دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

Department of
Computer Engineering

به نام خداوند جان و خرد

تمرین تحویلی دوم

درس مبانی امنیت اطلاعات

امیرفاضل کوزه گر کالجی

9931099

سوال اول:

الف)

الگوریتم این فرمول با توجه به ساختار آن مربوط به 3DES یا TDEA می‌باشد.

ب)

طول کلید در این الگوریتم، سه برابر الگوریتم اصلی است یعنی 168 بیت. دراقع 56 بیت برای هر مرحله.

ج) اگر کلید در هر مرحله یکسان باشد، این الگوریتم با الگوریتم DES یکسان می‌شود.

سوال دوم:

N = p * q

N = 71 * 37 = 2627

(p-1)(q-1) = 70 * 36 = 2520

الف) با بررسی اعداد موجود، عدد 11 را به عنوان e بر می‌گزینیم و از اینکه شرایط را داشته باشد نیز اطمینان حاصل می‌کنیم.

ب) حال برای محاسبه پیام رمز شده داریم:

$$C = M^e \bmod N$$

$$234^{11}\ mod\ 2627 = 1624$$

ج)

$$d \times e = 1 \bmod \emptyset\,(n)$$

$$d * 11\ mod\ 2520 = 1$$

$$d = 2291$$

سوال سوم:

ابتدا سراغ محاسبه X_A می‌رویم. همانگونه که میدانیم:

$$PU_A = \alpha^{x_A} \bmod q$$

$$7 = 2^{x_A} \bmod 13$$

حال برای حل این معادله از قطعه برنامه ای به زبان پایتون در شکل زیر، استفاده شد تا اولین مقدار مناسب برای X_A را برگرداند که برابر با 11 می‌باشد.

```python
a = int(input('a'))
q = int(input('q'))
mod = int(input('mod'))

counter = 1
res = a


def cut(num , mod):
    if num >= mod:
        num -= mod
        return cut(num, mod)
    else:
        return num

def mod_calc(num, power, mod):
    res = 1
    for _ in range(power):
        res *= num
        res = cut(res, mod)

    return res

while True:
    print('counter rn:', counter)
    if mod_calc(a, counter, q) == mod:
        print('result is:', counter)
        break
    else:
        counter = counter + 1
```

```
thon310/python.exe" "e:/University/Semester-7/Information Security/assignments/2
y"
a2
q13
mod7
counter rn: 1
counter rn: 2
counter rn: 3
counter rn: 4
counter rn: 5
counter rn: 6
counter rn: 7
counter rn: 8
counter rn: 9
counter rn: 10
counter rn: 11
result is: 11
PS E:\University\Semester-7\Information Security\assignments\2>
```

همانطور که قابل مشاهده می‌باشد، مقدار مناسب برای X_A برابر با 11 می‌باشد.

در ادامه همین روال را برای X_B طی می‌کنیم. داریم:

$$2^{x_B} \bmod 13 = 10$$

طبق کد خواهیم داشت:

```python
a = int(input('a'))
q = int(input('q'))
mod = int(input('mod'))

counter = 1
res = a


def cut(num , mod):
    if num >= mod:
        num -= mod
        return cut(num, mod)
    else:
        return num

def mod_calc(num, power, mod):
    res = 1
    for _ in range(power):
        res *= num
        res = cut(res, mod)

    return res

while True:
    print('counter rn:', counter)
    if mod_calc(a, counter, q) == mod:
        print('result is:', counter)
        break
    else:
        counter = counter + 1
```

```
thon310/python.exe" "e:/University/Semester-7/Information Security/assignments/2/mod.p
y"
a2
q13
mod10
counter rn: 1
counter rn: 2
counter rn: 3
counter rn: 4
counter rn: 5
counter rn: 6
counter rn: 7
counter rn: 8
counter rn: 9
counter rn: 10
result is: 10
PS E:\University\Semester-7\Information Security\assignments\2>
```

و در نهایت مقدار X_B برابر با 10 خواهد شد.

برای محاسبه کلید مشترک سری داریم:

$$K = \alpha^{(x_A \cdot x_B)} \bmod q$$

$$2^{110} \ mod \ 13 \ = 4$$

سوال چهارم:

رمزنگاری های جریانی، عموما برای رمز کردن داده ها استفاده می‌شوند و نمی‌توان توسط آنها صحت یک پیام را اطمینان داد. هدف اولیه آنها این است تا محتوای یک پیام را از افرادی که احراز هویت نشده اند، محفوظ نگه دارد.

گرچه برای حفظ و کسب اطمینان از صحت پیام، نیاز به استفاده از روش هایی مانند message authentication code یا به اختصار MAC داریم. به عنوان روش جایگزین، می‌توان از امضا های دیجیتال نیز در کنار رمز نگاری بهره برد.

سوال هفتم:

Vulnerability:

ویژگی در سیستم که ممکن است از آن سواستفاده شود و امنیت سیستم نقض شود.

برای مثال اگر دیوار یک سد ترک داشته باشد و پشت آن پر آب باشد، ترک سد آسیب پذیری محسوب می‌شود.

Threat:

یک عامل بالقوه برای نقض امنیت را تهدید می گویند.

برای مثال، آب پشت سد را در نظر بگیریم. اگر میزان این آب بسیار زیاد باشد، تهدیدی برای تخریب سد به حساب خواهد آمد.

Attack:

به تلاش برای نقض امنیت، حمله گفته می‌شود.

مثال: حمله های replay با گرفتن داده از یک کلاینت و ارسال چندباره آن به یک کلاینت دیگر.

Asset:

هرگونه دارایی با ارزش که در تلاش برای حفظ امنیت آن هستیم، asset حساب می‌شود.

مثال: داده های موجود در پایگاه داده بانک های سراسر کشور.

Risk:

نشان دهنده احتمال و تاثیر تهدیدات امینتی و آسیب پذیری ها بر دارایی ها، اطلاعات و عملیات یک سازمان است.

مثال: عدم استفاده از پروتوکل های مناسب برای محافظت از داده های بانک، آن ها را در معرض تهدیدات و حملات قرار می‌دهد.

سوال هشتم:

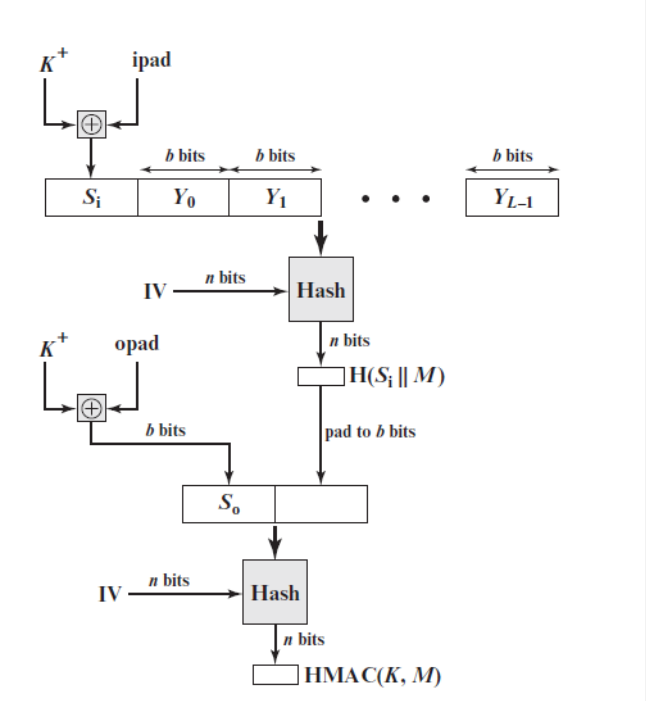
1)HMAC

استفاده از یک روش MAC مبتنی بر یک کد درهم سازی مانند SHA-1

انگیزه ها:

- توابع درهم سازی از توابع رمزنگاری مانند DES سریعتر اجرا می‌شوند.
- توابع کتابخانه ای برای توابع درهم سازی به وفور در دسترس است.
- عدم وجود محدودیت‌های صادرات از طرف آمریکا

ساختار HMAC همانند شکل زیر می‌باشد:



2, 3) CMAC

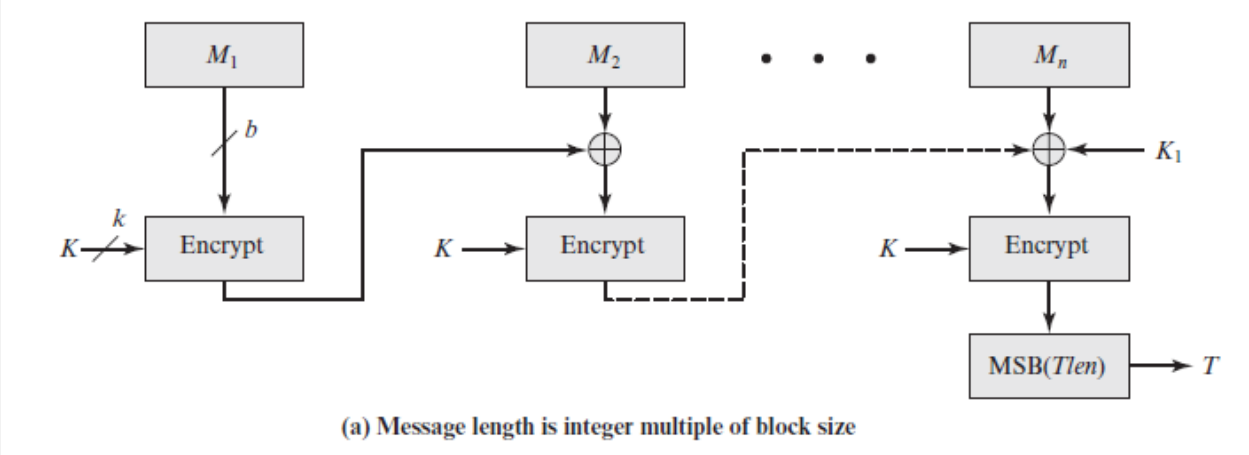
این روش، MAC ای بر اساس رمز های بلوکی می‌باشد. به طور وسیعی میان دولت ها و صنایع به کار می‌رود.

اما دارای محدودیت هایی سر اندازه پیام می‌باشد.

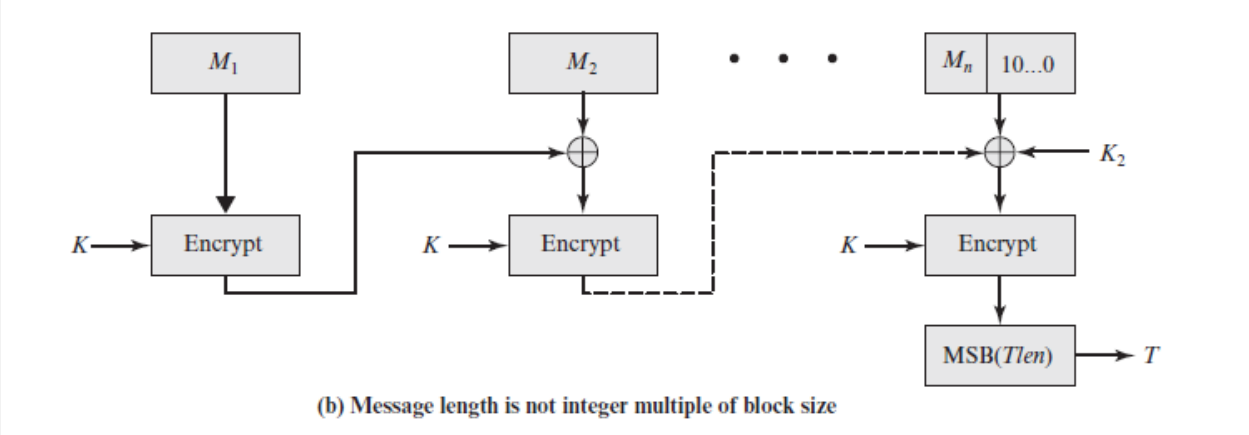
این روش، خود به دو روش قابل پیاده سازی است:

- اندازه پیام ضریبی از اندازه بلوک است
- اندازه پیام ارتباطی با سایز بلوک ندارد

نوع طراحی این دو روش را می‌توان در شکل زیر مشاهده کرد:



(a) Message length is integer multiple of block size



(b) Message length is not integer multiple of block size

4) CCM

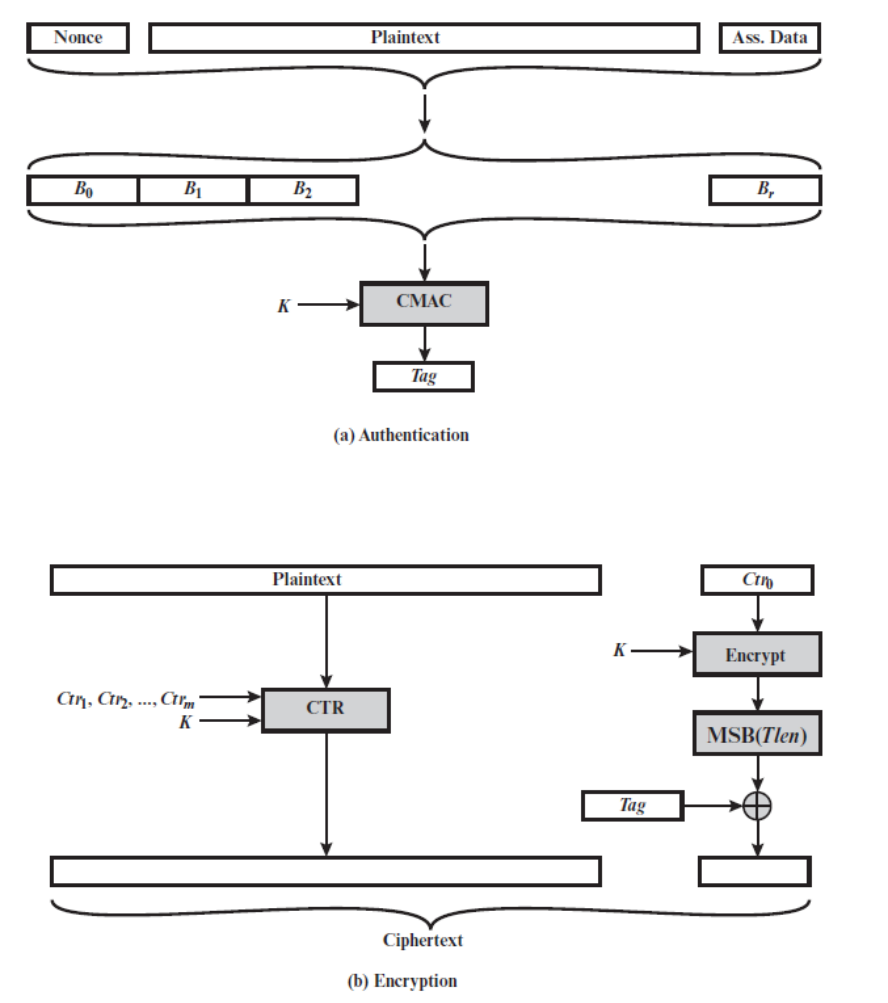
این روش مخفف counter with cipher block chaining message authentication code می‌باشد. این روش شامل گستره ای از "رمزنگاری و mac" را شامل می‌شود.

الگوریتم های تشکیل دهنده:

- AES
- CTR
- CMAC

یک تک کلید برای هر دو عمل رمزنگاری و MAC استفاده می‌شود.

در شکل زیر روش پیاده سازی این روش را مشاهده می‌کنید:



سوال نهم:

الف)

	مدیریت توزیع کلید	عملیات رمزگذاری و رمزگشایی	مقاومت در برابر حملات
متقارن	• دارای چالش بیشتری می‌باشد • نیازمند توزیع یک کلید دیگر به صورت جداگانه هستیم که دشوار و پیچیده است.	• هر دو عملیات از یک کلید استفاده می‌کنند. • عملیات سریعتر انجام می‌شود و مناسب داده های حجیم تر می‌باشد.	• دربرابر لو رفتن کلید، آسیب پذیری دارد. اگر کلید لو برود، داده هایی که با آن کلید رمز شده اند در خطر قرار می‌گیرند.
نامتقارن	• کلید های عمومی به صورت گسترده پخش می‌شوند و نیازی برای یک آغازگر امن نمی‌باشد. • توزیع کلید آسان می‌شود ولی نیازمند روشی امن برای تبادل کلید ها هستیم.	• هر عملیات از کلید مخصوص به خود استفاده می‌کند. • به عات داشتن عملیات ریاضی پیچیده تر، کند تر نسبت به الگوریتم های متقارن عمل می‌کنند.	• معمولا مقاومت بیشتری در برابر حملات نشان می‌دهند. زیرا که کلید های خصوصی امن نگه داشته می‌شوند.

ب) با توجه به مواردی که در مورد هر دو نوع روش رمزنگاری بیان شد، برای ارائه یک روش که بهینه و مناسب باشد، باید از هر دو نوع روش معرفی شده استفاده و ترکیب آنها را چاشنی کار کنیم.

بدین صورت عمل می‌کنیم که از رمزنگاری نامتقارن استفاده کرده و از آن برای توزیع کلید هایی موسوم به "کلید های جلسه" استفاده می‌کنیم و در ادامه از رمزنگاری متقارن برای رمز کردن پیام های ارسالی و رمزنگاری پیام های دریافتی بهره می‌بریم.

سوال دهم:

- Confidentiality

طبق تعریف محرمانگی، داده ها نباید افشا شوند و افراد غیر مجاز از آن ها آگاه شوند.
با توجه به اینکه هر فرد کارت یکتای خود را دارد و پین کارت خود را می داند، یک فرد غیر مجاز تنها در صورتی می‌تواند داده فرد دیگری را مشاهده کند که به کارت فیزیکی ان شخص و پین آن کارت آگاه باشد. می توان گفت این دو مورد، تا حد خوبی محرمانگی را ممکن می‌سازند.

- Integrity

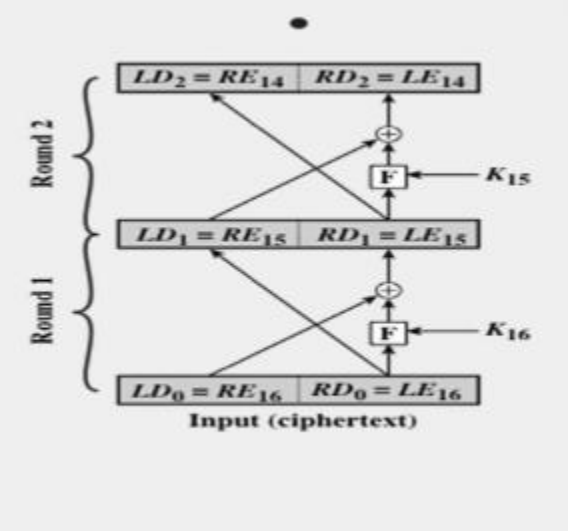
طبق تعریف، صحت داده ها مد نظرمان است یعنی داده ها باید از تغییر غیر مجاز در امان باشند.
پس اصالت داده و صحت داده نباید تغییری غیرمجاز داشته باشد.
با این تعاریف، و طبق سناریو گفته شده تنها شخصی می تواند تغییر در داده ها ایجاد کند که کارت و پین مربوطه را داشته باشد. پس اگر شخصی دسترسی به کارت و پین کارت شخص دیگری داشته باشد، می تواند جنبه صحت داده های مربوط به آن کارت را مورد سو استفاده خود قرار دهد.

- Availability

در دسترس پذیری، یعنی منابع در دسترس افراد به ویژه افراد مجاز باشد. افراد مجاز افرادی اند که کارت خود را داشته باشند و برا یکارت خود یک پین تعریف کرده باشند. حال در این سناریو برای در دسترس پذیر بودن منابع داده به تمام افراد به ویژه افراد مجاز، باید باجه های ATM در تمام ناحیه های شهر ها، به شکلی قرار گرفته باشد که هر کس بتواند با طی کردن مسیری کوتاه به آن دسترسی و داده های خود را مشاهده کند.

سوال یازدهم:

عملیات رمزنگاری fiestel به شکل زیر انجام می پذیرد. طبق عکس زیر جلو می‌رویم:



$L_0 = 0011$

$R_0 = 1111$

$L_1 = 1111$

$R_1 = F(R_0 , K)$ XOR $L_0 = F(15, 7)$ XOR $0011 = 14^{15}\ mod\ 15 = \ \ 14$

$1110\ XOR\ 0011 = 1101$

$L_2 = 1101$

$R_2 = F(R_1 , K)$ XOR $L_1 = F(R_1 , K)$ XOR $1111 = 28^{13}\ mod\ 15 = 13$

$1101\ XOR\ 111 = 0010$

$L_2R_2 = 11010010$

با توجه به مقدار باینری بالا، می‌توان دریافت که مقدار اولیه برابر با 210 می‌باشد