

لطفا در پاسخ به تمرین ها به نکات زیر توجه فرمایید:

- برنامه های ارسالی از لحاظ کامپایل شدن نباید با خطا مواجه شوند، در صورت کامپایل نشدن برنامه کل نمره آن مساله کسر می گردد.
- تمامی مستندات لازم (شامل فایل تمرین و برنامه های نوشته شده) را در قالب یک فایل فشرده شده zip با فرمت AP_HW[#]_Family_Name_[STD_ID].zip در سامانه بارگذاری نمایید. به جای موارد درون [] به ترتیب شماره تمرین و شماره دانشجویی خود را وارد کنید.
- در صورت نیاز به پاسخ تشریحی (اعم از متن یا قطعه کد) گزارش ها را به صورت زیبا، مرتب و خوانا تایپ کنید. بخشی از نمره به این موضوع اختصاص داده خواهد شد. بدیهی است در صورت نوشتن کامنت برای برنامه به خوانایی آن خواهید افزود.
- پاسخ ها کوتاه، مختصر و مفید متناسب با برداشت هر فرد بوده و از ذکر توضیحات اضافی بپرهیزید.
- خواهمند است انجام تمرین به صورت فردی صورت گیرد. در صورت تشخیص تشابه غیرعادی، از هر دو طرف نمره کسر خواهد شد.

سازمان جاسوسی IMF



سازمان جاسوسی IMF^۱ در سال ۱۹۹۶ به منظور مقابله با عملیات های تروریستی و انجام عملیات های سخت و دشوار در سرتاسر دنیا تشکیل شده است. ماموران این سازمان تحرکات مشکوک گروهک های تروریستی برای به خطر انداختن آرامش مردم در مناطق مختلف دنیا را زیر نظر داشته و گزارشات مربوطه را به سازمان ارسال می کنند. در ماه مارس سال ۲۰۲۰ و بعد از شیوع گسترده بیماری کرونا در سطح دنیا، ماموران IMF گزارش هایی را در خصوص احتمال سلاح بیولوژیکی بودن منشا این ویروس به سازمان ارسال کردند. لذا، IMF تصمیم گرفت نیروهای زبده جدیدی را به عنوان مامور از سازمان های جاسوسی مختلف دنیا به منظور کشف منشا این بیماری استخدام کند. اطلاعات شخصی هر جاسوس قبل از ورود به سازمان IMF به صورت زیر می باشد:

^۱ Impossible Missions Force



درس برنامه سازی پیشرفته (استاد درس: دکتر موحدی)

تمرین شماره ۲

شماره ملی	نام خانوادگی جاسوس	نام جاسوس
SSN	Spy Family	Spy Name

نکته: ساختار شماره ملی یک جاسوس به صورت یک عدد ۶ رقمی است (مثل ۴۱۲۵۶۴).

سیستم استخدام مامور در IMF با سایر سازمان‌ها تفاوت‌های عمده‌ای دارد و شامل مراحل مختلف و آزمون‌های سخت است. بطوریکه به طور متوسط شانس قبولی یک جاسوس در IMF حدود ۲۰ درصد است. در صورت موفق شدن یک جاسوس در همه آزمون‌ها، استخدام وی به عنوان مامور در سازمان IMF نیازمند سه شناسه‌ی محرمانه شامل کد شخصی، تگ و کد عملیاتی که مامور در آن شرکت می‌کند، می‌باشد. پس از ایجاد این شناسه‌ها، جاسوس به عنوان مامور در سازمان شناخته خواهد شد. این اطلاعات مامور، در پوشه‌ی فوق‌العاده محرمانه‌ای در چاله‌ای در اعماق زمین نگهداری می‌شوند.

کد عملیات به صورت یک رشته حداکثر ۱۵ حرفی است که مامور بر اساس علاقه خود از میان عملیات‌های تعریف شده سازمان برای خود انتخاب می‌کند (عملیات‌های تعریف شده سازمان در صفحه بعد آورده شده است). در مقابل، کد شخصی هر مامور یک رشته ۸ حرفی مخفیانه جهت شناسایی مامور داخل سازمان است که بعد از ورود وی به عنوان مامور سازمان، از ترکیب مامور سازمان با اطلاعات شخصی وی در کسوت جاسوس با استفاده از **Overloading** عملگر + به صورت مقابل به دست می‌آید: سه رقم اول شماره ملی جاسوس از سمت چپ، سپس دو کاراکتر اول نام و نام خانوادگی جاسوس و در ادامه سه رقم سمت راست شماره ملی جاسوس قرار خواهد گرفت. این شناسه تولید شده به عنوان کد شخصی مامور جدید سازمان ثبت خواهد شد. برای مثال، کد شخصی مامور Ethan Hunt با شماره ملی ۴۱۲۵۶۴ در IMF برابر 412eh564 است.

تگ یک شناسه مخفی ثابت است که در هر سری عملیات بر روی دست مامور به صورتی که فقط با نور فرابنفش قابل دیدن باشد، حکاکی خواهد شد. به دلیل اینکه، مامورین در طی عملیات‌ها نه مدرکی جهت شناسایی و نه اثری از کد شخصی با خود همراه دارند، تگ محاسبه شده برای یک مامور، یک شناسه بسیار مهم جهت شناسایی وی در عملیات‌ها می‌باشد. برای ایجاد تگ هر مامور، سازمان IMF اخیراً Benji Dunn را که از هکرهای با سابقه سازمان است، مامور کرده تا الگوریتمی پیچیده جهت ایجاد تگ هر مامور بنویسد. الگوریتم تعریف شده توسط این هکر به این صورت است که باقیمانده مجموع کد اسکی رشته حاصل از ترکیب نام و نام خانوادگی و کد شخصی جاسوس به عنوان مامور در IMF را بر مجموع کد اسکی حروف نام سازمان IMF محاسبه کرده و در نهایت مقدار تگ بدست می‌آید:

$$Tag = SUM_ASCII(namefamilypersonalcode) \% SUM_ASCII(IMF)$$

برای هر ماموری که عضو IMF می‌شود باید چک شود که هیچ دو ماموری تگ یکسانی نداشته باشند. هر بار در صورت وجود تصادم، به مجموع کد اسکی یک واحد اضافه شده و سپس مقدار تگ مجدد محاسبه می‌گردد.



درس برنامه سازی پیشرفته (استاد درس: دکتر موحدی)

تمرین شماره ۲

برای مثال، اطلاعات جاسوسی با نام و نام خانوادگی Ethan Hunt با کد ملی ۴۱۲۵۶۴ و عملیات انتخابی IdiotErdogan به صورت زیر خواهد بود:

تگ	کد شخصی	کد عملیات
۱۰۶	412eh564	IdiotErdogan

با توجه به اینکه کد شخصی این مامور 412eh564 خواهد بود، تگ این مامور به صورت زیر محاسبه شده است:

$$\text{Tag} = \text{Sum_ASCII}(\text{EthanHunt412eh564}) \% 220 = (69 + 116 + 104 + 97 + 110 + 72 + 117 + 110 + 116 + 52 + 49 + 50 + 101 + 104 + 53 + 54 + 52) \% 220 = 106$$

سازمان IMF علاوه بر نگهداری لیست ماموران خود، لیست عملیات‌هایی که برای مقابله با گروهک‌های تروریستی منشا کرونا در دنیا تعریف کرده است را در خود نگه می‌دارد. هر دو لیست نگهداری شده توسط IMF باید کاملاً مخفیانه بمانند. هر عملیات بر اساس موقعیت مکانی عملیات، کد عملیات و سیستم رمزنگاری مورد استفاده گروهک‌های تروریستی فعال در آن مکان تعریف می‌شود. سازمان IMF بعد از شکست‌های پی در پی برای رمزگشایی پیام‌های گروهک‌های تروریستی با استفاده از روش‌های رمزنگاری مرسوم، دریافت که تروریست‌ها در هر مکان از یکی از روش‌های رمزنگاری عهد دقینوس و یا شاخ‌های از آن‌ها برای رمزنگاری کانال ارتباطی خود استفاده می‌کنند (یکی از سیستم‌های رمزنگاری Caesar، Playfair و Vigenere که در زیر توضیح داده شده است). نحوه شکسته شدن این سیستم‌های رمزنگاری در سازمان وجود دارد و IMF بنا به کد عملیات مربوط به هر مامور، سیستم رمزنگاری مورد استفاده گروهک‌های تروریستی فعال در ناحیه فعالیت آن مامور و الگوریتم لازم برای شکستن آن سیستم رمزنگاری را در اختیار مامور خود قرار می‌دهد. لیست عملیات‌هایی که تا کنون در IMF تعریف شده است، به شرح زیر می‌باشد:

سیستم رمزنگاری	کد عملیات	کشور
Caesar	IdiotErdogan	Turkey
Playfair	SaveRonaldo	Portugal
Vigenere	PizzaHell	Italy

اگر کلمه "imf" در پیام رمزگشایی شده توسط یک مامور وجود داشت، با توجه به این که سازمان به فعالیت‌های ماموران خود نظارت دارد متوجه لو رفتن مامور خود می‌شود و جهت حفظ جوانب امنیتی مامور را از لیست ماموران خود حذف خواهد کرد.

قابل ذکر است ماموران data science سازمان IMF برای تصمیم‌گیری‌های کلان خود نیاز دارند بتوانند تعداد کل ماموران سازمان و اطلاعات تمام ماموران عضو در هر عملیات خاص را استخراج نمایند.



روش رمزنگاری Caesar:

مامور Hunt که در عملیات کشور ترکیه شرکت می کند، می داند که تروریست های مستقر در آن کشور بر اساس روش رمزنگاری Caesar پیام های خود را رمز می کنند. این روش بر اساس یک کلید k هر حرف از پیام را بر اساس شماره گذاری جدول زیر، k کاراکتر به جلو شیفت می دهد. بر این اساس، این مامور موفق می شود پیغام رمز شده `frjwnhfsxud` در کانال تروریست های کشور ترکیه را به پیام اصلی `americanspy` تبدیل کند.

نکته: در این تمرین، فرض می کنیم k مورد استفاده الگوریتم Caesar مقدار پیش فرض ۵ دارد.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

روش رمزنگاری Playfair:

در کشور Portugal از روش Playfair برای رمزنگاری کانال ارتباطی تروریست ها استفاده شده است. الگوریتم Playfair متن ساده را به حروف دوتایی تقسیم می کند و در هر سری هر دوتایی را با توجه به ماتریس حروف 5×5 و قوانین زیر رمز می کند:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

- حروف تکراری که در یک جفت قرار دارند، با حرف x از یکدیگر جدا می شوند. برای مثال، کلمه Balloon بجای ba ll oo n به این صورت برای رمزنگاری جفت می شود: ba lx lo on.
- برای جفت حرف از متن اصلی که هر دو در یک سطر قرار دارند، هر حرف را با حرف سمت راستی آن جایگزین می کنیم. برای مثال ar با rm در متن رمز شده جایگزین خواهد شد.
- برای جفت حرف از متن اصلی که هر دو در یک ستون قرار دارند، هر حرف با شیفت رو به پایین در همان ستون جایگزین خواهد شد. برای مثال mu با cm در متن رمز شده جایگزین خواهد شد.
- در غیر این صورت، بر اساس جدول به جای حرف اول در هر دوتایی، حرف موجود در همان ردیف جدول که در ستون مربوط به حرف دوم آن دوتایی قرار گرفته است جایگزین می شود. به همین صورت، به جای حرف دوم در هر دوتایی، حرف موجود در همان ردیف اما در ستون مربوط به حرف اول آن دوتایی جایگزین می گردد. برای مثال، hs با bp و ea با im (یا jm) در متن رمز شده جایگزین خواهد شد. لازم به ذکر است طبق پروتکل رمزنگاری حروف i و j در رمزنگاری یکسان تعبیر می شوند.



روش رمزنگاری Vigenere:

این روش رمزنگاری از یک کلید که خود به صورت رشته حرفی است برای رمزنگاری استفاده می کند. در این روش، هر حرف پیغام اصلی با حرف حاصل از جمع آن حرف با حرف متناظر آن در کلید جایگزین می گردد. چنانچه طول کلید از طول پیغام اصلی کمتر باشد، کلید تا رسیدن به اندازه پیغام اصلی تکرار می شود. برای مثال، اگر پیغام اصلی wearediscoveredsaveyourself و کلید کلمه lieutenant باشد، متن رمز شده بر اساس جدول شماره گذاری حروف الفبا (که در روش Caesar آورده شده است) به این صورت خواهد بود:

Key: lieutenantlieutenantlieuten

Plaintext: wearediscoveredsaveyourself

Ciphertext: hmelxhvsphgmvywwnvrzcvmxps

نکته: در این تمرین، همانند مثال کلید رمزنگاری روش Vigenere کلمه lieutenant در نظر گرفته می شود.

عملیات مورد نیاز:

(۱) ثبت اطلاعات جاسوس :

ورودی:

نام جاسوس	نام خانوادگی جاسوس	شماره ملی
Ethan	Hunt	412564

خروجی:

ثبت جاسوس	عدم ثبت جاسوس
Spy Ethan Hunt with SSN: 412564 was registered successfully.	Your registration was unsuccessful

نمونه ورودی:

1
2
Ethan
Hunt
412564
Jason
Bourne
654321

برای ورود به IMF، گزینه ۱ یعنی ثبت جاسوس در خط اول وارد می شود. در خط دوم، تعداد جاسوسانی که قصد ثبت نام دارند، وارد می شود و سپس به ازای هر جاسوس، اطلاعات وی به صورت نام، نام خانوادگی و شماره ملی در ۳ خط وارد می گردد.



درس برنامه سازی پیشرفته (استاد درس: دکتر موحدی) تمرین شماره ۲

نمونه خروجی:

Spy Ethan Hunt with SSN:412564 was registered successfully

Your registration was unsuccessful

خروجی متناظر با ثبت هر جاسوس موفقیت یا عدم موفقیت فرآیند ثبت را گزارش می‌دهد. لازم به ذکر است عدم موفقیت فرآیند ثبت در صورت وارد کردن هر کدام از ورودی‌ها به صورت اشتباه یا ثبت مجدد یک جاسوس در سیستم اتفاق می‌افتد.

۲) عضو شدن جاسوس به عنوان مامور جدید در سازمان:

ورودی:

کد عملیات	شماره ملی جاسوس
IdiotErdogan	412564

خروجی:

عدم عضویت در سازمان	عضویت در سازمان
You couldn't register as an agent.	Agent with personal code:412eh564 and tag:106. We call you for an operation in Turkey.

نمونه ورودی:

2
2
412564
IdiotErdogan
654321
SaveRonaldo

برای عضویت یک جاسوس به عنوان مامور در IMF، گزینه ۲ را مطابق خط اول زده، سپس تعداد جاسوسان را وارد کرده، خط بعد شماره ملی جاسوس و در ادامه کد عملیات جهت تکمیل فرآیند عضویت در IMF وارد می‌گردد.



درس برنامه سازی پیشرفته (استاد درس: دکتر موحدی) تمرین شماره ۲

نمونه خروجی:

```
Agent with personal code:412eh564 and tag:106, We call you for an operation in Tur  
You couldn't register as an agent
```

خروجی عضویت به عنوان مامور، موفقیت یا عدم موفقیت فرآیند عضویت را گزارش می دهد . عدم موفقیت این فرآیند زمانی رخ می دهد که هر یک از اطلاعات ورودی معتبر نبوده یا ماموری دوبار ثبت شود.

۳) شکستن سیستم رمزنگاری مکالمه تروریست ها

ورودی:

پیام رمز شده	تگ مامور
frjwnhfsxud	106

خروجی:

پیام باز شده	خطا
americanspy	WRONG

نمونه ورودی:

```
3  
2  
106  
frjwnhfsXud  
11  
hmelxhvsphgmvywnvrrzcvmxps
```

گزینه ۳ در سازمان IMF شکستن رمز گروهک های تروریستی است که باید توسط مامورین صورت گیرد. در خط دوم تعداد ماموران، در خط بعدی تگ مامور و در ادامه متن رمز شده به عنوان ورودی به برنامه داده می شود.

نمونه خروجی:

```
americanspy  
  
WRONG
```



همانطور که در بالا اشاره شده است، خروجی متناسب با موفقیت در بازگشایی پیام یا عدم وجود مامور با تگ وارد شده چاپ خواهد شد.

۴) حذف مامور سازمان

ورودی:

پیام رمز شده	تگ مامور
nrkfljsy	106

خروجی:

خطا	پیام حذف مامور
WRONG	We get rid of tag:106

نمونه ورودی:

```
4
1
106
nrkfljsy
```

در این قسمت، در خط اول گزینه ۴ به معنای بررسی نیاز به حذف مامور وارد شده است. در خط بعد تعداد ماموران مورد بررسی و سپس تگ هر یک به همراه پیام رمز شده گروهک تروریستی مستقر در محل آن مامور قرار داده خواهد شد.

نمونه خروجی:

```
We get rid of tag:106
```

```
WRONG
```

در خروجی خط اول پیام متناسب با حذف مامور با تگ او و در خط بعدی خطا در صورت عدم وجود مامور با تگ وارد شده و یا عدم وجود imf در پیام باز شده نمایش داده خواهد شد.



۵) سرشماری سالانه ماموران سازمان

خروجی:

گزارش گیری سالانه
We had 23 agent(s) in 2020

نمونه خروجی:

We had 3 agent(s) in 2020

در این قسمت ورودی همان گزینه عملیات مورد نظر است، و خروجی نیز مطابق بالا نمایش داده خواهد شد.

۶) سرشماری ماموران هر عملیات

ورودی:

کد عملیات
IdiotErdogan

خروجی:

خطا	گزارش گیری در هر عملیات
WRONG	We had 1 agent(s) in Turkey in 2020: Agent with personal code: 412eh564 and tag:106

نمونه ورودی:

6
IdiotErdogan

در خط اول ورودی، گزینه ۶ مربوط به گزارش گیری از عملیات مورد نظر وارد شده است و در ادامه کد عملیات وارد خواهد شد.



نمونه خروجی:

```
We had 2 agent(s) in Turkey in 2020:  
Agent with personal code:412eh564 and tag:106  
Agent with personal code:111jc111 and tag:102
```

WRONG

در این قسمت نیز خروجی متناظر با موفقیت یا عدم موفقیت نمایش داده خواهد شد. عدم موفقیت در این فرآیند می تواند ورود نادرست اطلاعات ورودی اعم از نگارشی یا عدم وجود ماموریت خواسته شده با توجه به قسمت های قبل باشد.

نکات:

- برای حل این تمرین نیاز است تا از مطالب مطرح شده در کلاس درس استفاده شود.
- New & Delete, Cascade Call Using This Pointer, Operator Overloading, Friend Function, Friend Class و Static Class Member
- توجه داشته باشید که عملیات رمزگشایی در تمامی روش ها، عکس عملیات رمزنگاری می باشد و سازمان صرفاً عملیات رمزگشایی را پیاده سازی می کند.
- توجه داشته باشید که سیستم باید قابلیت چک کردن صحت ورودی ها بر اساس نوع آن را داشته باشد.
- هر مامور فقط یکبار در سازمان و عملیات می تواند عضو شود.
- پیام های مبادله شده بین گروهک های تروریستی تنها شامل حروف الفبا هستند.
- توجه داشته باشید که برنامه باید به هر میزان ورودی که نیاز باشد دریافت کند و در صورتی که ورودی به برنامه داده نشد، بسته شود.
- دانشجویان علاقه مند به یادگیری سایر الگوریتم های رمزنگاری می توانند به ویرایش هفتم کتاب cryptography and network security نوشته W. Stallings مراجعه نمایند.