«به نام خدا»

تکلیف دوم سوال اول - مرضیه علیدادی – 9631983

.1

i) کلید = V

```
In [15]: decrypt("HdxmjnjaoZsxcvibznzmqzm")
Out[15]: 'MICROSOFTEXCHANGESERVER'
```

ii) کلید = F

```
In [20]: decrypt("KfpjSjykqncfuutsUqfdXytwjhfzlmymnofhpnslBmfyxFuuxjxxntsx")
Out[20]: 'FAKENETFLIXAPPONPLAYSTORECAUGHTHIJACKINGWHATSAPPSESSIONS'
```

کد در دو فرمت py. و ipynb. ضمیمه شده است.

.2

1. در ابتدا IC را برای این متن محاسبه کرده است، تا با توجه به مقدار آن حدسی درباره ی طول کلید داشته باشد. با توجه به اینکه برابر 0.043 شده، نشان می دهد که طول کلید بزرگتر مساوی 5 است. پس، از این متد برای تحلیل متن رمز شده و بدست آوردن متن اصلی استفاده می کند.

در ابتدا، پترن هایی که بیش از یکبار در متن تکرار شده اند را به همراه فاصله ی آن ها بدست می آوریم. از فاکتور های فاصله ی پترن های تکراری، می توان طول کلید را حدس زد.

دو تا طولانی ترین پترن تکراری موجود را در نظر می گیریم. 6 فاکتور مشترک فاصله های آن ها ست. به بقیه ی پترن ها هم که نگاه کنیم، 2 و 3 در اغلب آن ها فاکتور فاصله شان است. پس حدس می زنیم که طول کلید برابر 6 باشد. پس این حدس را بررسی می کنیم.

برای بررسی آن، متن را در 6 ستون می نویسیم. هر کدام از ستون ها قرار است با یک حرف رمز گشایی بشوند. مثل این است که هر ستون با سزار رمزنگاری شده است. پس باید هرستون را با روشی که برای سزار داشتیم، تحلیل کنیم.

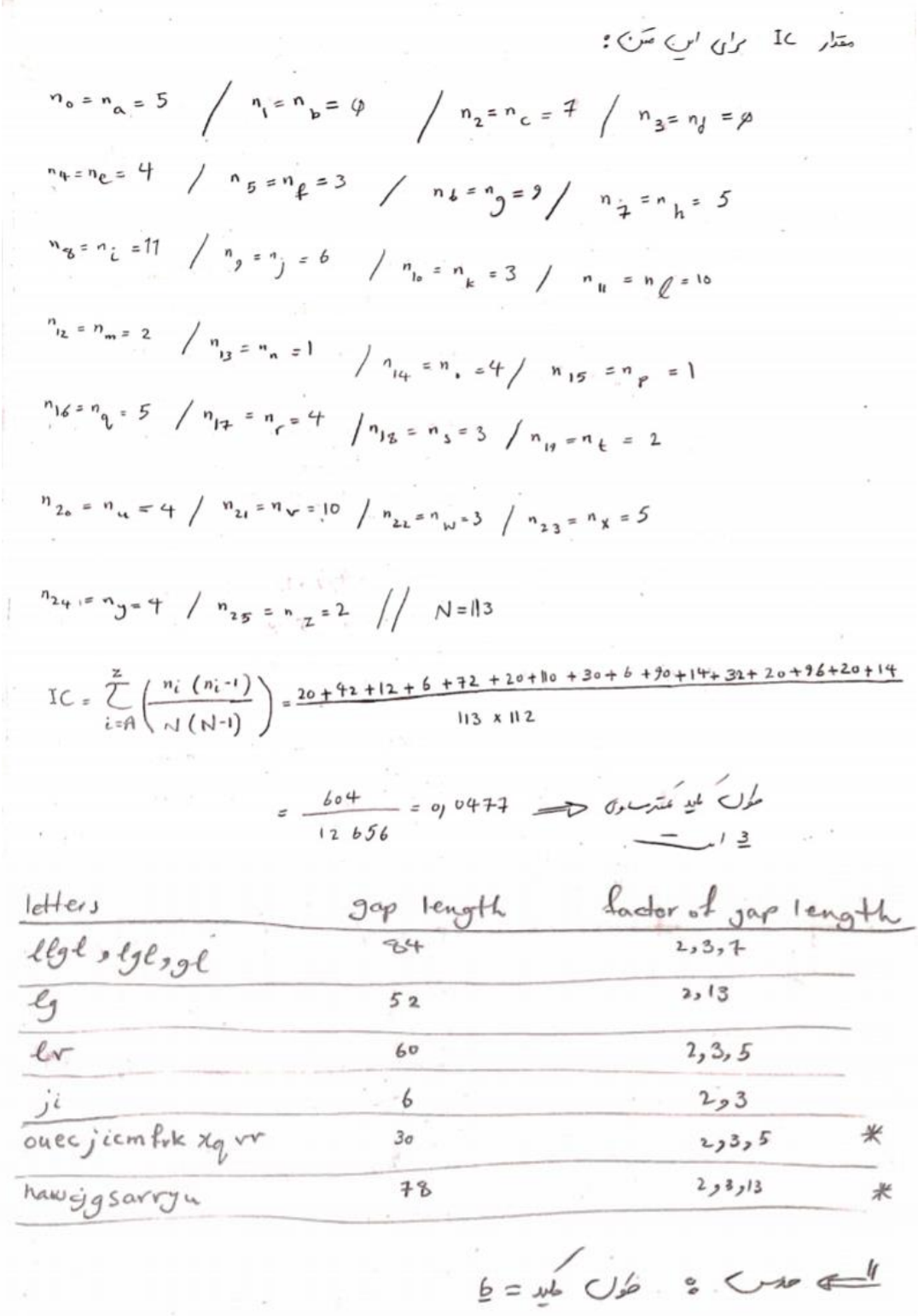
برای هر کدام از ستون ها IC را محاسبه می کنیم، تا ببینیم که آیا IC آن ها نزدیک به زمانی است که متن با کلید با طول 1 رمز شده است یا خیر. همچنین، در هر کدام از ستون ها فراوانی حروف الفبا را مشخص می کنیم. سپس با توجه به توزیع فراوانی متون واقعی انگلیسی و ترتیب توزیع فراوانی ها در بین حروف الفبا، حدسی درباره ی کلید هر ستون می زنیم و حروف بدست آمده از حدسمان را در متن رمز شده جایگذاری می کنیم. به ترتیب می توان این کار

را برای هر کدام از ســـتون ها انجام داد. همچنین می توان با جایگذاری چند حرف از یک کلمه، بقیه ی حروف آن را حدس زد و با توجه به آن درباره ی کلید ســـتون نظیر آن حرف، کلیدی را حدس زد. این کار ها را تکرار می کنیم، تا کلید هر ستون به دست آید و به یک متن اصلی valid برسیم.

وقتی به متن valid برسیم، کلید ستون ها را کنار هم قرار می دهیم. و این همان کلید ویژنر است.

.2

"Llglv eji ouec jicmfrk xq vv hawcjgsarvyu efh ouec jicmfrk xq vv lgtgzlp.oi clv xzi qhvw olq xvgahg qyillgl ks ti jigixyn ii hawcjgsarvyu"



1	2	3	4	5	6
ℓ	ℓ	g	ℓ	r	e
j	ι	o	u	e	c
j	i	c	m	t	r
K	x	q	r	r	h
a	w	c	j	g	s
a	r	r	J	u	e
f	h	o	u	e	c
j	i	c	m	t	r
K	x	q	r	r	ℓ
g	t	J	z	ℓ	p
o	i	c	ℓ	r	x
z	i	q	h	r	w
o	ℓ	q	x	r	g
a	h	g	q	J	i
ℓ	ℓ	g	t	K	s
t	i	j	i	J	i
x	J	n	i	i	h
a	w	c	j	g	s
a	r	r	J	u	

⟹ IC تغیر حروف هر کدام از ستون ها را به دست می‌آوریم:

* ستون 1:

a→5/ ℓ→1/ g→1/ j→3/ K→2/ ℓ→2
o→2/ t→1/ x→1/ z→1 /N=19

$IC = \frac{20+6+2+2+2}{19\times18} = \frac{32}{342} = 0,0935$

* ستون 2:

ι→2/ i→6/ ℓ→3/ r→2/ ℓ→1/
w→2/ x→2/ g→1 /N=19

$IC = \frac{2+30+6+2+2+2}{19\times18} = \frac{44}{342} = 0,1286$

* ستون 3:

c→5/ g→4/ j→1/ n→1/ o→2/
ι→4/ r→2/ N=19

$IC = \frac{20+12+4+12}{19\times18} = \frac{48}{342} = 0,140$

* ستون 4:

h→1/ i→2/ j→2/ ℓ→3/ m→2
q→1/ u→2/ r→2/ g=2/ z→1
x=1/ N=19

$IC = \frac{4+6+8}{342} = \frac{18}{342} = 0,0526$

* ستون 5:

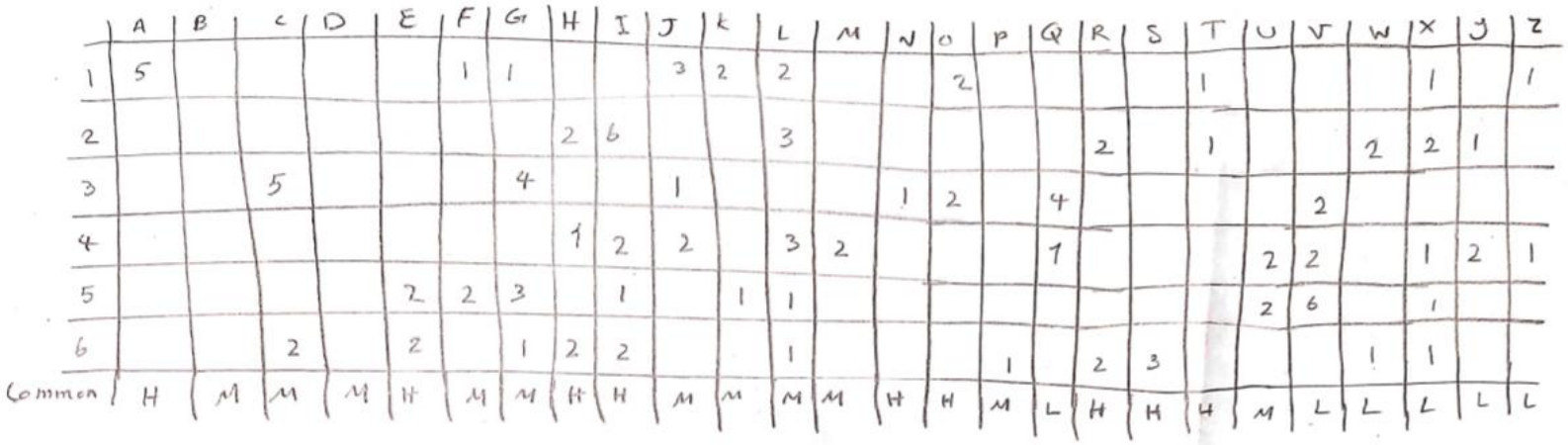
e→2/ f→2/ g→3/ i→1/ k→1
ℓ→1/ u→2/ r→6/ y=1 /N=19

$IC = \frac{6+6+30}{342} = \frac{42}{342} = 0,1228$

* ستون 6:

c→2/ e→2/ g→1/ h→2/ i→2/ ℓ→1
p→1/ r→2/ s→3/ w=1/ x=1 /N=18

$IC = \frac{10+6}{18\times17} = \frac{16}{306} = 0,0522$



با توجه به توزیع فراوانی حروف در ستون 3، به نظر میرسد که C همان A است و G همان E است. پس، کلید 2 است.

"Llelv eji muec jiamfrk xo vv hawajgsartyu efh muec jiamfrk xo vv lgtezlp.oi alv xzi ohvw olo xvgahe qyillel ks ti higixyl ii hawajgsartyu"

با توجه به توزیع فراوانی حروف در ستون 6، به نظر میرسد که کلید 4 است.

"Llelv aji muey jiamfnk xo vv dawajgoartyu afh muey jiamfnk xo vv hgtezll.oi alv tzi ohvs olo xvcahe qyellel ko ti higexyl ii dawajgoartyu"

با توجه به کلمه ی muey ، به نظر می رسد که این کلمه، many باشد. با بررسی توزیع فراوانی دو ستون 4 و 5، این حدس را چک می کنم.

این حدس به نظر درست می آید. پس کلید ستون 4 را برابر 20 و کلید ستون 5 را برابر 17 در نظر می گیرم.

"Llere aji many jiasonk xo be dawappoarted afh many jiasonk xo be hgteful.oi are tzi ones olo decahe wheller to ti hopexyl or dawappoarted"

با توجه به کلمه ی hopexyl، به نظر می رسد که این کلمه، hopeful باشد. با بررسی توزیع فراوانی دو ستون 1 و 2، این حدس را چک می کنم.

این حدس به نظر درست می آید. پس کلید ستون 1 را برابر 18 و کلید ستون 2 را برابر 4 در نظر می گیرم.

درنهایت با توجه به این حدسیات، متن زیر با استفاده از کلید "secure" با طول 6 به دست می آید؛ که یک متن valid با کلمات با معنی است:

“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”

پس متن به درستی رمزگشایی شد.

.3

- رمز های نامتقارن امنیت بیشتری را برای داده ها ایجاد می کنند. امن ترین رمزنگاری است؛ چرا که هرگز لازم نیست کاربران، private key ها را share کنند. بنابراین، شانس حملات به private key ها کاهش می یابد.
از معایب رمز های متقارن، ناتوانی آن ها در نگه داشتن کلید به صورت secret است. این مسئله زمانی دشوار می شود که رمزنگاری و رمزگشایی قرار است در دو مکان متفاوت اتفاق بیفتد، و نیاز است که کلید جابه جا شود.
از آن جایی که دو کلید private و public نمی توانند از طریق هم به دست بیایند، می توان به راحتی کلید public را منتشر کرد و نگران نقض امنیت نبود.
- Certificate شامل یک public key است، که یک identity از شخص یا کامپیوتر یا سرور و یا سرویس به آن ضمیمه شده است.
Certificate یک راه ایمن برای تبادل public key فراهم می کند. تا از طریق آن، بتوان برای آن شخص، پیامی رمزنگاری کرد و فرستاد.
- replay attack و forward search attack و dictionary attack و sniff و MITM
- این مسئله که طول کلید به اندازه ی طول متن باشد و تصادفی باشد و همیشه جدید باشد، خیلی ایده آل است. اگر کلید رندوم نباشد و قابل حدس باشد، محرمانگی زیر سوال می رود. اگر حین انتقال کلید بین فرستنده و گیرنده لو برود، باز هم محرمانگی زیر سوال می رود. و اگر موقع ذخیره کردن در سیستم هایمان لو برود، یا به شیوه ی درستی ذخیره نشود، محرمانگی زیر سوال می رود.
در کل دلیل ما برای رمزنگاری این است که یک متن که معمولا طول بزرگی دارد، باید مخفی باشد و محرمانگی اش حفظ شود. و ما ترجیح می دهیم به جای اینکه یک متن بزرگ را از همه پنهان کنیم، آن را به نحوی رمزنگاری اش کنیم وفقط کلید رمز نگاری که طول کمتری دارد، را مخفی کنیم. حال وقتی در این الگوریتم، طول کلیدمان به اندازه ی طول متن باشد، ما همان دغدغه هایی که برای متن اصلی داریم، را برای کلید هم خواهیم داشت. چون کلید بزرگ است، تولید تصادفی اش سخت است و انتقال و ذخیره سازی اش دشوار است. اگر ما می توانستیم کلیدی به اندازه ی پیام ایجاد کنیم و آن را انتقال دهیم به نحوی که محرمانگی اش حفظ شود، اصلا رمز نگاری نمی کردیم. همان متن اصلی را محرمانگی اش را حفظ می کردیم.
پس این روش رمزنگاری خیلی ایده آل است و رسیدن به آن ممکن نیست.

.4 کلید رمزنگاری در الگوریتم RSA ، نسبت به کلید رمز متقارن ضعیف تر است. یعنی مثلا برای دست یابی به یک سطح از محرمانگی که در رمز متقارن با کلید با طول 80 بیت مهیا می شود، در RSA باید از کلید با طول 1024 بیت استفاده کرد. بنابراین، کوتاه بودن طول کلید، موجب آسیب پذیری می شود.

.5

- امنیت Simplicity – Efficiency - End-to-end
- امنیت End-to-end نقض شده است.
- در پروتکل اول، B مطمئن نیست دارد با A صحبت می کند. خط سوم توسط eve می تواند شنود شود و حمله ی

replay رخ دهد. Eve با شنود آن و ارسال آن می تواند بین خودش و B یک session تشکیل دهد. و می تواند پیام های A به B را تکرار کند.

- برای رفع این مشکل که در پروتکل اول رخ می دهد. B می تواند یک عدد رندوم تولید کند و آن را با کلید session رمز کند. A باید آن را رمز گشـــایی کند و منهای 1 کند و دوباره آن را با کلید session رمز کند و برای B ارســـال کند. پس از اینکه A به درستی این مراحل را طی کند، session بین آن ها برقرار می شود.

- سوالات اختیاری:

- تنها راهی که میتوان با کمک آن الگوریتم vigenere را secure کرد، این است که از یک کلید که تماما تصادفی است و طول آن بزرگتر مساوی طول متن اصلی است، استفاده کنیم. همچنین هرگز نباید از یک کلید دو بار استفاده کرد. در این صورت، الگوریتم تبدیل به one-time pad میشود.

- S-box یک باکس برای عمل substitution است. تنها کامپوننت در DES است که غیر خطی است. هدف اصلی آن مبهم کردن رابطه ی بین کلید و متن اصلی و متن رمز شده است. s-box ها در مرکز تامین امنیت DES قرار دارند. بدون آن ها، متن رمز شده، خطی می شود و به راحتی قابل شکستن خواهد بود.