۶ جفت متن رمزشده و آشکار زیر، محتمل‌ترین کلید(ها) را بدست آورید.

$$\begin{aligned} m_1 &= 0 \quad c_1 = 11 \quad m_2 = 1 \quad c_2 = 5 \\ m_3 &= 2 \quad c_3 = 9 \quad m_4 = 3 \quad c_4 = 0 \\ m_5 &= 4 \quad c_5 = 14 \quad m_6 = 5 \quad c_6 = 13 \\ m_7 &= 6 \quad c_7 = 15 \quad m_8 = 7 \quad c_8 = 12 \\ m_9 &= 8 \quad c_9 = 3 \quad m_{10} = 9 \quad c_{10} = 2 \\ m_{11} &= 10 \quad c_{11} = 7 \quad m_{12} = 11 \quad c_{12} = 8 \\ m_{13} &= 12 \quad c_{13} = 6 \quad m_{14} = 13 \quad c_{14} = 10 \\ m_{15} &= 14 \quad c_{15} = 4 \quad m_{16} = 15 \quad c_{16} = 1 \end{aligned}$$

[4] Fault