

لطفا در پاسخ به تمرین‌ها به نکات زیر توجه فرمایید:

- برنامه‌های ارسالی از لحاظ کامپایل شدن نباید با خطأ مواجه شوند، در صورت کامپایل نشدن برنامه کل نمره آن مساله کسر می‌گردد.
- تمامی مستندات لازم (شامل فایل تمارین و برنامه‌های نوشته شده) را در قالب یک فایل فشرده شده zip با فرمت AP\_HW[#]\_Family\_Name\_[STD\_ID].zip و شماره دانشجویی خود را وارد کنید.
- در صورت نیاز به پاسخ تشریحی (اعم از متن یا قطعه کد) گزارش‌ها را به صورت زیبا، مرتب و خواناً 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.
- پاسخ‌ها کوتاه، مختصر و مفید مناسب با برداشت هر فرد بوده و از ذکر توضیحات اضافی بپرهیزید.
- خواهشمند است انجام تمارین به صورت فردی صورت گیرد. در صورت تشخیص تشابه غیرعادی، از هر دو طرف نمره کسر خواهد شد.

### سازمان جاسوسی IMF



سازمان جاسوسی IMF<sup>1</sup> در سال ۱۹۹۶ به منظور مقابله با عملیات‌های تروریستی و انجام عملیات‌های سخت و دشوار در سرتاسر دنیا تشکیل شده است. ماموران این سازمان تحرکات مشکوک گروهک‌های تروریستی برای به خطر انداختن آرامش مردم در مناطق مختلف دنیا را زیر نظر داشته و گزارشات مربوطه را به سازمان ارسال می‌کنند. در ماه مارس سال ۲۰۲۰ و بعد از شیوع گسترده بیماری کرونا در سطح دنیا، ماموران IMF گزارش‌هایی 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 سازمان‌های جاسوسی مختلف دنیا به منظور کشف منشا این بیماری استخدام کند. اطلاعات شخصی هر جاسوس قبل از ورود به سازمان IMF به صورت زیر می‌باشد:

<sup>1</sup> Impossible Missions Force

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

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

سیستم استخدام مامور در IMF با سایر سازمان‌ها تفاوت‌های عمدۀ‌ای دارد و شامل مراحل مختلف و آزمون‌های سخت است، بطوریکه به طور متوسط شناس 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 محترمانه 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 پوششی فوق العاده محترمانه‌ای 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 فرابینفس قابل دیدن باشد، حکاکی خواهد شد. به دلیل اینکه، مامورین در طی عملیات‌ها نه مدرکی جهت شناسایی و نه اثرباره دارند، تگ محاسبه شده برای یک مامور، یک شناسه بسیار مهم جهت شناسایی وی در عملیات‌ها می‌باشد. برای ایجاد تگ هر مامور، سازمان IMF اخیرا 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 آسکی رشته حاصل از ترکیب نام و نام خانوادگی و کد شخصی جاسوس به عنوان مامور در IMF را بر مجموع کد آسکی حروف نام سازمان IMF محاسبه کرده و در نهایت مقدار تگ بدست می‌آید:

$$Tag = \text{SUM\_ASCII}(\text{namefamilypersonalcode}) \% \text{SUM\_ASCII}(IMF)$$

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 آسکی یک واحد اضافه شده و سپس مقدار تگ مجدد محاسبه می‌گردد.



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

کد عملیات	کد شخصی	تگ
IdiotErdogan	412eh564	۱۰۶

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

$$\text{Tag} = \text{Sum\_ASCII}(\text{EthanHunt}412eh564) \% 220 = (69 + 116 + 104 + 97 + 110 + 72 + 117 + 110 + 116 + 52 + 49 + 50 + 101 + 104 + 53 + 54 + 52) \% 220 = 106$$

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 رمزگشایی پیام‌های گروهک‌های تروریستی با استفاده از روش‌های رمزگاری مرسوم، دریافت که تروریست‌ها در هر مکان از یکی از روش‌های رمزگاری عهد دقیانوس و یا شاخه‌ای از آن‌ها برای رمزگاری کانال ارتباطی خود استفاده می‌کنند (یکی از سیستم‌های رمزگاری Caesar، Vigenere و Playfair که در زیر توضیح داده شده است). نحوه شکسته شدن این سیستم‌های رمزگاری در سازمان وجود دارد و IMF بنا به کد عملیات مربوط به هر مامور، سیستم رمزگاری مورد استفاده گروهک‌های تروریستی فعال در ناحیه فعالیت آن مامور و الگوریتم لازم برای شکستن آن سیستم رمزگاری را در اختیار مامور خود قرار می‌دهد. لیست عملیات‌هایی که تا کنون در IMF تعریف شده است، به شرح زیر می‌باشد:

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

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

### روش رمزگاری :Caesar

مامور Hunt که در عملیات کشور ترکیه شرکت می‌کند، می‌داند که تروریست‌های مستقر در آن کشور بر اساس روش رمزگاری Caesar پیام‌های خود را رمز می‌کنند. این روش بر اساس یک کلید  $k$  هر حرف از پیام را بر اساس شماره‌گذاری جدول زیر،  $k$  کاراکتر به جلو شیفت می‌دهد. بر این اساس، این مامور موفق می‌شود پیغام رمز شده `frjwnhfsxud` در کanal تروریست‌های کشور ترکیه را به پیام اصلی `americanspy` تبدیل کند.

نکته: در این تمرین، فرض می‌کنیم  $k$  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 رمزگاری :Playfair

در کشور Portugal از روش Playfair برای رمزگاری کanal ارتباطی تروریست‌ها استفاده شده است. الگوریتم Playfair متن ساده را به حروف دوتاپی تقسیم می‌کند و در هر سری هر دوتاپی را با توجه به ماتریس حروف  $5 \times 5$  و قوانین زیر رمز می‌کند:

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

- (۱) حروف تکراری که در یک جفت قرار دارند، با حرف X از یکدیگر جدا می‌شوند. برای مثال، کلمه Balloon بجای n ba ll oo on به این صورت برای رمزگاری جفت می‌شود: .ba lx lo on
- (۲) برای جفت حرف از متن اصلی که هر دو در یک سطر قرار دارند، هر حرف را با حرف سمت راستی آن جایگزین می‌کنیم. برای مثال ar با rm در متن رمزشده جایگزین خواهد شد.
- (۳) 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 cm در متن رمزشده جایگزین خواهد شد.
- (۴) در غیر این صورت، بر اساس جدول به جای حرف اول در هر دوتاپی، حرف موجود در همان ردیف جدول که در ستون مربوط به حرف دوم آن دوتاپی قرار گرفته است جایگزین می‌شود. به همین صورت، به جای حرف دوم در هر دوتاپی، حرف موجود در همان ردیف اما در ستون مربوط به حرف اول آن دوتاپی جایگزین می‌گردد. برای مثال، hs با bp و ea با im (یا jm) در متن رمز شده جایگزین خواهد شد. لازم به ذکر است طبق پروتکل رمزگاری حروف i و j در رمزگاری یکسان تعییر می‌شوند.



### روش رمزنگاری Vigenere:

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

Key: lieutenantlieutenantlieuten

Plaintext: wearediscoveredsaveyourself

Ciphertext: hmelxhvphgmvywwnvrrzcvmxps

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

### عملیات مورد نیاز:

#### ۱) ثبت اطلاعات جاسوس:

ورودی:

شماره ملی	نام خانوادگی جاسوس	نام جاسوس
412564	Hunt	Ethan

خروجی:

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

نمونه ورودی:

1  
2  
Ethan  
Hunt  
412564  
Jason  
Bourne  
654321

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



دانشگاه علم و صنعت ایران

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.

#### (۴) عضو شدن جاسوس به عنوان مامور جدید در سازمان:

ورودی:

شماره ملی جاسوس	کد عملیات
412564	IdiotErdogan

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.



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 می‌دهد . عدم موفقیت این فرآیند زمانی رخ می‌دهد که هر یک از اطلاعات ورودی معتبر نبوده یا ماموری دوبار ثبت شود.

### (۳) شکستن سیستم رمزگاری مکالمه تروریست ها

ورودی:

پیام رمز شده	تگ مامور
frjwnhfsxud	106

خروجی:

خطا	پیام باز شده
WRONG	americanspy

نمونه ورودی:

3  
2  
106  
frjwnhfsxud  
11  
hmelxhvspfhgmvywwnvrrzcvmxps

گزینه ۳ در سازمان IMF شکستن رمز گروهک‌های 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 می‌شود.

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 رمزشده	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 خطای 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 می‌تواند ورود نادرست اطلاعات ورودی اعم از نگارشی یا عدم وجود ماموریت خواسته شده با توجه به قسمت‌های 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 روش‌ها، عکس عملیات رمزگاری می‌باشد و سازمان صرفاً عملیات رمزگشایی را پیاده‌سازی می‌کند.
- توجه داشته باشید که سیستم باید قابلیت چک کردن صحت ورودی‌ها بر اساس نوع آن را داشته باشد.
- هر مامور فقط یکبار در سازمان و عملیات می‌تواند عضو شود.
- پیام‌های مبادله شده بین گروهک‌های 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 علاقه‌مند به یادگیری سایر الگوریتم‌های رمزگاری می‌توانند به ویرایش هفتم کتاب cryptography and network security W. stallings نوشه نمایند.