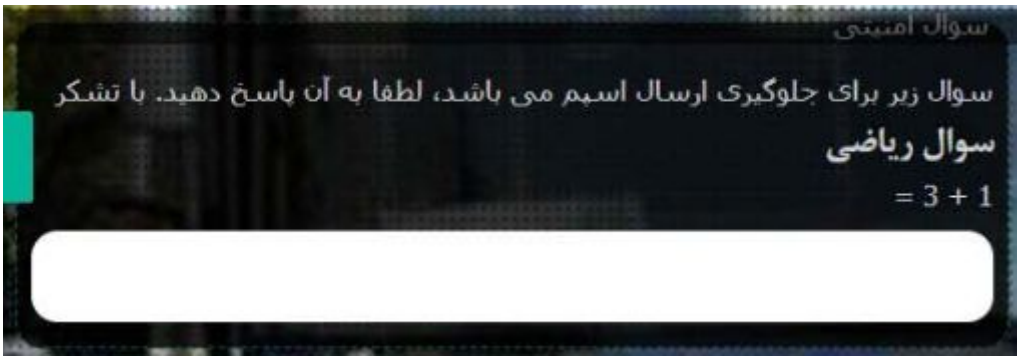
1-

خط مشی امنیتی سامانه نقلیه :

1) در ابتدا برای هر فرد دانشگاهی دانشجو و پرسنل به ترتیب شماره دانشجویی و شماره پرسنلی به عنوان نام‌کاربری و کد ملی به عنوان کلمه عبور انتخاب شده‌است.
2) در هر بار احراز اصالت (وارد شدن) سامانه از فرد می‌خواهد که به یک سوال ریاضی پاسخ دهد.



3) بعد از وارد شدن به برای بار اول، از کاربر می‌خواهد که کلمه عبور خود را تغییر دهد و از کاربر می‌خواهد که یک آدرس ایمیل معتبر وارد کند.

پیشنهاد : بهتر است ثبت‌نام در سامانه از قبل صورت نگرفته باشد تا هیچ کسی با دردست داشتن شماره دانشجویی و شماره ملی فرد نتواند وارد سامانه شود و با تغییر دادن کلمه عبور فرد با استفاده از ایمیل خودش، دسترسی شخص را به سامانه قطع کند (Availability).

خط مشی امنیتی سامانه خوابگاه دختران و خود خوابگاه دختران:

1) روش کارکلی سامانه به این صورت است که در طول شبانه‌روز در بازهی زمانی خاص (که توسط مسئولین محترم خوابگاه اعلام میگردد) و همچنین توسط دستگاههایی که در محل خوابگاه نصب هستند، اقدام به حضور و غیاب نموده و نتیجه را در یک پنل وب(به آدرسdormitory.iut.ac.ir)گزارش می‌دهد.
2) همه روزه، در یک بازه ساعتی خاص حضورو غیاب دانشجویان خوابگاهی از طریق دستگاه‌های نصب‌شده در خوابگاه انجام می‌گیرد. تعیین ساعت حضور و غیاب در اختیار مسئولین محترم خوابگاه است.
3) در صورتی که دانشجو در بازه ای قصد ترک خوابگاه را دارد، باید اقدام به ثبت درخواست خروج شبانه کند. درخواست خروج شبانه از طریق پنل تحت وب در دسترس دانشجویان محترم میباشد.
4) در صورتی که دانشجویی ساعت حضور و غیاب اقدام به ثبت حضور خود نکند، اگر درخوابگاه حضور دارد باید حداکثر تا ساعت 6صبح با مراجعه به دفتر خوابگاه حضور خود را ثبت نماید. در این حالت حضور وی قید "باتاخیر"ثبت خواهدشد .و اگردانشجو در محلی غیر از خوابگاه حضور دارد باید حداکثر تا قبل از ساعت 12شب از طریق پنل وب فرم درخواست خروج شبانه را تکمیل کند.
5) در صورتی که دانشجو از ساعت شروع حضور و غیاب(ساعت 11شب)به بعدوارد خوابگاه بشود، حضور او در خوابگاه توسط دستگاه گیت ثبت شده و این ورود به عنوان ورود غیرمجاز ثبت خواهدشد.
6) در این سامانه کاربر امکان تغییر رمز عبور خود را دارد. رمز عبور کاربران سامانه باید حداقل دارای 6 کاراکتر باشد.
7) هر دانشجو موظف به ثبت شماره تلفن همراه خود میباشد.

پیشنهاد : بهتر است اگر دانشجویی در زمان مقرر حضور خود را ثبت نکرد، با وی تماس گرفته شود تا اگر گرفتاری دارد بتوان هرچه زودتر به او کمک کرد.

2-

Access Control in Operating Systems

Windows:

In general, Access Control in Windows is designed as a Discretionary Access Control model that is fitted to act as a Role-Based Access Control (RBAC : in RBAC, access is granted based on the roles individual users have in their organization based on their job functions. Permissions are assigned to roles based on the requirements of job functions and users are made members of roles, thus gaining permissions assigned to these roles)) model due to its groups and administrative privileges' capabilities. Groups can be regarded as roles, permissions and privileges can be assigned to these groups/roles. and finally, users can be joined to the said groups/roles.

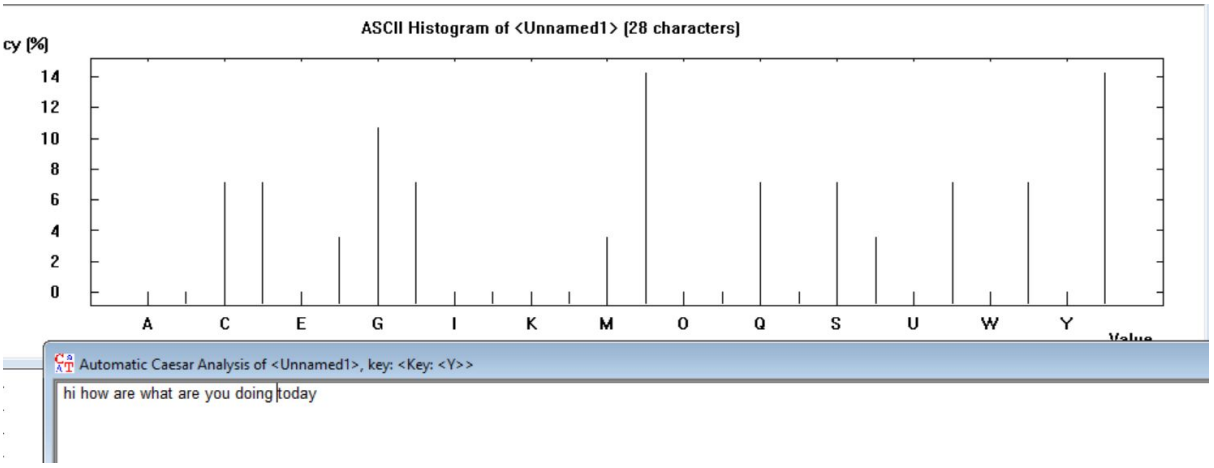
LINUX:

Linux was initially developed as a clone of the Unix operating system in the early 1990s. As such, it inherits the core Unix security model _a form of Discretionary Access Control (DAC). Unix DAC is a relatively simple security scheme, although, designed in 1969, it does not meet all of the needs of security in the Internet age. However, the option of designing a totally new security system from the ground up is not available _new features have to be retrofitted and compatible with the existing design of the system. In practical terms, this has meant that we end up with a collection of security enhancements rather than a monolithic security architecture.

(refrences are hyperlinked in the titles)

3-

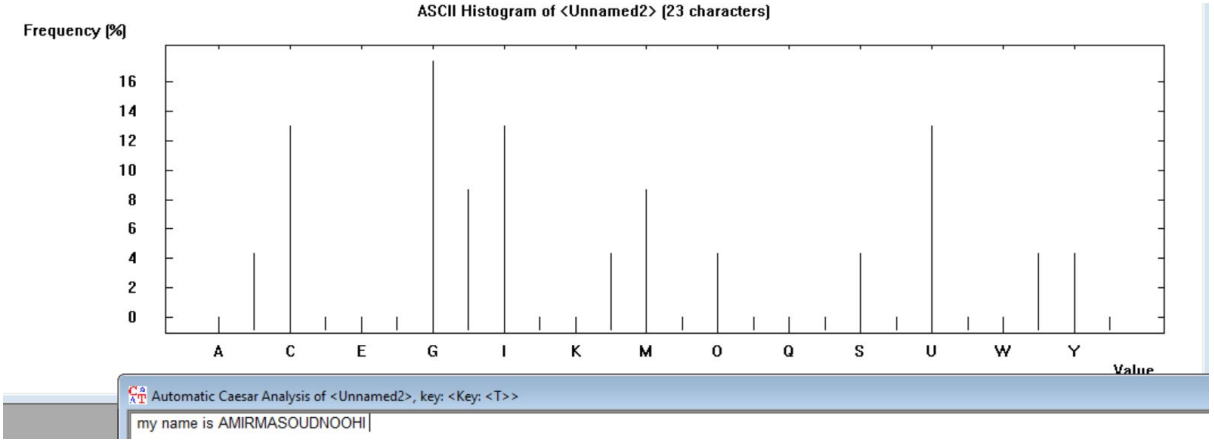
1) Hi how are what are you doing today



2) code is attached under hw2.

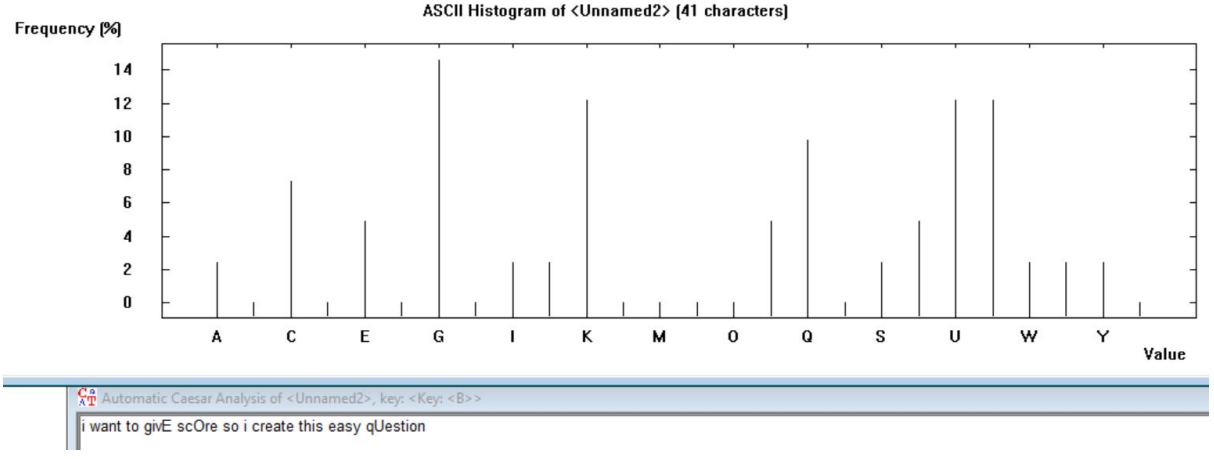
All cipher text got decrypted with the most probable phi(i).

My name is AMIRMASOUDNOOHI



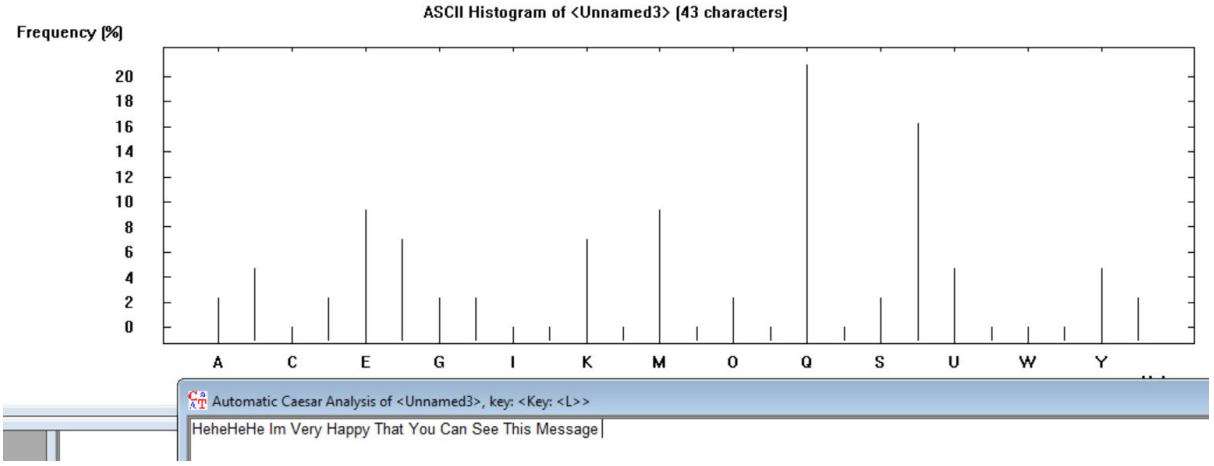
3)

i want to givE scOre so i create this easy qUestion



4)

HeheHeHe Im Very Happy That You Can See This Message



4-

a) Kasiski noticed that repetitions occur when characters of the key appear over the same characters in the ciphertext. The number of characters between the repetitions is a multiple of the period. We choose the longest repetition to be the key size. Then we split the text into key size parts and implement frequency analysis on each of those parts. We can check if they are from the same alphabet by compairing their index of coincidence.

b) (refrence)

   i) if you were able to decrypt this sentence then try decrypting otvzuoqrpotqoaeuaxv to get some cool secret information do not share this information with others it is also optional for you to find this information and you can continue to track hidden information behind this encryption believe in me and follow me.
   Key = CYBERSECURITY

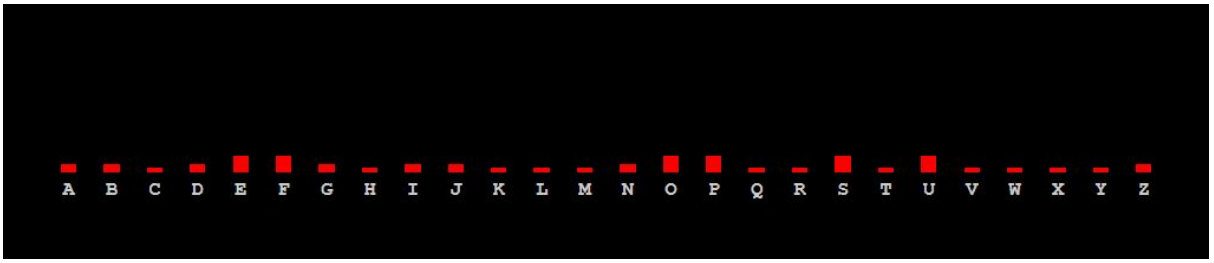
Repeated Sequence	Spacing	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
CVM	182	X					X						X	X						
EIT	26	X											X							
ITJ	26	X											X							
TJC	26	X											X							
JCR	26	X											X							
CRN	26	X											X							
NZV	143										X		X							
BLH	78	X	X			X							X							
LHM	78	X	X			X							X							
HMS	78	X	X			X							X							
MSQ	78	X	X			X							X							
SQR	78	X	X			X							X							
QRL	78	X	X			X							X							
RLM	78	X	X			X							X							
LMQ	45		X		X				X						X					
LMQ	33		X								X									
MQH	78	X	X			X							X							
NCV	48	X	X	X		X		X				X				X				
EEV	37																			
EITJ	26	X											X							
ITJC	26	X											X							
TJCR	26	X											X							
JCRN	26	X											X							
BLHM	78	X	X			X							X							
LHMS	78	X	X			X							X							
HMSQ	78	X	X			X							X							

MSQR	78	X	X			X							X							
SQRL	78	X	X			X							X							
QRLM	78	X	X			X							X							
RLMQ	78	X	X			X							X							
LMQH	78	X	X			X							X							
EITJC	26	X											X							
ITJCR	26	X											X							
TJCRN	26	X											X							
BLHMS	78	X	X			X							X							
LHMSQ	78	X	X			X							X							
HMSQR	78	X	X			X							X							
MSQRL	78	X	X			X							X							
SQRLM	78	X	X			X							X							
QRLMQ	78	X	X			X							X							
RLMQH	78	X	X			X							X							

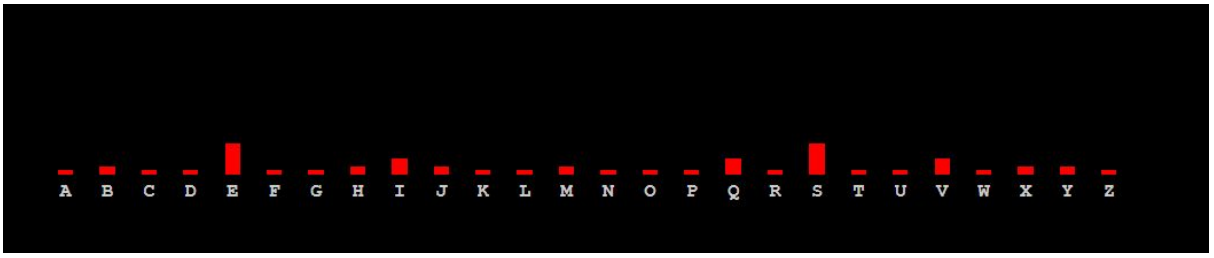
So its most likely for key size to be 13.

Characters 1 , 14 , 27 , … frequency analysis

Characters 2 , 15 , 28 ,... frequency analysis

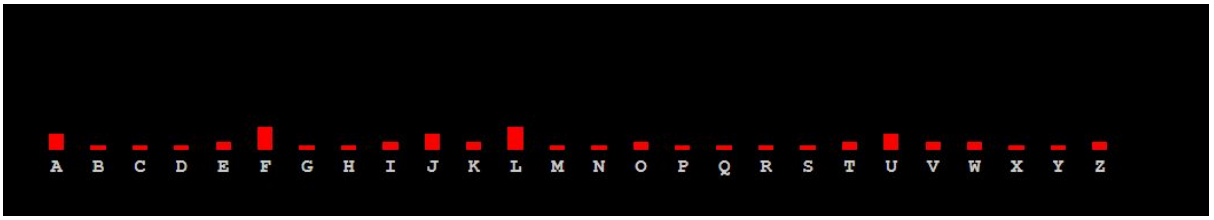


Characters 3 ,16, 29, … frequency analysis

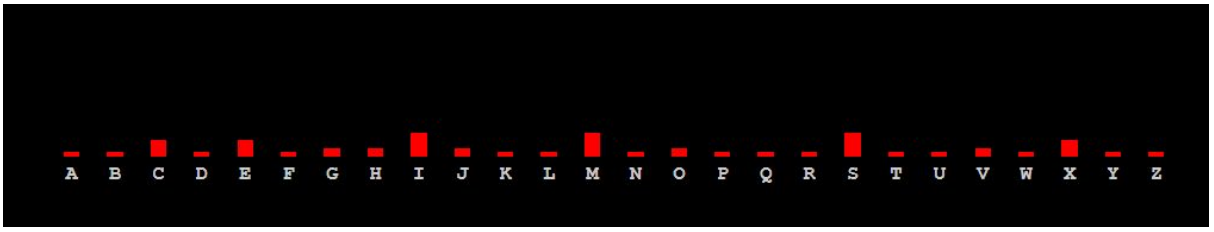


Characters 4, 17, … frequency analysis

Characters 5,18,... frequency analysis



Characters 6, 19, … frequency analysis

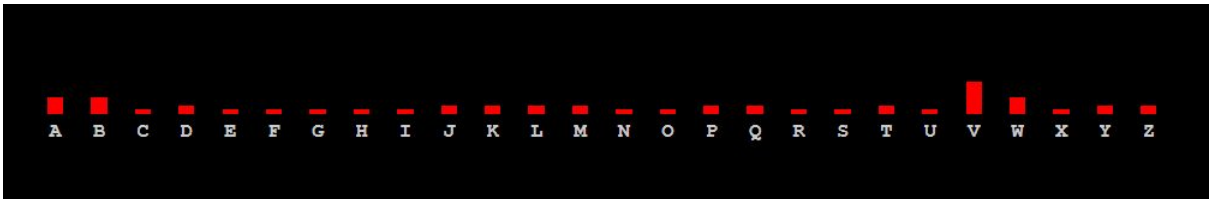


Characters 7, 20 , 33, … frequency analysis

Characters 8, 21 , 34, frequency analysis

Characters 9, 22 , 35, … frequency analysis

Characters 10, 23 , 36 , … frequency analysis



Characters 11,24,37,... frequency analysis

Characters 12,25,38,... frequency analysis

Characters 13,26,39,... frequency analysis
Comparing with :

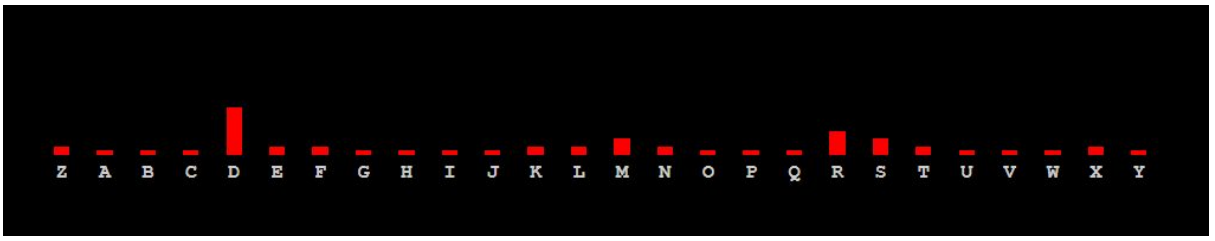
Columns need 2, 24, 1, 4, 17, 18, 4, 2, 20, 17, 8, 19, 24 shifts respectively which makes the key to be CYBERSECURITY.

ii) NOW LETS GO DEEPER SHALL WE GUESS WHAT EVERY SINGLE CHOICE YOU HAVE MADE IN YOUR LIFE HAS LED YOU TO THI PLACE HERE READING THIS TEXT YOUR CAREER YOUR SOCIAL LIFE AND ANY OTHER DECISION YOU HAVE MADE SINCE BIRTH NOW PLACES YOU AT THE MOMENT IN THIS TIME IN HISTORY WE SOMETIMES FORGET THE POWER OF FATE AND FINALITY OF THIS RULE

Key = ZELVCQUUDNJBL

Vigenere Repeat Distance: Repeated Sequence	Spacing	Possible length of key (or factors) 02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
JYF	135		X		X				X						X					
LXV	13												X							
FFU	91						X						X							
FUF	91						X						X							
UFR	91						X						X							
ITR	52	X		X									X							
FFUF	91						X						X							
FUFR	91						X						X							
FFUFR	91						X						X							
JXOFU	112	X		X			X	X						X		X				
XOFUE	112	X		X			X	X						X		X				

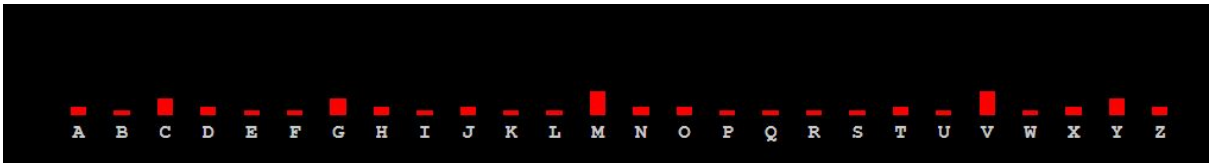
We choose the key size to be 13.



Characters 1,14,...frequency analysis

Characters 2,15,... frequency analysis

Characters 3,16,... frequency analysis



Characters 4,17,... frequency analysis

Characters 5,18,... frequency analysis

Characters 6,19,... frequency analysis

Characters 7 , 20 , … frequency analysis

Characters 8 , 21, … frequency analysis

Characters 9, 22 , … frequency analysis

Characters 10 , 23 , … frequency analysis

Characters 11 , 24 , … frequency analysis

Characters 12 , 25 , … frequency analysis

Characters 13 , 26 , … frequency analysis

Comparing with :

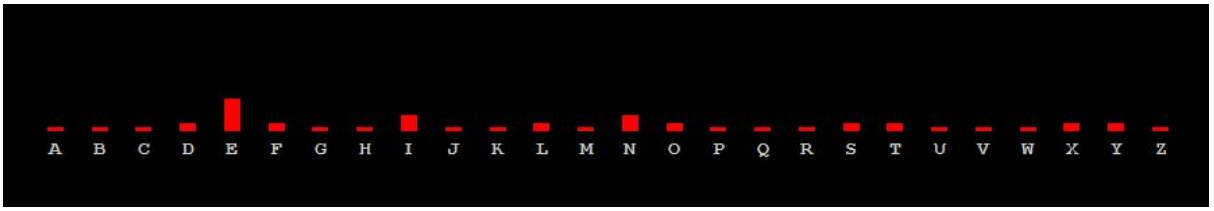
Columns need 25, 4, 11, 21, 2, 16, 20, 20, 3, 13, 9, 1, 11 shifts respectively which makes the key to be ZELVCQUUDNJBL.

iii) ITS GOOD TO GET A LITTLE FREAKED OUT EVERY NOW AND THEN STEPPING OUT OF YOUR COMFORT ZONE IN ANYWAY CAN EXPOSE YOU TO NEW IDEAS AND HELP YOU SEE THE WORLD IN NEW POTENTIALLY BETTER WAYS AND THERES NO BETTER WAY TO FREAK YOURSELF OUT THAN BY UPENDING YOUR GRASPON KNOWLEDGE

Key = ABCDEFGHIJKLMN

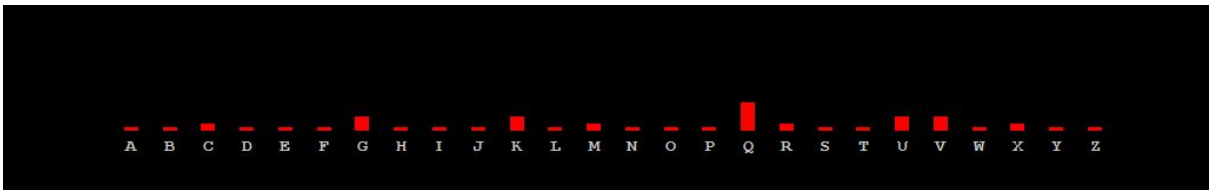
Vigenere Repeat Distance: Repeated Sequence	Spacing	Possible length of key (or factors) 02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
IUV	32	X		X				X								X				
JXO	112	X		X			X	X						X		X				
XOF	112	X		X			X	X						X		X				
OFU	112	X		X			X	X						X		X				
FUE	112	X		X			X	X						X		X				
DUB	112	X		X			X	X						X		X				
JXOF	112	X		X			X	X						X		X				
XOFU	112	X		X			X	X						X		X				
OFUE	112	X		X			X	X						X		X				
JXOFU	112	X		X			X	X						X		X				
XOFUE	112	X		X			X	X						X		X				

We choose the key size to be 14 (i tried 16 and it didnt work :))))



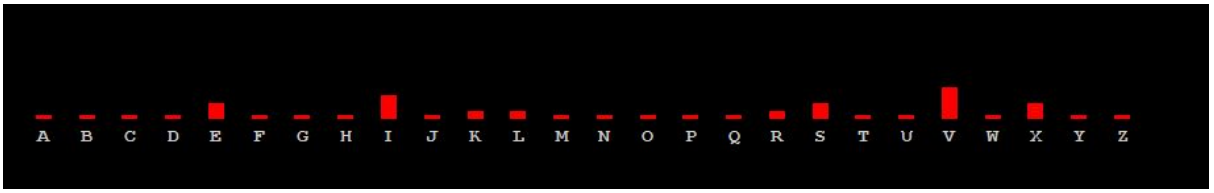
Characters 1, 15 , … frequency analysis

Characters 2, 16 , … frequency analysis



Characters 3,17 , … frequency analysis

Characters 4 , 18 , … frequency analysis



Characters 5,19,... frequency analysis

Characters 6,20,... frequency analysis

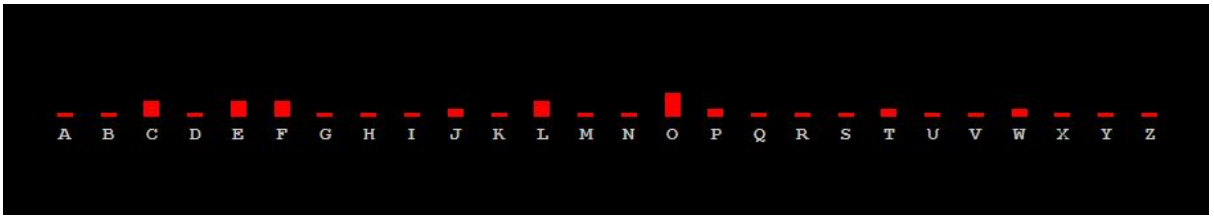
Characters 7,21,... frequency analysis

Characters 8,22,... frequency analysis

Characters 9 , 23 , … frequency analysis

Characters 10 , 24 , … frequency analysis

Characters 11 , 25 , … frequency analysis



Characters 12 , 26 , … frequency analysis

Characters 13, 27 , … frequency analysis

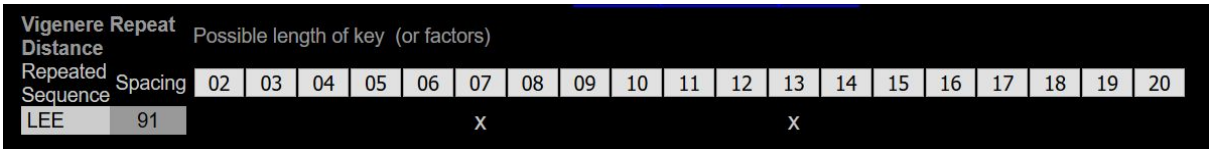
Characters 14 , 28 , … frequency analysis

Comparing with :

Columns need 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 shifts respectively which makes the key to be ABCDEFGHIJKLMN.

iiii) the world is a pretty strange place things often dont happen according to plan and weird coincidences are generally the norm with this in mind its not surprising that there would be unexpected facts

Key = QAZWSXEDCRFVT



We choose the key size to be 13 (i tried 7 and it didnt work).

Characters 1,14,... frequency analysis

Characters 2,15,... frequency analysis

Charactes 3 ,16 , … frequency analysis

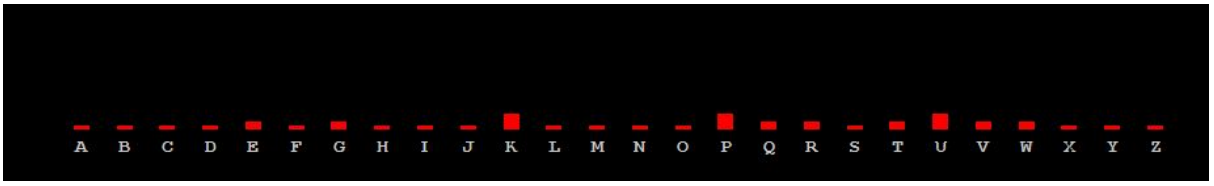
Characters 4,17,... frequency analysis

Characters 5,18,... ferquency analysis

Characters 6,19,... frequency analysis

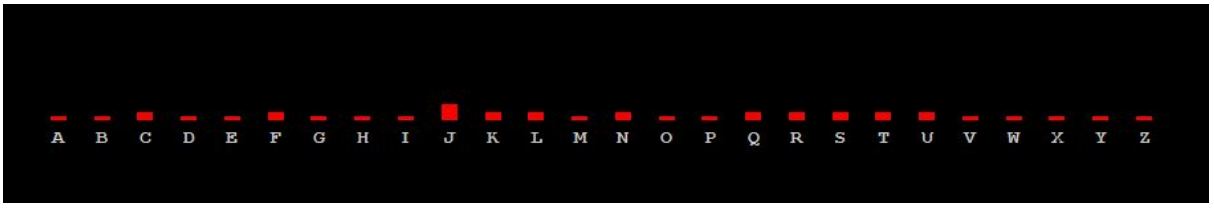
Characters 7,20,... frequency analysis

Characters 8,21,... frequency analysis



Characters 9,22,... frequency analysis

Characters 10,23,... frequency analysis



Characters 11,24 , … frequency analysis

Characters 12,25 … frequency analysis

Characters 13,26,... frequency analysis

Comparing with :

Columns need 16, 0, 25, 22, 18, 23, 4, 3, 2, 17, 5, 21, 19 shifts respectively which makes the key to be QAZWXEDCRFVT.

5-

T # h # i # s # # i # s # # E # x # a # m # p # l # e # # T # o # # f # u # l # l # y # # U # n # d # e # r # s # t # a # n # d # # R # s # a # # T # o # p # i # c

---

084 # 104 # 105 # 115 # 032 # 105 # 115 # 032 # 069 # 120 # 097 # 109 # 112 # 108 # 101 # 032 # 084 # 111 # 032 # 102 # 117 # 108 # 108 # 121 # 032 # 085 # 110 # 100 # 101 # 114 # 115 # 116 # 097 # 110 # 100 # 032 # 082 # 115 # 097 # 032 # 084 # 111 # 112 # 105 # 099

16077 # 34195 # 26032 # 19155 # 22226 # 26032 # 19155 # 22226 # 07373 # 16528 # 21188 # 26159 # 29707 # 17591 # 33829 # 22226 # 16077 # 39842 # 22226 # 10020 # 07925 # 17591 # 17591 # 14209 # 22226 # 05162 # 48984 # 01073 # 33829 # 41534 # 19155 # 37998 # 21188 # 48984 # 01073 # 22226 # 19457 # 19155 # 21188 # 22226 # 16077 # 39842 # 29707 # 26032 # 06445

6-

a) It is attached under public.pem

b)

E = 65537

D = 9.427998080195858e+307

P = 1.2931065684082719e+154

Q = 1.2296460097306952e+154

c)

1024 bit private key

d)

i)

tctn5NNKm1LvHF0fJ68esaceFalWQ5bBvLqHn05bGjQ6jSbFvxHcutejynPm6oAswyu3PCb2WfCvvxGWcgujyHCKNnCOG7QgI9vz4eedBZ3A4j2nUGRwmWLQ420J6lShs+TxqM8Sn+TMETjYBUh8B+T2J6kzCN5TuTrnbRL8M4U=

ii)

ac17iz3MngBXCtPF2crFDyooE8/uuzG88WmN48ShT88BgLUgZELN9ezNuCOei97KGfNeJnpLKDngvXoWJ9RIhLC+bGAU2tBWiznzmgXzNdbPrAie+oFNXaSfXCYFGec6/k96ApSSsUnPv6CnLRramZs3uBttTD0VKLyfTFzDqJc=

e)

i) what re you waiting for?

ii) i don’t know why you cant decrypt this?

7-

```python
import hashlib
def HMAC(key, message, block_size):
    if len(key)<block_size:
        key = key.rjust(block_size-len(key),'0')
    elif len(key)>block_size:
        key = hashlib.sha256(key.encode('utf-8')).hexdigest()
    opad = '5c'*block_size
    ipad = '36'*block_size
    key_opad = str(hex(int(key,16)^int(opad,16)))
    key_ipad = str(hex(int(key,16)^int(ipad,16)))

    return hashlib.sha256((key_opad+str(hashlib.sha256((key_ipad+message).encode('utf-8')).hexdigest())).encode('utf-8')).hexdigest()

HMAC('security!','We are in interesting Position',8)
```

4570a104e9a8c4fef5e75fbebed75073e83406e528c84f0f6b5442482503621e