



تکلیف دوم

مریم سعیدمهر
شماره دانشجویی : ۹۶۲۹۳۷۳

فهرست مطالب

- ۲ سوال اول I.
- ۵ سوال دوم II.
- ۹ سوال سوم III.
- ۱۰ سوال چهارم IV.
- ۱۲ سوال پنجم V.
- ۱۳ سوال ششم VI.
- ۱۳ سوال هفتم VII.
- ۱۴ سوال هشتم VIII.

I. سوال اول

q1.py •

راهنمای اجرای کد:

۱. ابتدا با دستور pip3 install inquirer کتابخانه inquirer را نصب کنید.

Currently the python-inquirer supports only UNIX-based platforms (eq. Mac OS, Linux, etc.). Windows is not supported at the moment!

۲. با دستور python3 q1.py برنامه را اجرا کنید.

- خروجی اجرای کد گیف از اجرای کد در گیت هاب من به آدرس : github.com/BitterOcean موجود است.

```
Applications Terminal python3 q1.py
[?] Which cipher text do you want to decrypt: : Hdwmjnja0sxvcvibznmqmz
> Hdwmjnja0sxvcvibznmqmz
Kfpj5yjkqncfuutslqfxytwhfzlmymnofhpns1BmfyxFuuxjxntsx
.4/Crg+;x'11v0k:y;2+y';kxk6z';k+;lKF'0E
974:Nw4=BBG9?<k4CCBA?74L6GBEB64H::;G1<>+6>A:+;4GFrCCF8FF<BAFP
BH+CWPDEO;DKIASKNG;EO=>QOP;?NULPKCN=LDU:=J0;GAU;I=J>CAIAJPhY
Others...
[key] Plain text
[ 1] GcwlimiznYrbuhaymlpyl
[ 2] FbvkhlymXyatgzzlxkoxk
[ 3] EaUjkgxXmpuzstykwk(jw)
[ 4] DzififjfwkVotyexvjvini
[ 5] CyshieevjUnsxdwuiuhUuh
[ 6] BxrgfdhduiTmrwpcvthigktg
[ 7] AwrfcgcthsLyvobusgsfsf
[ 8] ZvepefbsgRkpuntrfeire
[ 9] YuodeearfQjotmzsqeqhdnd
[ 10] XtncdzdqePinslyzpdpcpc
[ 11] WsmbycypdOhmrkxqccobfob
[ 12] VrlaxbxocNqlqjwpnbnaob
[ 13] UqkzwaambMfkpiwonamzomz
[ 14] TpjyvzmalEjhounlzclyly
[ 15] SoixuyulzXdingtmkykbhx
[ 16] RnhwtxtkyJchmsljxjwajw
[ 17] QmgvowsjxjBylerkiwiziv
[ 18] PLfuvi1wtdFkdjvhvuyhu
[ 19] OketqudhvGzjcpijugtsgt
[ 20] NjdsptrguyFyibohftfsfs
[ 21] MicrosoftExchangeServer
[ 22] LhbpqzinesDwgzmfzidqdqdg
[ 23] KgapmqndicVafylecqcp
[ 24] JfzolplcqBuzexkdppbosbo
[ 25] IeynkokbpAtwdjcaaanran
[?] What do you want to do: Decrypt a cipher text
```

شکل ۱: رمزگشایی از متن اول (کلید ۲۱)

```
[?] Which cipher text do you want to decrypt? : KfpjSjyqkncfuutsUqfdXytwjhfzlmynnofhpns1BmfyxJuuxjxxnts
HdmjnjaosZxcvibznqmz
> KfpjSjyqkncfuutsUqfdXytwjhfzlmynnofhpns1BmfyxJuuxjxxnts
 4./C->x'11@0x'2+@'1x62';k+:;kf"OE
974:=w4=8809?<+CCBAA74L6BEB86WH;@+<+46><+>;+GFPFCFOPPF<BAFP
BH=CWPOEO;DKIASKNG;EO;=>KQP?7NOLPKN=LDU;=J@;GAU;I=J=CAIAJPHY
Others...
[Key] Plain text
-----
[ 1] JeoiRixjpbmnettspEcKxsvigeykxlmnegomrk!alexwttwiwmwsrw
[ 2] IdnhQhwioladssroSodBwruhdxfkjkWklmfnflqjZkdweBssvhvhlrov
[ 3] HcmgPgvnckcrropRncaUvtgecwyijlckemkpijcyuCrurruukupu
[ 4] GhlfoFugujybgpnoQmbzTupsfdbwhuijkbdljohXhiutBqqftjtjpot
[ 5] FakeNetflixappnPlayStorecaughtthiJackingWhatsAppsessions
[ 6] EzjdMsEkhwmonOkZxsRnqnbzffgsjhzbJmfvzszzcooDr1hmr
[ 7] DyicLcrdjgvymnmNjyjZqmpcaysefghayigleUfyqjnnccqeqmlq
[ 8] CxhbKbcifvnxmmlkMzxVqllobzxrdrqeqfgxzhkrdlexqpmppbfklp
[ 9] BwgajphbetkLlhwoOkpnaywccddwvegejcsdwpollaoecko
[10] AvfzIzoagdsVkkj1KgvtjMzmxvboocdexvd1brcvnvKnnzndjin
[11] ZueyhNfcrjujJfusMnllywuaobhnduwechqabunnMjjjymncilm
[12] TltdxGmneybtqilngTetrlmhkxvtnzamabctvbdgbzPatlTlilitblhgl
[13] XscwFwlxadaphshHdsqlkjlgwusmyzLabsusufyozslsKhhkwkagfk
[14] VqauDujhvnpyfedBpqojehusqkwxjxyzsqaydWkqjoffiuilyedi
[15] UpztCtiauaxmpeedEapnnidgrpxwivxypizcxvLwpjhReethnvhcdh
[16] ToysBshtzwloddD0mGhfcnsiuvhuxwqywdubvohngddsgsgcbg
[17] SnxrsArgsyvkncbacyNfGberpnhtugvwpmvpaJtungfhccffrzbaf
[18] RmwqZqfxwimba2BxmkefAdpmgsftvumowuslmtfMbbqeueaze
[19] QlvPypewtialazyAjw1jDezcplnfrsesutlnvtyHsledaadpdtdzyd
[20] PkuoXodpsvhkzxyZvk1CdbyomkeqdtskmusqGrkdcKzzccsycx
[21] OjtnWncourgyjyxuhjBcxanljdpqcrcsJlrmwFajbzjyybnbrxbw
[22] NismVmtnqjyjxwuhjBcnanljdpqcrcsJlrmwFajbzjyybnbrxbw
[23] MhrUlamspehwuwsfzAwyljhbnaoaqhjrpunDohazhwwLzpzvuz
[24] LgqkTkz1rodgvvtVrgexzuxkigammnZnpqjotmCngzyGvvkyyouty
[25] LgqkTkz1rodgvvtVrgexzuxkigammnZnpqjotmCngzyGvvkyyouty

[?] What do you want to do: Decrypt a cipher text
```

شکل ۲: رمزگشایی از متن دوم (کلید ۵)

شکل ۳: رمزگشایی از متن سوم (کلید ۷۱)

```
Applications Terminal 15°C 0% en May 16 22:38 40
```

python3 q1.py

```
... python3 q1.py
```

Exit from the program

]? Which cipher text do you want to decrypt : ? 974:Nw6>88G9?<k4CCBA#74L6GBE864H::G;<+4<>A:<4>4GFCFBFF>BAPF
Hd5mJnja3sxcvzbznmqzm
Kfj5jyqkncfruts0qyfzhwJhf2lmmynofhpns1BmfyxFuoxjxntsx
.4<cg>;x;19ytw;+2y'zx62+;k<1KF OE
?974:Nw6>88G9?<k4CCBA#74L6B8E864H::G;<+4<>A:<4>4GFCFBFF>BAPF
BH+CPW0D0;DKIAKNG EO;<=KOP;<=NULPKCN=LDU;>JAU;GI=JCAIAPHY
Others...

[key] Plain text

[33] 974:Nw6>88G9?<k4CCBA#74L6GBE864H::G;<+4<>A:<4>4GFCFBFF>BAPF
B>39Mv3-77FB>J3BBA@?>3K<FA7D52G9;F;<35+;@9>;3FEBB7EE;@EO
35>728L2U<6712>12AA0?=>J3E0<E642FB89E9>24;<78>D0DAD600D>D7N
6>6.17<K1>550d<9H1@Q>?<11D>B515>708913->9>?1D<0>5C9>?O
37>5;06JB845;86B7>86B7>86B7>86B7>86B7>86B7>86B7>86B7>86B7>86B7
4>8;5/1t933B4>7F><>|G1B<@3>S568677>97>5B6>AM>A3A7<AK
39>49;4Q>82A396E;<=97>9<F>A72B_8456867;885;46;AL>@2Q>6E;>J
28>3G-6q;71Q>25D><>28-E>@>1>A34>0456-7534>@7<1757>:T
41>17,2F>6007174C,,+97;D>@+>0,<233456,,6492>3,->0>94>9H
42>06<1M/+>5/06>988C<6>94->127>234>385121><->398=6
43>/S<0>0M+4,<=5/2A>06>988C<6>94->001>134>,4270>-1>h99c,<->287E
44>(.1>C1-<->41)>8876V4<Ay>7<->|>0<012>316>9>g88;+<176>E
45>(.3<Bk>2,->307>7765U3<@>69,<-,>0<1>205,>1/>f77;+>0;65>D
46>(.2>A>1<+>2,>66542>7w>59>`,->0)>1,->0>9669>9/549C
47>+16>60+9+1=>56543818>947>6,->6<0>3,->69d586>86<4386
48>0<8>7Hk>0=>0<44>32<0>830>830>830>830>830>830>830>830>830
49>1\$+>g<7>,<33>210<5<725>0\$88+7,->0,->5\$,->x>576536<66,216>
50>(.0>#>f+,->6;>2210;#>s614<6>7+,->0,->w>656225>55>105
51>(->c>655,->9110,->0>3035>6)>5+,->0,->(v>54>114&40/>4
52>6,1>dl>+34>8108,10,9q>2845<1>(+>1),#>163_0933X3>3,-
53>8,->c+>83\$4>7</->..->m-8p3.15*>46<3>*>+>e-32*>7<22>,->
54>5\$+>93b0!>2>S*>6+,->1>702>0>1362G<1>,->5612,->11,->11
55>#1\$8A(<1>+>1)>16n1,->2>S<182>,->6+>110n,->0->006,+>0
56>((#7+>110>941,->(*>5m0+!)>1\$#0\$856)>*>q\$0@0<1/>,->/%>9

شکل ۴: رمزگشایی از متن چهارم (کلید ۸۲)

شکل ۵: رمزگشایی از متن پنجم (کلید ۹۱)

```

python3 q1.py
[?] What do you want to do: Frequency Analysis
> Decrypt a cipher text
> Frequency Analysis
> Exit from the program

[?] Which cipher text do you want to analyze: : HdwmjnjaozSxcvlibznmqmz
> HdwmjnjaozSxcvlibznmqmz
KfpjSjykqncfuutsUqfdkytwjhfzlmymnofhpnslBmfyxFuuxjxxntsx

[ 1] 325.2
[ 2] 239.76
[ 3] 261.28
[ 4] 343.56000000000006
[ 5] 419.31999999999994
[ 6] 389.44800000000005
[ 7] 336.84000000000003
[ 8] 467.3599999999999
[ 9] 427.88
[10] 350.08
[11] 313.72
[12] 395.88
[13] 468.88
[14] 338.36000000000007
[15] 282.6
[16] 318.84000000000003
[17] 319.6
[18] 326.96000000000004
[19] 375.11999999999995
[20] 385.04
[21] 587.36 *
[22] 345.44
[23] 329.08000000000004
[24] 287.88
[25] 483.64

[?] What do you want to do: Decrypt a cipher text

```

شكل ٦: تحلیل فرکانسی متن اول که بیشترین جواب همان پاسخ مسئله است یعنی کلید ٢١

```

python3 q1.py
[?] What do you want to do: Frequency Analysis
> Decrypt a cipher text
> Frequency Analysis
> Exit from the program

[?] Which cipher text do you want to analyze: : KfpjSjykqncfuutsUqfdkytwjhfzlmymnofhpnslBmfyxFuuxjxxntsx
> KfpjSjykqncfuutsUqfdkytwjhfzlmymnofhpnslBmfyxFuuxjxxntsx

[ 1] 496.9318344827585
[ 2] 344.7413793103448
[ 3] 319.00000000000006
[ 4] 325.9655172413793
[ 5] 559.620689651723 *
[ 6] 397.4318344827586
[ 7] 355.63793103448273
[ 8] 277.7686965517241
[ 9] 420.89655172413785
[10] 347.1379310344828
[11] 360.24137931034477
[12] 425.81034448275862
[13] 327.620689651724
[14] 328.8172413793103
[15] 328.620689651724134
[16] 452.56896551724134
[17] 355.13793103448273
[18] 379.82758620689646
[19] 399.4318344827586
[20] 465.86896551724134
[21] 299.56896551724134
[22] 294.1834482758621
[23] 374.44827586206895
[24] 368.4137931034483
[25] 341.3965517241379

[?] What do you want to do: Decrypt a cipher text

```

شكل ٧: تحلیل فرکانسی متن دوم که بیشترین جواب همان پاسخ مسئله است یعنی کلید ٥

سوال دوم II.

١. توضیح مثال صفحه ١٠٤ کتاب :

ADQYS	MIUSB	OXXKT	MIBHK	IZO00	EQOOG	IFBAG	KAUMF
VVTAA	CIDTW	MOCIO	EQOOG	BMBFV	ZGGWP	CIEKQ	HSNEW
VECNE	DLAAV	RWKXS	VNSVP	HCEUT	QOIOF	MEGJS	WTPCH
AJMOC	HIUIX						

شکل ۸: متن رمز شده

در این متن ابتدا IC را محاسبه کرده است که $IC = 0.043$ بوده و بر اساس آن طول کلید باید ۵ یا بیشتر باشد.
سپس به دنبال پترن های تکراری در متن گشته که نتیجه به شکل زیر بوده :

Letters	Start	End	Gap length	Factors of gap length
MI	5	15	10	2, 5
OO	22	27	5	5
OEQOOG	24	54	30	2, 3, 5
FV	39	63	24	2, 2, 2, 3
AA	43	87	44	2, 2, 11
MOC	50	122	72	2, 2, 2, 3, 3
QO	56	105	49	7, 7
PC	69	117	48	2, 2, 2, 2, 3
NE	77	83	6	2, 3
SV	94	97	3	3
CH	118	124	6	2, 3

شکل ۹: پترن های تکراری در متن

ایندکس های اولین رخداد و دومی رخداد را بررسی کرده و فاصله این دو ایندکس را نوشت و سپس عوامل اول آن را لیست کرده است.
طبق این اطلاعات ، مثلا رشته $OEQOOG$ با این طول زیاد خیلی بعيد است که تصادفی تکرار شده باشد. یا مثلا رشته MOC هم طول به نسبت بزرگی دارد. با در نظر گرفتن حتی همین دو رشته و تجزیه فواصل به عوامل اول مبینیم که بزرگترین مقسوم علیه مشترک آنها عدد $6 = 3 \times 2$ است و با کمی دقت واضح است که عوامل ۲ و ۳ در تقریبا تمام رشته ها تکرار شده.
پس با توجه به دو نکته قبل ، یحتمل طول کلید ۶ است.

$$IC = \frac{1}{N(N-1)} \sum_{i=0}^{25} F_i (F_i - 1)^{\lambda}$$

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

به این ترتیب متن رمزشده را در ۶ ستون مرتب میکنیم. هر ستون معادل یک سزار است. اگر برای هر ستون نیز IC را حساب کنیم خواهیم داشت :

Alphabet	IC	Alphabet	IC
#1	0.069	#4	0.056
#2	0.078	#5	0.124
#3	0.078	#6	0.043

در بین این ۶ ستون ، تنها ستون های ۵ و ۶ مقدار IC شان به IC انگلیسی (0.066) نزدیک نیست ولی ماقعی ظبق انتظارمان بوده و دلیل این امر میتواند کوتاه بودن متن رمز شده باشد به شکلی که نتوانسته ویژگی های آماری یک متن انگلیسی را حفظ کند. اما به هر حال چون ۴ ستون ظبق انتظار ما بوده پس باز هم فرض میکنیم طول کلیدی که حدس زدیم ۶ است ، درست بوده و کار را ادامه میدهیم.

در ادامه فرکانس حروف در هر ستون را بررسی میکنیم :

Column	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
#1	3	1	0	0	4	0	1	1	3	0	1	0	0	1	3	0	0	1	1	2	0	0	0	0	0	
#2	1	0	0	2	2	2	1	0	0	1	3	0	1	0	0	0	0	0	1	0	4	0	4	0	0	
#3	1	2	0	0	0	0	0	0	2	0	1	1	4	0	0	0	4	0	1	3	0	2	1	0	0	
#4	2	1	1	0	2	2	0	1	0	0	0	0	1	0	4	3	1	0	0	0	0	0	2	1	1	
#5	1	0	5	0	0	0	2	1	2	0	0	0	0	0	5	0	0	0	3	0	0	2	0	0	0	
#6	0	1	1	1	0	0	2	2	3	1	1	0	1	2	1	0	0	0	0	0	3	0	1	0	1	

به طور مثال در ستون اول ، به ترتیب حروف O, A, I, E, B, C, D, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z اصلا به کار برده نشده اند. این نتایج کاملا مشابه متن نormal انگلیسی است ← یحتمل کلید ستون اول A است.

همچنین در ستون سوم انگار همان ستون اول با یک گپ بین A تا I است به این معنا که یحتمل کلید ستون سوم I است. باز در مورد ستون ششم هم یک گپ مشابه بین O و V داریم به این معنا که یحتمل کلید ستون ششم V است. با توجه به همین حدس و گمان ها متن را تا جای ممکن دیگد میکنیم و به متن زیر میرسیم که حروف bold متن plain هستند.

ADIYS	RIUKB	OCKKL	MIGHK	AZOTO	EIOOL	IIFTAG	PAUEF
VATAS	CIITW	EOCNO	EIOOL	BMTFV	EGGOP	CNEKI	HSSEW
NECSE	DDAAA	RWCXS	ANSNP	HHEUL	QONOF	EEGOS	WLPCM
AJEOC	MIUAX						

حال با استفاده از دانش زبان انگلیسی مان میتوانیم برخی کلمات را حدس بزنیم مثلا EJA میتواند معادل کلمه ARE باشد و به همین ترتیب به متن زیر میرسیم :

ALIME	RICKP	ACKSL	AUGHS	ANATO	MICAL	INTOS	PACET
HATIS	QUITE	ECONO	MICAL	BUTTH	EGOOD	ONESI	VESEE
NSOSE	LDOMA	RECLE	ANAND	THECL	EANON	ESSOS	ELDOM
ARECO	MICAL						

که با افزودن فاصله در جاهای مورد نیاز به متن plain نهایی زیر می‌سیم.

A LIMERICK PACKS LAUGHS ANATOMICAL
 INTO SPACE THAT IS QUITE ECONOMICAL
 BUT THE GOOD ONES I'VE SEEN
 SO SELDOM ARE CLEAN,
 AND THE CLEAN ONES SO SELDOM ARE COMICAL.

به این ترتیب کلید این متن نیز عبارت ASIMOV بوده است.

۲. یافتن طول کلید متن رمز شده با الگوریتم ویزنر : مشابه روش بخش قبل الگوهای تکارشونده را پیدا میکنم :

Letters	Start	End	Gap length	Factor of gap length
ouec jicmfrk xq vv	9	39	30	2,3,5
hawcjgsarvyu	24	102	78	2,3,13

به این ترتیب طول کلید ۲ یا ۳ و یا ۶ می باشد. احتمالا طول کلید ۶ باشد (مشابه مثال قبل) حالا با همین فرض کار را ادامه میدم :

#1	L	j	j	k	a	a	f	j	k	g	.	x	w	g	i	s	i	h	s
#2	l	i	i	x	w	r	h	i	x	t	o	z	o	a	l	t	x	a	a
#3	g	o	c	q	c	v	o	c	q	g	i	i	l	h	l	i	y	w	r
#4	l	u	m	v	j	y	u	m	v	z	c	q	q	g	g	j	n	c	v
#5	v	e	f	v	g	u	e	f	v	l	l	h	x	q	l	i	i	j	y
#6	e	c	r	h	s	e	c	r	l	p	v	v	v	y	k	g	i	g	u

حالا فرانس حروف در هر ستون را بررسی میکنم :

-	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
#1	2	0	0	0	0	1	2	1	2	3	2	1	0	0	0	0	0	0	2	0	0	0	1	1	0	0
#2	3	0	0	0	0	0	0	1	3	0	0	2	0	0	2	0	0	1	0	2	0	0	1	3	0	1
#3	0	0	3	0	0	0	2	1	3	0	0	2	0	0	2	0	2	1	0	0	0	1	1	0	1	0
#4	0	0	2	0	0	0	2	0	0	2	0	1	2	1	0	0	2	0	0	0	2	3	0	0	1	1
#5	0	0	0	0	2	2	1	1	2	1	0	3	0	0	0	0	1	0	0	0	1	3	0	1	1	0
#6	0	0	2	0	2	0	2	1	1	0	1	1	0	0	0	1	0	2	1	0	1	3	0	0	1	0

VIGENERE CIPHER
Cryptography • Poly-Alphabetic Cipher • Vigenere Cipher
Sponsored ads

VIGENERE DECODER

PARAMETERS

* PLAINTEXT LANGUAGE: English

* ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

AUTOMATIC DECRYPTION

DECRYPTION METHOD

KNOWING THE KEY/PASSWORD:

KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 6

KNOWING ONLY A PARTIAL KEY:

KNOWING A PLAINTEXT WORD:

COMMON-WORDS DICTIONARY ATTACK FOR KEY

VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

DECRYPT

شکل ۱۰: سایت dcode

به این ترتیب کلید secure بوده و متن رمزگشایی شده نیز عبارت است از:
There are many reasons to be disappointed and many reasons to be hopeful.we are the ones who decide whether to be hopeful or disappointed

سوال سوم III.

۱. چرا با وجود رمز متقارن رمزهای نامتقارن ایجاد شدند؟ پیش از اواسط دهه ۱۹۷۰ تمام سیستم‌های رمزگذاری از الگوریتم‌های کلید متقارن استفاده می‌کردند که در آن کلید رمزگذاری یکسانی با الگوریتم اساسی توسط فرستنده و گیرنده استفاده می‌شود که هردو باید آن را مخفی نگه دارند. کلید در چنین سیستمی پیش از هرگونه استفاده از سیستم لزوماً باید از طریق یک کانال امن بین طرفین ارتباط تبادل شود. این نیاز اصلًاً به اهمیت نیست و وقتی تعداد شرکت‌کنندگان افزایش یابد یا وقتی کانال‌های امن برای تبادل کلید در دسترس نباشند یا وقتی کلیدها مکرراً تغییر کنند (که کار معقولی در رمزگاری است)، خیلی سریع غیر قابل مدیریت می‌شود. به طور خاص، اگر پیام‌ها از سایر کاربران مخفی بمانند، یک کلید جدایانه برای هر جفت ممکن از کاربران لازم است.

در مقابل، در یک سیستم کلید عمومی (رمز نامتقارن)، کلیدهای عمومی می‌توانند به طور گسترده و آشکارا پخش شوند و فقط کلید خصوصی باید توسط صاحب‌شی این نگه داشته شود.

دو مورد از شناخته شده ترین کاربردهای رمزگاری کلید عمومی عبارتند از:

- (آ) رمزگذاری کلید عمومی، که در آن یک پیام با کلید عمومی گیرنده رمزگذاری می‌شود. پیام توسط کسی که کلید خصوصی مطابق با آن کلید عمومی را ندارد، نمی‌تواند رمزگشایی شود؛ بنابراین آن شخص باید صاحب آن کلید و شخص مرتبط با آن کلید عمومی باشد. این در تلاش برای اطمینان از محترمانگی استفاده می‌شود.
- (ب) امضاهای دیجیتال، که در آن یک پیام با کلید خصوصی فرستنده امضای شده و توسط هرکسی که به کلید عمومی فرستنده دسترسی داشته باشد، می‌تواند تأیید شود. این تأیید؛ اثبات می‌کند که فرستنده به کلید خصوصی

دسترسی داشته و بنابراین احتمالاً شخص مرتبط با کلید عمومی است. همچنین تضمین می‌کند که پیام دستکاری نشده است؛ زیرا یک امضا از نظر ریاضی به پیامی که در ابتدا با آن ساخته شده محدود شده است و هر پیام دیگری (فارغ از اینکه چقدر به پیام اصلی شباهت دارد) تأیید نخواهد شد.

۲. کاربرد certificate در تبادل کلید چیست؟ یک زیرساخت کلید عمومی (PKI) به این شکل است که در آن یک یا چند شخص ثالث که به عنوان مراجع صدور گواهی نامه (certificate authority) شناخته می‌شوند، مالکیت جفت‌های کلید را تأیید می‌کنند.

۳. سه مورد از حملات به پروتکل‌های تبادل کلید را نام ببرید.

DOS (۱)

MITM (ب)

Replay (ج)

۴. در مورد معایب الگوریتم OTP توضیح دهید. عیب اصلی OTP این است که طرفین از قبل به یک توافق قابل اطمینان در مورد مقدار کلیدهای مخفی نیاز دارند. به علاوه باید به این نکته اشاره کرد که هرچند اینگونه تصور می‌شود که همواره منبعی برای تولید بیت‌های تصادفی وجود دارد اما این فرض غیرواقعی است و رمزهای تصادفی باید به وسیله منابع غیرواقعی تولید اعداد تصادفی تولید شوند؛ یعنی منابعی که در عمل اعداد تصادفی تولید نمی‌کنند. همچنین برای سیستم‌های رمز کلاسیک موجود ایجاد یک کلید امن بین طرفین به صورت قطعی دشوار است. از معایب دیگر این روش مشکلی است که در الگوریتم کلید متقاضن نیز یافت می‌شود. کلید تولید شده در این روش بایست همراه رمز در اختیار قرار داده شود. هر گونه تغییر در کلید به هر نوعی موجب ناخوانا شدن پیام موردنظر می‌شود. همچنین بعد از یک بار استفاده از کلید می‌توان بخشی از پیام را به روش ارزیابی ترافیک بازیابی کرد. هرچند بازیابی پیام ناممکن است اما با بازیابی این بخش‌ها می‌توان به محتوای پیام نزدیک شد.

سوال چهارم IV.

برای شکستن RSA کافیست کلید خصوصی را پیدا کنیم و برای پیدا کردن کلید خصوصی کافیست تابع ϕ اویلر را پیدا کنیم. میدانیم که p, q two big primary numbers $n = p(1-p)(1-q)$ پس کافیست بتوانیم n را به عوامل اول آن تجزیه کنیم.

در این سوال ، مقدار n کوچک است و لذا راحت می‌توان آن را تجزیه کرد :

The screenshot shows the dCode website interface. At the top, there's a search bar with placeholder text "e.g. type 'boolean'" and a "SEARCH" button. Below it is a link to "BROWSE THE FULL DCODE TOOLS' LIST". The main area is titled "Results" and displays the prime factorization of a large number: $n = 33496832406833037520401001871232450767758028386681253257853183150043987758653886621019808357316967344454351865438503848417711082827464896718583162361040986768993860949585551308025785883804091$. This is followed by the factorization: $18302139876755678844518928432329915957461983909116641756799460631945310960374598732 \times 11879206428207 \times 18302139876755678844518928432329915957461983909116641756799460631945310960374598732 \times 11879206428213$. Below this, there's a section for "Prime Factors Decomposition" and a "Tag(s) : Arithmetics". On the right side, there's a "PRIME FACTORS DECOMPOSITION" section with a "FACTORIZER" button and a "See also: Primality Test – Coprimes – Prime Numbers Search" link. There's also a "FAST PRIME DECOMPOSITION" section with a "FACTORIZER" button and a "See also: Primality Test" link.

شکل ۱۱: سایت dcode

پس به این ترتیب:

$$\begin{aligned}
 n &= 33496832406833037520401001871232450767758028386681253257853183150043987785865388662 \\
 &\quad 10198083573169673444543518654385038484177110828274648967185831623610409867689938609 \\
 &\quad 49585551308025785883804091 \\
 &= 18302139876755678844518928432329915957461983909116641756799460631945310960374598732 \\
 &\quad 11879206428207 \\
 &\times 18302139876755678844518928432329915957461983909116641756799460631945310960374598732 \\
 &\quad 11879206428213
 \end{aligned}$$

همچنین میتوان از کتابخانه sympy.ntheory و تابع factorint استفاده کرد. (در کد این روش استفاده کرده ام). فایل q4.py خمیمه شده است.

```

maryam@bitterocean:~/Documents/Uni/99_8/Computer Security/HW2/Solution
~/Doc/U/99_8/C/HW2/Solution > python3 q4.py
Plain text : b'flag{Isfahan_University_of_Technology}'
~/Doc/U/99_8/C/HW2/Solution >

```

شکل ۱۲: خروجی فایل q4.py

V. سوال پنجم

• سه خصوصیت پروتکل امن تبادل کلید :

۱. برای هر session یک session-key جدید تولید شود.

۲. هر دو طرف ارتباط هویت خود را اثبات کنند (تصدیق هویت)

۳. کلید session باید مستحکم باشد و اگر اتکر آن را یافت باز هم کلید های اصلی پنهان بماند.

• با توجه به بخش قبل معاایب این پروتکل ها را نام ببرید.

۱. پروتکل اول :

- هویت طرفین اثبات نمیشود. (هر شخص دیگری میتواند خود را به جای A جا بزند)

- هیچ sequence number یا برجسب زمانی روی پیام های رد و بدل شده وجود ندارد و لذا امکان حمله replay برای اتکر فراهم است.

۲. پروتکل دوم :

- هیچ برجسب زمانی روی پیام های رد و بدل شده وجود ندارد و لذا امکان حمله replay برای اتکر فراهم است.

- هویت طرفین اثبات نمیشود. (هر شخص دیگری میتواند خود را به جای A جا بزند)

- اگر کلید session لو برود کلید اصلی نیز لو رقه است.

• آیا امکان سواستفاده از این پروتکل ها توسط Eve وجود دارد ؟

۱. پروتکل اول : بله، با حمله replay و یا MITM میتوان از پروتکل سواستفاده کرد.

۲. پروتکل دوم : بله، با حمله replay میتوان از پروتکل سواستفاده کرد.

• راه حل برای ارتقا امنیت این پروتکل ها

۱. پروتکل اول :

- برای تصدیق هویت ، آیدی طرفین در کنار session-key رمز و ارسال گردد.

- برای جلوگیری از حمله MITM میتوان از sequence number استفاده کرد.
 - برای جلوگیری از حمله replay میتوان از چالش استفاده کرد.
 - برای رعایت تازگی کلید نیز بهتر است از nonce و یا برجسب زمانی استفاده کرد.
۲. پروتکل دوم :

- برای جلوگیری از حمله MITM میتوان از sequence number استفاده کرد.
- برای جلوگیری از حمله replay میتوان از چالش استفاده کرد.
- برای رعایت تازگی کلید نیز بهتر است از nonce و یا برجسب زمانی استفاده کرد.

سوال ششم VI.

اسکریپت q6.sh ضمیمه شد.
 برای اجرا اسکریپت باید دستور `./q6.sh -run` را در ترمینال بزنید. (توجه ! اگر خطای دسترسی دارید کافیست دستور `chmod +x q6.sh` را امتحان کنید)
 بعد از اتمام اجرا ، میتوانید محتویات فایل ها را بررسی کنید و در نهایت برای حذف شدن فایل های ایجاد شده کافیست دستور `./q6.sh -remove` را در ترمینال بزنید.
 گیف از اجرای اسکریپت در گیت هاب من به آدرس : github.com/BitterOcean موجود است.

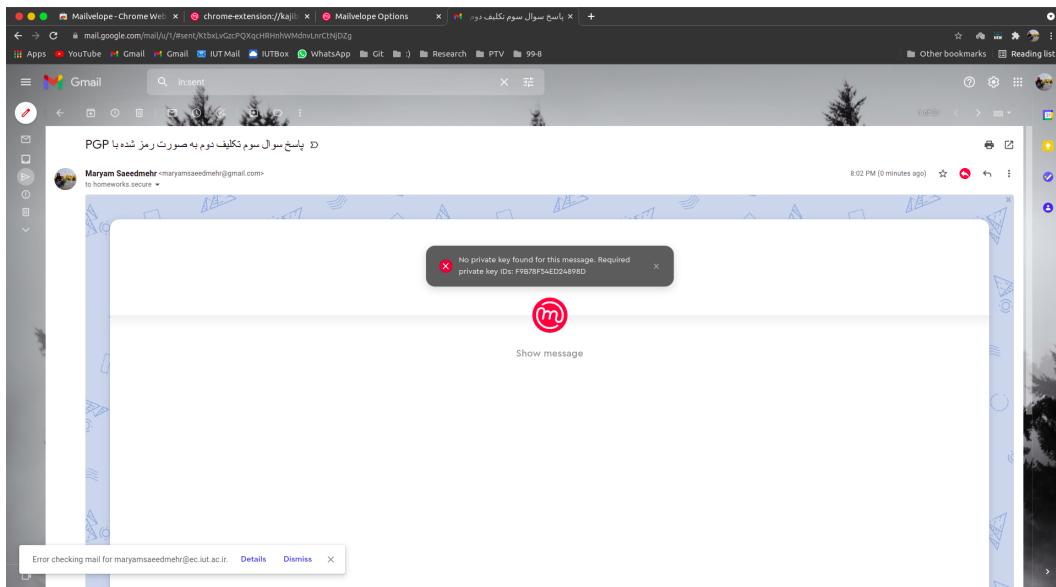
سوال هفتم VII.

فایل q7.py ضمیمه شده است.

```
maryam@bitterocean:~/Documents/Uni/99_8/Computer Security/HW2/Solution
~/Doc/U/99_8/C/HW2/Solution > python3 q7.py
2fee9d571a64e042bd05616043a16c33c0eaadb6f2edfe526ac7a3fb1b69e5f
~/Doc/U/99_8/C/HW2/Solution >
```

شکل ۱۳ : خروجی فایل q7.py

سوال هشتم VIII.



شکل ۱۴: اسکرین شات از ایمیل رمز شده ارسال شده.