

H2

Mandana Ghadamian

Cryptography and Information Security

CIS3362

Professor Arup Guha

September 02, 2026

- 1) Decode the following message, which was encrypted using the substitution cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

hstduespudulsvasnxoqmpkocochknpenlsesbnttoqtuyshopkdazwpuman
wkzoasesevsacwsqloqmphukuracuqvasnxoqmncrvcpoprpuqdownsabut
tuhoqmcsysanthauqmtsnlcnqlmsppoqmquhksaspksqurpubpksvtrsocnh
hualcnwwsnaophnctoxsenmodpksqowtnzslnvurppsgeoqrpscubhksstub
buaprqsnglknlduewtspstzdandxslpksdulscrdkocpksqnprasubdulsva
snxoqmenqzhauqmpraqctopptwaumascnqlpksqkuwsbrttzntrdxzvasnx

Step 1: Find the letter frequencies

I begin by using a cryptography tool to analyze the ciphertext and calculate the frequency of each letter and n-gram.

From the frequency table, I can see that S is the most frequent letter, since E is the most frequently occurring letter in English, I make the initial assumption: S → E

Enter Text:

hstduespudulsvasnxoqmpkocochknpenlsesbnttoqtuyshopkdazwpuman
wkzoasesevsacwsqloqmphukuracuqvasnxoqmncrvcpoprpuqdownsabut
tuhoqmcsysanthauqmtsnlcnqlmsppoqmquhksaspksqurpubpksvtrsocnh
hualcnwwsnaophnctoxsenmodpksqowtnzslnvurppsgeoqrpscubhksstub
buaprqsnglknlduewtspstzdandxslpksdulscrdkocpksqnprasubdulsva
snxoqmenqzhauqmpraqctopptwaumascnqlpksqkuwsbrttzntrdxzvasnx

Frequency of Letters

A 6.1%	B 2.2%	C 4.7%	D 3.3%	E 2.5%	F 0.0%	G 0.0%	H 3.3%	I 0.0%
J 0.0%	K 4.7%	L 3.6%	M 3.3%	N 7.2%	O 6.1%	P 7.7%	Q 6.9%	R 3.6%
S 12.2%	T 5.2%	U 7.5%	V 2.2%	W 2.7%	X 1.9%	Y 0.5%	Z 1.9%	

Compute

Step 2: Look at the repeated N-grams

Next, I use the Repeated NGrams section of the tool to find the most frequent patterns, for example:

- OQM: 15 times PKS: 10 times KSQ: 7 times PKSQ: 7 times

Repeated NGrams

2, DUE: 2, DULSVASN XOQM: 2, HAUQM: 2, HKS: 2, KOC: 2, KSA: 2, LCN: 2, LPKS: 2, LSVASN XOQM: 2, OQMP: 2, PRA: 2, SES: 2, SVASN XOQM: 2, ULSVASN XOQM: 2, UMA: 2, UQM: 2, URP: 2

Compute

Step 3: Look for common English words that could match these patterns. For example:
Identify PKS, already assumed S → E, A common 3 letter English word that fits is: THE
PKS → THE

Step 4: Find other similar patterns to identified words. For example: PKSQ is similar to PKS
PKSQ → THEN, Q → N

Step 5: Repeat step 3 and 4 for other frequent patterns. For example:
OQM: 15 times, several longer patterns: XOQM, NXOQM, ASN XOQM, SN XOQM.
Therefore, OQM → ING

Step 6: Use the current mappings to find longer words and use “Decipher” to check the plain text:

Your Guess

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

r- -s-c-n- - -v- - h- -d g -a-i -t n-u e- -l -o b- -p-k -v y-

- we- l- c- o- me- t- o- c- o- de- b- r- rre- a- k- in- g- th- i- s- i- s- wh- a- t- m- a- de- me-
f- a- l- l- in- l- o- ve- w- i- th- cr- rry- p- t- ogr- rr- a-
- ph- y- ir- rre- me- mb- e- r- rr- s- pe- n- d- in- g- t- w- oh- our- rr- s- on- b- r-
rre- a- k- in- g- a- sub- s- t- i- tu- t- i- on- c- i- ph- e- r- rr f- o-
l- o- w- in- g- se- ve- r- rr- a- l- wr- rr- on- g- le- a- d- s- an- dge- t- t- in- gn- o- wh- e- r-
rre- th- e- n- ou- t- o f- th- e- b- lue- i- s- a- w

Decipher

Cipher	A	B	C	D	E	F	G	H	I	J	K	L	M
Plain	R	F	S	C	M	-	-	W	-	-	H	D	G

Cipher	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plain	A	I	T	N	U	E	L	O	B	P	K	V	Y

Plain Text

Welcome to code breaking. This is what made me fall in love with cryptography. I remember spending two hours on breaking a substitution cipher, following several wrong leads and getting nowhere. Then out of the blue, I saw words appear. It was like magic. Then I played about ten minutes of Wheel of Fortune and had completely cracked the code. Such is the nature of code breaking: many wrong turns, little progress, and then hopefully a lucky break.

- 2) **Decode the following message, which was encrypted using the substitution cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message. Here is the ciphertext:**

zapbtslcllsjrwgrbstcogtsvvgrcisbbigbpgcbzapargazuaylmgkszskc
iiufylbbtgmglparxtanpgcdlbtgkavgzaprywngpbtpggzsplbcrvzaiiax
lbtgsrlbpykbsarlbtcbcpjgsogrsrbtcbwgllcjgsylgvbatsvgbtglgbts
rjlciaogpbtgmickggograzzkcwmylnybsrwuaivcjsogjabbbgriceucrv
raxcvculfylbtsgbtsrjlsrbtgtgknysivsrjsblgclsgpzapuayciiclxg
iinybtamgzyiiughyciiuzyrclvsjrsrjrbtgvspbbaanbcsruaypbpgcb

Step 1: Find the letter frequencies

I begin by using a cryptography tool to analyze the ciphertext and calculate the frequency of each letter and n-gram.

From the frequency table, I can see that G is the most frequent letter, since E is the most frequently occurring letter in English, I make the initial assumption: G → E

Enter Text:

iiufylbbtgmglparxtanpgcdlbtgkavgzaprywngpbtpggzsplbcrvzaiiax
lbtgsrlbpykbsarlbtcbcpjgsogrsrbtcbwgllcjgsylgvbatsvgbtglgbts
rjlciaogpbtgmickggograzzkcwmylnybsrwuaivcjsogjabbbgriceucrv
raxcvculfylbtsgbtsrjlsrbtgtgknysivsrjsblgclsgpzapuayciiclxg
iinybtamgzyiiughyciiuzyrclvsjrsrjrbtgvspbbaanbcsruaypbpgcb

Frequency of Letters

A 6.6%	B 10.0%	C 7.2%	D 0.2%	E 0.2%	F 0.5%	G 11.6%	H 0.2%	I 5.5%
J 3.0%	K 1.9%	L 6.6%	M 1.3%	N 1.6%	O 1.3%	P 4.7%	Q 0.0%	R 6.6%
S 8.0%	T 5.5%	U 2.5%	V 3.6%	W 1.3%	X 1.1%	Y 4.1%	Z 3.3%	

Compute

Step 2: Look at the repeated N-grams

Next, I use the Repeated NGrams section of the tool to find the most frequent patterns, for example:

- BTG: 21 times ZAP: 7 times BTS: 6 times CII: 6 times

Repeated NGrams

GBTSRJL: 2, GCB: 2, GPBT: 2, IIA: 2, JGS: 2, JSR: 2, LBTG: 2, NYB: 2, OGR: 2, PGCB: 2, RBTG: 2, RJL: 2, RJS: 2, RLB: 2, SOG: 2, SRBTG: 2, SRJL: 2, SRJS: 2, SVGBT: 2, TCB: 2, TGK: 2, TGM: 2, TSRJL: 2, TSVGBT: 2, VGBT: 2, YCII: 2, YLB: 2

Compute

Step 3: Look for common English words that could match these patterns. For example:

Identify BTG, already assumed G → E, A common 3 letter English word that fits is: THE

BTG → THE

I then tested each assumption against other repeated patterns in the ciphertext. If a mapping did not make sense or produced words that were not English, I rejected it and tried a different one.

I repeated this process until I found several patterns that matched common English words:

SRJ → ING ZAP → FOR, CII → ALL UAY → YOU

Step 4: Use the current mappings to find longer words and use “Decipher” to check the plain text:

Your Guess

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

-o -t -a - - -j -e - -l g - -s - - -r - -n -i -h -y - - - -u -f

f-o -r-t-h-i-s-a-s-s-i-g-n-e-n-t-i-h-a-e-h-i--e-n-a-l-i-t-t-l-e-t-r-e-a-t-f-o
-r-o -n-e-o -f-y-o -u-s-e-i-f-i-a
-l-l-y-j-u-s-t-t-h-e-e-r-s-o -n-h-o -r-e-a-s-t-h-e-o --e-f-o
-r-n-u--e-r-t-h-r-e-e-f-i-r-s-t-a-n-f-o -l-l-o -
-s-t-h-e-i-n-s-t-r-u-t-i-o -n-s-t-h-a-t-a-r-e-g-i-e-n-i-n-t-h-a-t-e-s-s-a-g-e-i-u-s-e-t-o
-h-i-e-t-h-e-s-e-t-h-i

Decipher

For example, the highlighted part should be “assignment”, so W → M

Step 5: Repeat step 4 to find other letters.

Cipher	A	B	C	D	E	F	G	H	I	J	K	L	M
Plain	O	T	A	K	Z	J	E	Q	L	G	C	S	P

Cipher	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plain	B	V	R	-	N	I	H	Y	D	M	W	U	F

Plain text:

For this assignment, I have hidden a little treat for one of you, specifically just the person who breaks the code for number three first and follows the instructions that are given in that message. I used to hide these things all over the place, even off campus, but in my old age I've gotten lazy, and nowadays just hide things in the HEC building. It's easier for you all as well, but hopefully equally fun as digging in the dirt to obtain your treat.

3) Decode the following message, which was encrypted using the Vigenere cipher.

Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

jbqfbwlzidnmseyivshvsdpgammzdygybxwjeyegovqsabbxkfsgmwoxkwpwn
 wllargbymkwsflsqgynkmgzyhohjgmvbamirxnvbmzxwvbtlbfnprhjaxgr
 gcmmulqaaiualhcseqhlnmxzawqhwrlxdgbnjsuirtatjeoevepkwinumafj
 cnhezawabnbawqlorpmfvsjtvdttdshkwaylgeqnpjienkhklruwteegzvzl
 lqshpqlwiymnymjwikmqrnkcauxvaxcbnwppdnprwsgjxbbbaytfqsmxzwbro
 qspkhlrkrwsxubbidqhmaoidtrpqtsoicemvwsxuheyzyvwhcygsqeccv

In addition to describing your entire process, please include as attachments any code you used (c, cpp, java, py). A good portion of the grade is based on the description of the process and not getting the correct decrypt.

Step 1: Find the number of bins or key length

To determine the key length, I used CryptoTool's Index of Coincidence (IC) tool and tested different possible key lengths. For each key length, CryptoTool calculated an IC value for each bin. I then averaged these values to get one overall score for each candidate.

The results showed that 14 bins had an average IC of about 6.9, which is close to the expected value for English text (around 6.5–6.9). Therefore, I determined that the key length is 14.

Index of Coincidence 14

Find

6.0 Index 11: 11.66 Index 12: 4.66 Index 13: 4.66

Step 2: Splitting the ciphertext into 14 bins

With the key length confirmed as 14, I split the full ciphertext into 14 separate groups, grouping the letters according to their position in the ciphertext. Each group contains letters encrypted using the same key character.

Letter Frequency of the English Language



Letter Frequency Graph - Bin 1

Start at: q

Update



Letter Frequency Graph - Bin 2

Start at: A

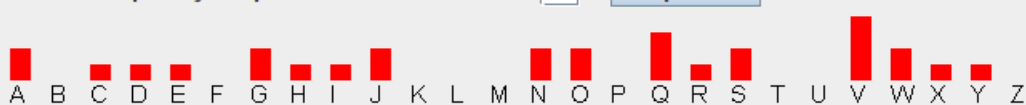
Update



Letter Frequency Graph - Bin 3

Start at: A

Update



Letter Frequency Graph - Bin 4

Start at: A

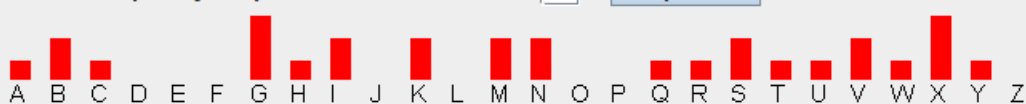
Update



Letter Frequency Graph - Bin 5

Start at: A

Update



Bins: 13

Compute

Step 3: Score Every Possible Shift for Each Bin

Since I was not able to reliably distinguish the bar lengths in CryptoTool's frequency graphs by eye, I wrote a Java program to calculate the scores more objectively.

For each of the 14 bins, my program tested all 26 possible shifts, corresponding to the key letters A through Z, using the Mutual Index of Coincidence (MIC) method.

I repeated this process for every bin and compared the scores for all 26 shifts. For each bin, the shift with the highest MIC score was considered the most likely shift because it produced the frequency pattern that most closely matched English text.

```
Best guessed key length: 14

--- MIC-based key letter guesses ---
The highest found: 0.0655 letter: q
The highest found: 0.0653 letter: u
The highest found: 0.0530 letter: i
The highest found: 0.0667 letter: n
The highest found: 0.0600 letter: t
The highest found: 0.0644 letter: e
The highest found: 0.0695 letter: s
The highest found: 0.0717 letter: s
The highest found: 0.0659 letter: e
The highest found: 0.0729 letter: n
The highest found: 0.0576 letter: a
The highest found: 0.0750 letter: i
The highest found: 0.0556 letter: a
The highest found: 0.0572 letter: l
```

Step 4: Assemble the Candidate Key

After scoring all 26 shifts for each of the 14 bins, I selected the highest-scoring shift from each bin and converted each shift into its corresponding letter. This produced the following sequence:

Q – U – I – N – T – E – S – S – E – N – A – I – A – L

Together, these letters form the candidate key:

“QUINTESSENAIAL”

This key was then used in the next step to decrypt the ciphertext and check whether it produced meaningful English text

Step 5: Decrypting and Verifying

With the corrected 14-letter key, "QUINTESSENTIAL," I decrypted the full ciphertext by subtracting each key letter from the corresponding ciphertext letter and repeating the key as needed across all 364 characters.

The resulting plaintext was then checked to make sure it produced clear, meaningful English text.

Plaintext:

This is the question for all the money literally, okay, so it's not too much, just twenty bucks. So you are going to four oh eight not the road but the office number in HEC. If you stand at this door and you face east you will see a beautiful view out a large window and in your sight line towards the bottom right you will see a fire extinguisher. If you open the door to it and lift the device underneath it is an envelope with your treat. Hope you enjoy good luck!