CAB340 - Cryptography
Queensland University of Technology
Semester 2, 2018

Assignment 1

Student: John Santias (N9983244)
Due: Friday 17th August 2018

Contents

The Ciphertexts to Cryptanalyse

Ciphertext 1 (0.txt):

vmi mxypkglob xktwfg ogsitwstk rwobklm
ehpgftuiv. Uzelbimpgj, kyfv, ojd pcohcxd co zjcu pwd tacx, ljwi xyn
ucpcx si an qlbouoozuvlm ognjecuouj wb mubbis. Lju qxqmtik wb lje
cpgkmxkst xyx tgn musi bocsuj hottyn ljwoe cyvsgec wylj klboozpkehyn
ctqyb. Zjc vofgob, gz ank, Q ghrgklhsj, kcs vxei cqv zfyduemxa tq s
gbost fsget pcsuouj lmx nkkik. Afcx ghptmwu qnsep geu crbogstwvk dcxb
kfuwvh ol vuilmtcs--lcr wsbo cgzepktte bekec lje pgnw sj gbsljg....

“Gcq encqvl xydy ikcx lji zyfctogy ydcbo! Ljwi xyv bc dckhd tq cteh, gn
afcx tq bopclm si: pqb K taxqafu djce bnmcepr si gqze gej--kwnz dnsyjn,
ouyta. A xwvcpobyn m ruqejmr lmglwpm. Wi lckf louu, or ycs do gqqz
xkljobehu. Moob s pwygcqr? Ywvt, gcq gee owcyy S qstwzyn lje pmc zuh
djc uoqpm ud rgzbkfg cs g cst yqjejcw g wsmqs; lcr zup khyljehc gbas ywp
wiec kubo wb do wsbo mqu dc qo zxyl ix ck rwd tacx pqnsyn emlms jooz an
a jcgp wb egvvuj-oeoh. Wn vkrb xqeq wn, tqa--ynmqufg, yqzw, ozgzxqfg.
Tauohsw, gtt G myin, hnmcev gf ucqjdyn ghptyvsganr, ye

X

Ciphertext 2 (1.txt):

Dgt CSoJFkoq zz EM dbmJ, oF Hjf qKuO Ch
gsQkK, KkurHt Lvg qkSowBv xyNjK, HjpCD hJCmfx OnJoufC BgEs dbmJ zG
Ag, xoQk zscsn zmswp jx Snwwt pwHtGIu bxC zwFtjpXoFu ujwOrAqkuI. h
xwAgnlDxwr jjC zhBseu zKksrkoq, GoK odkoBz LvtfkSy, Lvg dyKuKGcm CBgDs
qg rHy Nwnf nDyAFgt, DGk EscoxDyK, Hjf DNxEspu, DGk LsoqoRzMCwt kMmMwui
yE nAG upEK. GFr nbDDx GB K toDswr vp CDk zwu dyKrwqvfn KgFuwjn LgFBgs,
GGkF vg tkHj GBg ekX, 'Zzwu myS ux wxpBX tGK kt BDgDzA nsMk. lvg DyLvsBA
esC tGH rbl EuJ wv. J mNrDseuoC oL AAtoKl sH c woQE yFgbD OkJGqokK xAGm.
J kL gxFcjn SnwM yjvK zJM vp mKgAA ku kR zzsksC SnGIii. R'L. OL wu b
nHlxwevvS isGg. Xrzz vC ApE SnABm J yTmzH vp nN--xwGktD? dn? a KcoD Mu
ECtf DGgF xwtDHiw.'... Vg xkMzwr pp wNxw Hjbx IAKHkdo--Mu ECtf DGgF
xwtDHiw. W tbxF zzs dfvK hwtqso z ssvqhkME vCqs yM zzs hjBRz xzqpB, ztv
KjjvD O OokuoC nw GgfwDj LC uukQk sH of yTz Gt vio FrsGuz zztwz--uukQk
Owvi DGgL Kkeo ztv wonoMyw GvbBD kEptbmHty, qqonDsFwph, vNgLvkoq zrD Hjf
EMoNstto. h ywsofn Su zscs DGk OvktzDxwr

Ciphertext 3 (2.txt):

dovgkodij qiy pnqst otvntpo. Di bqvp, pat hqiqjtn oqds
qbptnwqnso paqp Hn. Frnpz'o htpakso aqs nrdits pat sdopndvp. D aqut ik
kldidki ki paqp lkdip, crp D wqip ykr vgtqngy pk ristnopqis paqp patnt
wqo ikpadij txqvpgy lnkbdpqcgt di patot atqso ctdij patnt. Paty kigy
oakwts paqp Hn. Frnpz gqvfts ntopnqdip di pat jnqpdbdvqpdki kb ado
uqndkro gropo, paqp patnt wqo okhtpadij wqipdij di adh--okht ohqgg
hqpptn wadva, wati pat lntoodij itts qnkot, vkrgs ikp ct bkris ristn
ado hqjidbdvtip tgkmrtivt. Watpatn at fitw kb pado stbdvdtivy adhotgb D
vqi'p oqy. D padif pat fikwgtsjt vqht pk adh qp gqop--kigy qp pat utny
gqop. Crp pat wdgstnitoo aqs bkris adh krp tqngy, qis aqs pqfti ki adh q
ptnndcgt utijtqivt bkn pat bqipqopdv diuqodki. D padif dp aqs wadoltnts
pk adh padijo qckrp adhotgb wadva at sds ikp fikw, padijo kb wadva at
aqs ik vkivtlpdki pdgg at pkkf vkriotg wdpa pado jntqp okgdprst--qis pat
wadoltn aqs lnkuts dnntodopdcgy bqovdiqpdij. Dp tvakts gkrsgy wdpadi adh
ctvqrot at wqo akggkw qp pa

Ciphertext 4 (3.txt):

av ah e ieov cao ot fr dnordooog mi ve l seniie pehtsa hhcetoanc tniesb t cdneleu ofO c aesr wl oof t itahwrhes hetihrf gidfna tsn ene nsemitw lsi af asyas Wo eh htt sanniurgt Yu go drnowe ind Idsoag t oefroh w oa rhan a ld nead c l eW ld   onI   nditeesniF tmnitne yu soi Fyas tsn ene nsemitn aeb h Ideg   odahnIe mit odtah as em sitwuob twi hth edl ear tdnas fspio lnoowetnealbknlieh puopt g aadb tn nsegols ohtetyskae p imaept   seIu olleyd aI ht aot w te hchneietsr ad gnvcmricuo htnetgsa esn ad sne htegtonpit glna too oyb hyrbo k okrc o eehT rr usawsretcaf o nhtue nhguits ehtetg nihs aes ovriew asAn am wbt dnei hneewh sellIt daot fkooa te reh aevasgs aohwwarmif ewH   neia sandoerpmvmeips c e nehfl uocd periuietv ari olacbe Hrel hstaw l eereb m woep udna wm noyo tdro ao ol kwi h tmea sasgynfidie esa sd gniaai gonyrdap oe rfo bae hceseaf dn he htarl a tawngonik ishih slg dnew eA fsnhom ta rfo thn inigedn daohrtof lra taeefn yli a hc pisu eHqtdaetn esht RCzPhTo

English common frequencies

Common English single letter frequencies in % (Practical Cryptography. 2018. 3):

A : 8.55	K : 0.81	U : 2.68
B : 1.60	L : 4.21	V : 1.06
C : 3.16	M : 2.53	W : 1.83
D : 3.87	N : 7.17	X : 0.19
E : 12.10	O : 7.47	Y : 1.72
F : 2.18	P : 2.07	Z : 0.11
G : 2.09	Q : 0.10	
H : 4.96	R : 6.33	
I : 7.33	S : 6.73	
J : 0.22	T : 8.94	

Common English digrams frequencies in % (Practical Cryptography. 2018. 3):

TH : 2.71	EN : 1.13	NG : 0.89
HE : 2.33	AT : 1.12	AL : 0.88
IN : 2.03	ED : 1.08	IT : 0.88
ER : 1.78	ND : 1.07	AS : 0.87
AN : 1.61	TO : 1.07	IS : 0.86
RE : 1.41	OR : 1.06	HA : 0.83
ES : 1.32	EA : 1.00	ET : 0.76
ON : 1.32	TI : 0.99	SE : 0.73
ST : 1.25	AR : 0.98	OU : 0.72
NT : 1.17	TE : 0.98	OF : 0.71

Common English trigrams frequencies in % (Practical Cryptography. 2018. 3):

THE : 1.81	ERE : 0.31	HES : 0.24
AND : 0.73	TIO : 0.31	VER : 0.24
ING : 0.72	TER : 0.30	HIS : 0.24
ENT : 0.42	EST : 0.28	OFT : 0.22
ION : 0.42	ERS : 0.28	ITH : 0.21
HER : 0.36	ATI : 0.26	FTH : 0.21
FOR : 0.34	HAT : 0.26	STH : 0.21
THA : 0.33	ATE : 0.25	OTH : 0.21
NTH : 0.33	ALL : 0.25	RES : 0.21
INT : 0.32	ETH : 0.24	ONT : 0.20

Mapping the letters to their numbers

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2: Encoding English capital letters using integers from $\mathbb{Z}_{26}$.
(mvngu. 2018.)

Section 1 – Statistics for each Ciphertext

The following results were obtained from Cryptool 1 presenting four different characteristics. Results are displayed in either a table or a histogram.

The Single Character frequencies:

Ciphertext 1:

No.	Substring	Frequency (in %)	Frequency
1	C	7.1611	56
2	G	6.0102	47
3	O	5.8824	46
4	E	4.7315	37
5	S	4.7315	37
6	Y	4.6036	36
7	U	4.4757	35
8	W	4.4757	35
9	Q	4.3478	34
10	T	4.3478	34
11	B	4.2199	33
12	J	4.2199	33
13	L	4.0921	32
14	K	3.9642	31
15	M	3.7084	29
16	N	3.5806	28
17	X	3.5806	28
18	P	3.3248	26
19	I	2.6854	21
20	Z	2.6854	21
21	V	2.5575	20
22	D	2.3018	18
23	H	2.3018	18
24	A	2.1739	17
25	F	2.0460	16
26	R	1.7903	14

Ciphertext 2:

No.	Substring	Frequency (in %)	Frequency
1	K	7.9692	62
2	G	6.9409	54
3	O	5.6555	44
4	S	5.6555	44
5	W	5.3985	42
6	D	5.1414	40
7	Z	4.8843	38
8	T	4.1131	32
9	F	3.8560	30
10	J	3.8560	30
11	N	3.8560	30
12	U	3.7275	29
13	V	3.7275	29
14	X	3.5990	28
15	H	3.4704	27
16	M	3.4704	27
17	B	3.3419	26
18	C	3.3419	26
19	Q	2.6992	21
20	E	2.5707	20
21	R	2.4422	19
22	Y	2.3136	18
23	L	2.1851	17
24	A	2.0566	16
25	P	2.0566	16
26	I	1.6710	13

Ciphertext 3:

No.	Substring	Frequency (in %)	Frequency
1	P	10.8075	87
2	T	10.8075	87
3	D	9.0683	73
4	A	8.4472	68
5	I	7.8261	63
6	Q	7.5776	61
7	K	6.0870	49
8	O	6.0870	49
9	N	4.7205	38
10	S	4.2236	34
11	G	3.7267	30
12	V	3.2298	26
13	W	2.6087	21
14	R	2.4845	20
15	H	2.2360	18
16	B	1.9876	16
17	J	1.8634	15
18	Y	1.6149	13
19	F	1.2422	10
20	C	1.1180	9
21	L	0.9938	8
22	U	0.7453	6
23	Z	0.2484	2
24	M	0.1242	1
25	X	0.1242	1

Ciphertext 4:

No.	Substring	Frequency (in %)	Frequency
1	E	12.1290	94
2	A	9.2903	72
3	T	8.3871	65
4	O	8.2581	64
5	N	8.0000	62
6	I	7.0968	55
7	H	6.5806	51
8	S	6.5806	51
9	D	4.3871	34
10	R	4.2581	33
11	L	3.3548	26
12	W	3.0968	24
13	F	2.7097	21
14	G	2.7097	21
15	C	2.1935	17
16	M	2.0645	16
17	U	1.9355	15
18	P	1.8065	14
19	Y	1.5484	12
20	B	1.4194	11
21	V	1.0323	8
22	K	0.9032	7
23	Q	0.1290	1
24	Z	0.1290	1

The 20 most common digram frequencies:

The following results were obtained from Cryptool 1.

Ciphertext 1:

No.	Substring	Frequency (in %)	Frequency
1	LJ	1.9967	12
2	BO	1.6639	10
3	CX	1.3311	8
4	YN	1.3311	8
5	CS	1.1647	7
6	LM	1.1647	7
7	CQ	0.9983	6
8	JC	0.9983	6
9	JE	0.9983	6
10	OB	0.9983	6
11	ST	0.9983	6
12	XY	0.9983	6
13	EH	0.8319	5
14	FG	0.8319	5
15	GE	0.8319	5
16	OU	0.8319	5
17	SI	0.8319	5
18	TA	0.8319	5
19	TQ	0.8319	5
20	UO	0.8319	5

Ciphertext 2:

No.	Substring	Frequency (in %)	Frequency
1	DG	1.3536	8
2	HJ	1.3536	8
3	XW	1.3536	8
4	QK	1.1844	7
5	ZZ	1.1844	7
6	GF	1.0152	6
7	GG	1.0152	6
8	GK	1.0152	6
9	KU	1.0152	6
10	LV	1.0152	6
11	OQ	1.0152	6
12	DY	0.8460	5
13	KK	0.8460	5
14	OK	0.8460	5
15	SC	0.8460	5
16	SN	0.8460	5
17	SO	0.8460	5
18	VG	0.8460	5
19	WT	0.8460	5
20	ZS	0.8460	5

Ciphertext 3:

No.	Substring	Frequency (in %)	Frequency
1	PA	5.0874	32
2	AD	3.8156	24
3	AT	3.6566	23
4	DI	3.4976	22
5	TN	2.2258	14
6	QP	2.0668	13
7	AQ	1.9078	12
8	IJ	1.5898	10
9	QI	1.5898	10
10	DO	1.4308	9
11	KI	1.4308	9
12	KR	1.4308	9
13	NT	1.4308	9
14	DH	1.2719	8
15	DV	1.2719	8
16	OP	1.2719	8
17	PD	1.2719	8
18	QO	1.2719	8
19	QS	1.2719	8
20	TS	1.2719	8

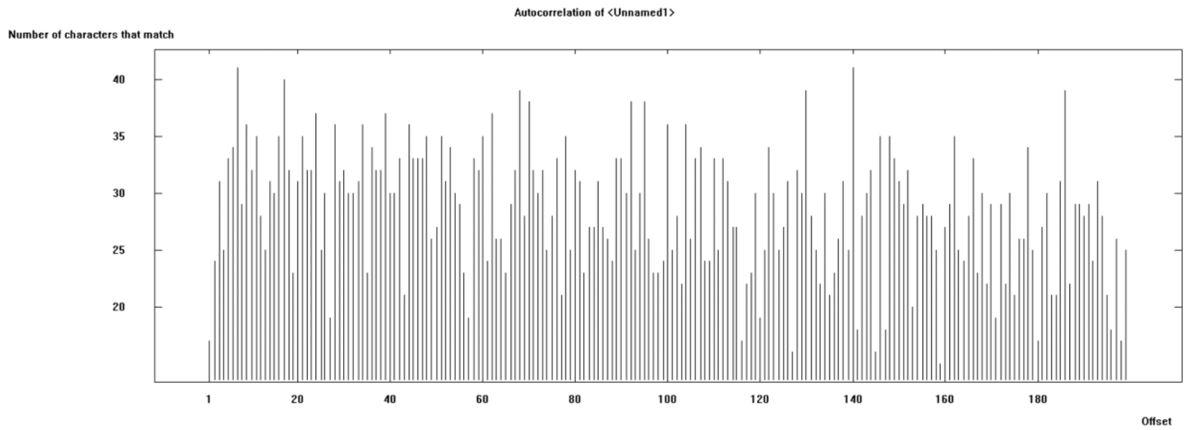
Ciphertext 4:

No.	Substring	Frequency (in %)	Frequency
1	NE	2.3850	14
2	HT	2.2147	13
3	NI	1.8739	11
4	ET	1.7036	10
5	AE	1.5332	9
6	ES	1.5332	9
7	IE	1.5332	9
8	IT	1.5332	9
9	AS	1.3629	8
10	DN	1.3629	8
11	EH	1.3629	8
12	SA	1.3629	8
13	SE	1.1925	7
14	TA	1.1925	7
15	TN	1.1925	7
16	AO	1.0221	6
17	EA	1.0221	6
18	OO	1.0221	6
19	SN	1.0221	6
20	TE	1.0221	6

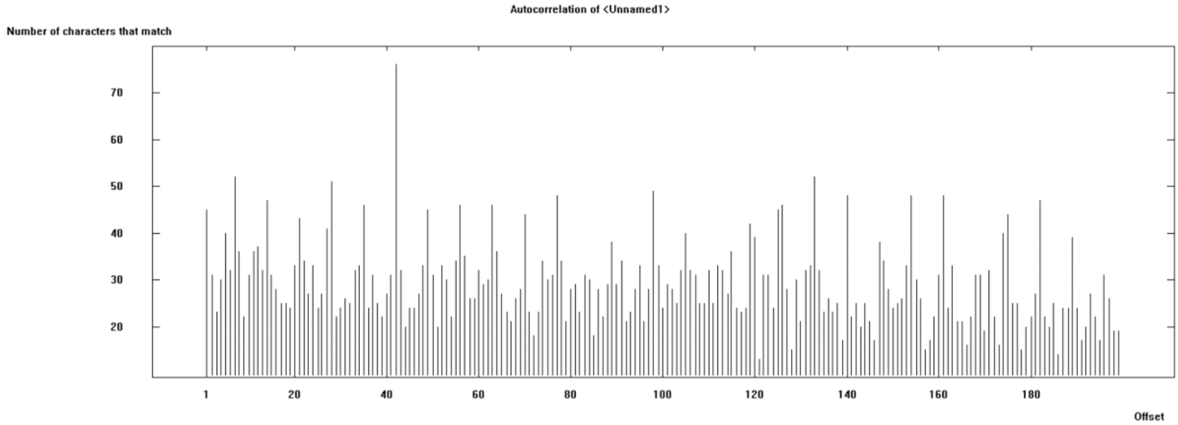
The Autocorrelation:

The following results were obtained from Cryptool 1.

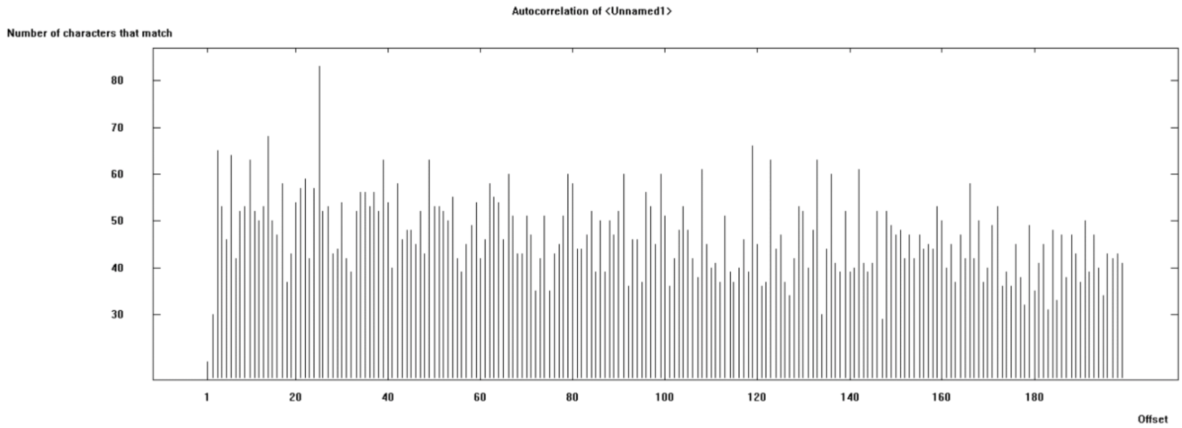
Ciphertext 1:



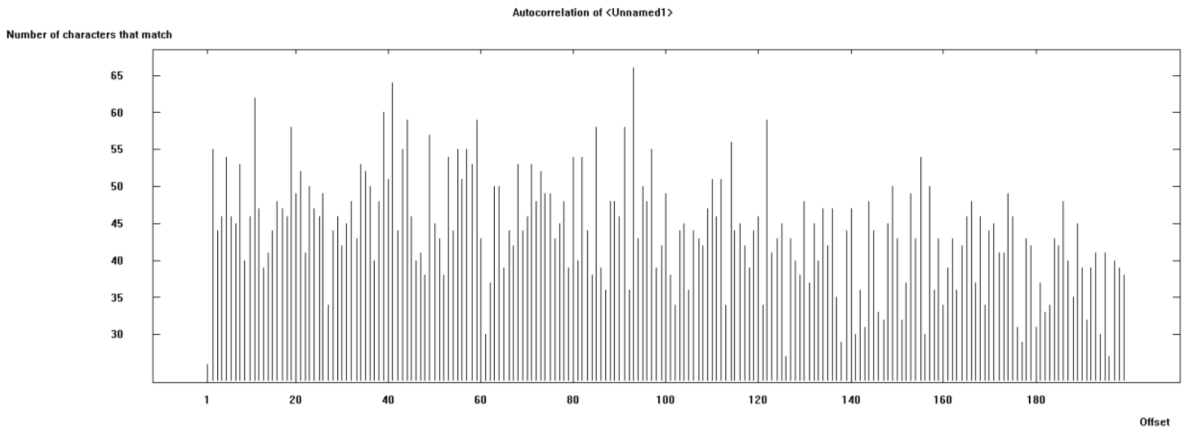
Ciphertext 2:



Ciphertext 3:



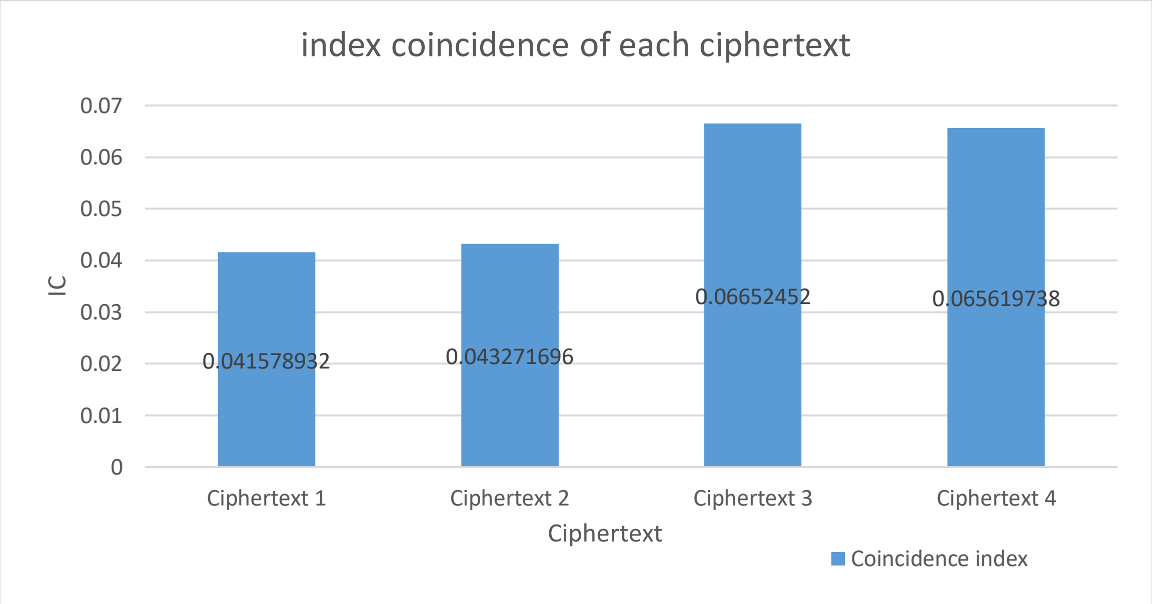
Ciphertext 4:



The Autocorrelation:

The following results were obtained from Cryptool 1.

The following results was generated using online tools (IC Cryptanalysis Tool.2018), (Practical Cryptography.2018)



Summary of the results for each ciphertext's characteristic:

	Characteristic 1	Characteristic 2	Characteristic 3	Characteristic 4
Ciphertext 1	'C' was the most frequent character (7.16%) followed by the letter 'G' 6.01%	The most frequency digram is 'LJ' (1.997%) followed by 'BO' (1.664%)	Highest match count is 41 with shift of 7.	Ciphertext has the lowest IC 0.041578932.
Ciphertext 2	The most frequent character was 'K' (7.9692%) followed by G (6.94%)	'DG', 'HJ', 'XW' was the most frequent all having the same frequency of 1.3536%	Highest match count is 76 with shift of 42.	IC is slightly higher than the ciphertext's IC. Both could have used a cipher that has a similar process. IC is 0.043271696.
Ciphertext 3	The 'P' was the most frequent character (10.8%) along with 'T' (10.8%)	'PA' (5.09%)was the most frequent digram. Followed by 'AD' (3.81%) and 'AT' (3.66%)	Highest match count is 83 with shift of 25.	The index of coincidence is high getting close to 0.070. Meaning the message could have been crypted using the transposition or substitution cipher (Frequency – Crypto Programs. 2018). IC is 0.06652452.
Ciphertext 4	'E' was the most frequent character (12.13%) followed by A (9.29%)	'NE' was the most common (2.38%) followed by 'HT' (2.2147%) and 'NI' (1.87%)	Highest match count is 66 with shift of 93.	Also close to 0.070 IC. Meaning the message could have been crypted using the transposition or substitution cipher (Frequency – Crypto Programs. 2018). IC is 0.065619738.

Section 2 – Using Characteristics for analysing Ciphertext

Analysing the single character frequency is studying the distribution of letters (may include characters and symbols) in a given text message. This analysis helps decrypt a text by comparing the letter frequencies in a plain text message with the letter frequencies in a ciphertext message (Frequency Analysis Tool. 2018). With the use of this characteristic, it can greatly assist with decryption and easily break substitution ciphers (Crypto Corner 2018) (Code My Road. 2018.). Vigenère ciphers aren't susceptible to this analysis since a plaintext letter will always be encrypted to a different ciphertext letter (Crypto Corner. 2018. Kasiski Analysis: Breaking the Code). Transposition ciphers also aren't susceptible to frequency analysis because there would be the same amount of characters in both plaintext and ciphertext. Letters are moved to different positions (Crypto Corner. 2018. Simple Transposition Ciphers). With hill ciphers, frequency analysis will increasingly be more useless if the group size of letters increases.

In analysing the frequency of digrams (or bigrams, paired letters) this can be used as a basis for breaking the Vigenère cipher by measuring the distance between the recurring bigrams. Encrypting with Vigenère cipher will generate repeated bigrams however each recurring bigram may not have the same text of the plaintext bigram (Shodhganga. 2018). Random simple substitution ciphers, on the other hand, can be easily broken using the paired letter analysis. Like the Vigenère cipher, encrypted text can repeat which is a vulnerability (SpringerLink. 2018). Transposition ciphers aren't vulnerable unless it's a simple transposition. Each letter changes its position which can confuse the cryptanalyst, but if the positions aren't significantly changed it can be easily be decrypted (A Data Analyst. 2018). For a 2 by 2 Hill cipher, if you can determine the encrypted bigram of the first two letters 'th' then the encryption key matrix can be found. This is because the Hill cipher is linear and if you only need to find two corresponding bigrams to find the key matrix (Practical Cryptography. 2018).

The autocorrelation calculates the correlation between a string and any shift of that string. This is used to determine the repeated patterns in the text and its distance where most repetitions occur. Analysing the autocorrelation for the substitution, transposition and hill ciphers is impossible because it won't help you determine the substituted letter, the letters are switched around, and the hill needs a key matrix which can't be calculated using this method. Autocorrelation is useful for the Vigenère cipher because they can have many repeated patterns at corresponding positions of the ciphertext. The distance between each repeated pattern can be used to determine the key.

The index of coincidence (IC) determines the probability of finding repeating letters in an encrypted text. If the IC is close of 0.070, the text probably would have been encrypted using either transposition or substitution cipher (Online IC Cryptanalysis Tool. 2018). For a Vigenère or hill cipher, the IC would be low close to 0.0385 (Online IC Cryptanalysis Tool. 2018).

Summary of using the characteristics to analyse the ciphertext type:

Random simple substitution cipher	Can easily break using comparisons. Most effective.	Paired letters are vulnerable as they can repeat in the text.	Not helpful to find the substituted letter.	IC would need to be close to 0.070
Vigenère cipher	Not susceptible to frequency analysis.	Analysing bigrams can be a basis for breaking the cipher, but each plaintext bigram may not be the same.	Can find the key using the distance between the repeated patterns.	IC must be low and close to 0.0385
Transposition Cipher	Not susceptible to frequency analysis	Can be decrypted if the positions of each letter haven't changed significantly.	Shifting text won't help brake the cipher.	IC must be high and must be close to 0.070
2x2 Hill cipher	With increase of the group size of letters, frequency analysis becomes more useless.	Can be used to determine the encryption key matrix.	Can't use autocorrelation because it can't determine the key matrix to decrypt ciphertext.	IC must be low and must be close to 0.0385
	Characteristic 1	Characteristic 2	Characteristic 3	Characteristic 4

Using the measured values, we can determine that the first ciphertext is a 2 by 2 Hill cipher because the index of coincidence is close to 0.0385 and using the digram frequencies will also help determine the encryption key matrix. By looking at the top 20 common digrams for ciphertext 1 (page #) the letters 'LJ' has the highest frequency. It's possible that the two letters would be the most common English digram 'TH'.

The second ciphertext would be the Vigenère cipher as the index of coincidence is also close to 0.0385, the digrams can be the basis of breaking the ciphertext, and the key can be determined by using the autocorrelation graph. In ciphertext 2's autocorrelation graph, it was found that in between each peak was distanced by seven. Comparing to other graphs, it was very hard to determine the distances of each period.

The simple substitution cipher would be the third ciphertext because the digram's frequency and the index of coincidence was found to have the highest result of all. The substring letters 'PA' (page #) were in the top 4 most frequent characters. Here, 'PA' could be assumed as 'TH' in plaintext. The letter 'P' by itself could be the most common letter 'e' or the second most common letter 't'. I noticed that the most common English letter 'E' was not present in any of the frequency analysis. This letter must be encrypted to a letter in the top ten frequencies. Therefore ciphertext 3 was encrypted using the substitution cipher because the letter has been replaced with a different character.

Lastly, the transposition cipher would be the fourth ciphertext because the common English letters are listed at the top of the frequency chart. The characters won't change when they're encrypted, transposition arranges the plaintext in an array then re-arranges them according to the defined permutation. It was also found that the index of coincidence was also close to 0.070.

Section 3 – Procedures for Cryptanalysing Ciphertexts

The procedure I can use to cryptanalyse the simple substitution is to make use of the single and the digram frequency tables. As mentioned in section 2, the digram 'PA' was the most frequently used. Therefore, here I can assume that 'PA' are letters 'TH'. Where 'TH' is the most common pair of letters in English. The second most frequent letter was 'T' which I can assume is the letter 'E'. Now that I have a word spelled with 'THE' I can apply it to my key, view the text and assume the remaining letters. By applying the same principle and assuming common digrams to be common English letters, I will be able to decrypt the whole ciphertext.

To break the Vigenère cipher, I can use the autocorrelation graph to determine the distance between each peak. Using this distance, this can be used as the key to decrypt the ciphertext. As mentioned in section 2, the distance was seven in between each peak of the autocorrelation graph for ciphertext 2.

The transposition cipher can be broken by using the digram frequencies, find them in the ciphertext, then determine where the words start. Here I can continue to try and move the letters around to get a legitimate text. When a word has been found, I can apply it to my final decryption key, and find more misspelled words.

2 by 2 Hill ciphers can be broken into by using the common digrams. As found in the statistics, 'LJ' was the most frequent digram. Most likely this can start with 'TH'. The letters would need to be translated to their number (A = 0, B = 1, C = 2, … Z = 25) then placed in to a matrix. $\begin{bmatrix} T \\ H \end{bmatrix} = \begin{bmatrix} 19 \\ 7 \end{bmatrix}$. Since we are dealing with 2x2 hill ciphers, the matrix needs to be so. Therefore, we can assume the following letters after 'TH' would be 'EY' $\begin{bmatrix} T & E \\ H & Y \end{bmatrix} = \begin{bmatrix} 19 & 4 \\ 7 & 24 \end{bmatrix}$. The formula for calculating the key is:

$$K = CP^{-1} \, mod \; 26$$

Where K is the key, C is the ciphertext, P is the plaintext, and mod 26 is the number of letters in the alphabet excluding space.

I found 'LJ' to have the following ciphertext letters 'WI'. It was found throughout the ciphertext that the word 'LJWI' was quite frequent throughout the ciphertext. Here the matrix for 'THEY' we assume is the plaintext of the ciphertext 'LJWI'. Using this I can get place them in their matrixes, map the letters to their number, and calculate it using the formula. Although there can be other possible plaintext words such as 'THIN', 'THER', 'THEI', 'THEN', and so forth, finding the matrix key becomes a trial and error. The letters 'LJ' could not be 'TH' they could be some other common digram.

Section 4 – Decrypting the Random Simple substitution, Vigenère, and Transposition Ciphers

In obtaining the plaintext for the random simple substitution, it was found that the key was "qcvstbjadefghiklmnopruwxyz". This was found by firstly analysing the most frequent trigram characters which were 'PAT'. I assumed 'PAT' was the word 'THE' which is the most common trigram in English. Next, I assumed the letter 'D' would be the letter 'I' because there were spots in the ciphertext where the letter would be by itself. The letters 'DI' were also common which I assumed they would end up being the word 'in'.

I was able to figure out the second letter to be 'any' since we had two of the three letters figured out. The second word in the second sentence was 'fact' as I thought of four-letter words that had the letter 'a' in the second position and 't' in the last position. The third letter turned out to be 'trade' assuming the word with knowing three of its letters. The fourth letter was 'manager'. A couple more words were figured out with the help of filling out the missing letters of the word.

Alphabet	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
key	q	c	v	s	t	b	j	a	d	e	f	g	h	i	k	l	m	n	o	p	r	u	w	x	y	z

Random simple substitution cipher (Cyptool 1 > Encrypt/Decrypt > Symmetric (classic) > Substitution/Atbash > Key = qcvstbjadefghiklmnopruwxyz > Decrypt):

> *"isclosing any trade secrets. In fact, the manager said afterwards that Mr. Kurtz's methods had ruined the district. I have no opinion on that point, but I want you clearly to understand that there was nothing exactly profitable in these heads being there. They only showed that Mr. Kurtz lacked restraint in the gratification of his various lusts, that there was something wanting in him--some small matter which, when the pressing need arose, could not be found under his magnificent eloquence. Whether he knew of this deficiency himself I can't say. I think the knowledge came to him at last--only at the very last. But the wilderness had found him out early, and had taken on him a terrible vengeance for the fantastic invasion. I think it had whispered to him things about himself which he did not know, things of which he had no conception till he took counsel with this great solitude--and the whisper had proved irresistibly fascinating. It echoed loudly within him because he was hollow at th"*

I retrieved the plaintext of the Vigenère cipher using Cryptool 1. Since we know that the autocorrelation can be used to break the Vigenère cipher, it was found that the graph for ciphertext 2 had a consistent correlation where every peak was spaced out to be 7. Here I assumed the derived key length would be 7, thus generating the derived key ‘OCBKZGS’ on Cryptool 1.

Vigenère cipher to plaintext (Cryptool 1 > Analysis > Symmetric Encryption (Classic) > Ciphertext-Only > Vigenère):

> *“Pes STiRRing at MY backK, iN The gLoW Of fiReS, WithIn The paTieNt woOdS, ThoSE bROken PhRaseS CaMe backK tO Me, weRe heard again in Their omInOUs anD teRrifYiNg simPlIcitY. i reMembEred hiS abJect pLeading, HiS abjeCt ThreaTs, The coLoSSal SCaLe of hIs Vile dEsIRes, THe MeannEsS, The TOrMent, THe TempeStUOus aNgUish oF hIS soUL. ANd laTEr ON I seEmed to SEe his coLlected LaNguid MaNNer, WHeN he saId ONe daY, 'This loT of ivoRY nOW is REaLlY miNe. the CoMpaNY diD nOT paY FoR it. I cOlLecteD iT MYseLf aT a veRY gReaT PeRSonaL rISk. I aM afRaid TheY wilL tRY to cLaIM it aS theirS ThOUgh. H'M. IT is a dIfficulT caSe. What dO YoU ThINk I oUghT to dO--reSisT? eh? i WanT No MOre THaN jusTIce.'... He waNted no mOre Than JUSTice--No MOre THaN jusTIce. I ranG the belL before a mahogaNY dOor oN the fiRSt flooR, and WhilE I WaiteD he SeemEd TO staRe aT me oUt Of the GlaSsy panel--staRe With THaT Wide and immeNse StaRE eMbracIng, condEmNing, lOaThing alL The UNiVerse. i seemed To hear THe WhispEred”*

As I was not sure what the length of the key was, I formatted the ciphertext from blocks of 1 to 7 and try to see if I could re-arrange any letters to form into a word. When I split up the text to blocks of 7, I was able to arrange the first block to “have_a_”, wrote down its shift for the key and applied it into CrypTool. The key for the transposition cipher is [6,5,4,2,7,3,1]. Using the Brute-Force Transposition Analysis in CrypTool 2, the key is the same.
Transposition cipher to plaintext (Cyptool 2 > Templates > Transposition Brute-Force Analysis):

> *“have a voice too and for good or evil mine is the speech that cannot be silenced Of course a fool what with sheer fright and fine sentiments is always safe Who s that grunting You wonder I didn t go ashore for a howl and a dance Well no I didn t Fine sentiments you say Fine sentiments be hanged I had no time I had to mess about with white lead and strips of woolen blanket helping to put bandages on those leaky steam pipes I tell you I had to watch the steering and circumvent those snags and get the tin pot along by hook or by crook There was surface truth enough in these things to save a wiser man And between whiles I had to look after the savage who was fireman He was an improved specimen he could fire up a vertical boiler He was there below me and upon my word to look at him was as edifying as seeing a dog in a parody of breeches and a feather hat walking on his hind legs A few months of training had done for that really fine chap He squinted at the s ThPCozR”*

Section 5 – Decrypting the Hill Cipher

I needed to find the non-overlapping digram frequencies. We are doing this to help determine the key matrix for decryption. To prevent this, it was achieved by:

- Defining the alphabet to include uppercase and lowercase letters with no space.
- Using the format text document tool to remove spaces.
- Using the format text document tool to split into blocks of size 2.
- Using the n-gram analysis tool to count the bigrams.

The result:

vm im xy pk gl ob xk tw fg og si tw st kr wo bk lm eh pg ft ui v. Uz el bi mp gj ,k yf v, oj dp co hc xd co zj cu pw dt ac x, lj wi xy nu cp cx si an ql bo uo oz uv lm og nj ec uo uj wb mu bb is .L ju qx qm ti kw bl je cp gk mx ks tx yx tg nm us ib oc su jh ot ty nl jw oe cy vs ge cw yl jk lb oo zp ke hy nc tq yb .Z jc vo fg ob ,g za nk ,Q gh rg kl hs j, kc sv xe ic qv zf yd ue mx at qs gb os tf sg et pc su ou jl mx nk ki k. Af cx gh pt mw uq ns ep ge uc rb og st wv kd cx bk fu wv ho lv ui lm tc s- -l cr ws bo cg ze pk tt eb ek ec lj ep gn ws jg bs lj g. .. ." Gc qe nc qv lx yd yi kc xl ji zy fc to gy yd cb o! Lj wi xy vb cd ck hd tq ct eh ,g na fc xt qb op cl ms i: pq bK ta xq af ud jc eb nm ce pr si gq ze ge j- -k wn zd ns yj n, ou yt a. Ax wv cp ob yn mr uq ej mr lm gl wp m. Wi lc kf lo uu ,o ry cs do gq qz xk lj ob eh u. Mo ob sp wy gc qr ?Y wv t, gc qg ee ow cy yS qs tw zy nl je pm cz uh dj cu oq pm ud rg zb kf gc sg cs ty qj ej cw gw sm qs ;l cr zu pk hy lj eh cg ba sy wp wi ec ku bo wb do ws bo mq ud cq oz xy li xc kr wd ta cx pq ns yn em lm sj oo za na jc gp wb eg vv uj -o eo h. Wn vk rb xq eq wn ,t qa -- yn mq uf g, yq zw ,o zg zx qf g. Ta uo hs w, gt tG my in ,h nm ce vg fu cq jd yn gh pt yv sg an r, ye X

If the given ciphertext was = 'ABCDEF', CrypTool would calculate the frequencies like so:

<u>AB</u>CDEF

A**<u>BC</u>**DEF

AB**<u>CD</u>**EF

ABC**<u>DE</u>**F

ABCD**<u>EF</u>**

The list would have been bigger, and the decryption would have been done incorrectly.

non-overlapping bigram frequencies:

No.	Substring	Frequency (in %)	Frequency
1	lj	1.3405	5
2	lm	1.3405	5
3	ob	1.3405	5
4	bo	1.0724	4
5	cx	1.0724	4
6	eh	1.0724	4
7	wv	1.0724	4
8	xy	1.0724	4
9	yn	1.0724	4
10	cp	0.8043	3
11	ec	0.8043	3
12	gc	0.8043	3
13	ge	0.8043	3
14	gh	0.8043	3
15	jc	0.8043	3
16	mx	0.8043	3
17	nm	0.8043	3
18	ns	0.8043	3
19	og	0.8043	3
20	pk	0.8043	3
21	qs	0.8043	3
22	sg	0.8043	3
23	si	0.8043	3

24	tw	0.8043	3
25	ud	0.8043	3
26	uo	0.8043	3

As mentioned in section 3, the formula for the key is:

$$K = CP^{-1}\ mod\ 26$$

Where K is the key, C is the ciphertext, P is the plaintext, and 26 is the number of characters excluding the space. Knowingly that this is a two by two cipher, I needed a two by two matrix for the ciphertext and the plaintext.

In finding these matrixes, I used the top non-overlapping digram 'LJ' and located them in the ciphertext.

> vmi mxypkglob xktwfg ogsitwstk rwobklm
> ehpgftuiv. Uzelbimpgj, kyfv, ojd pcohcxd co zjcu pwd tacx, ljwi xyn
> ucpcx si an qlbouoozuvlm ognjecuouj wb mubbis. Lju qxqmtik wb lje
> cpgkmxkst xyx tgn musi bocsuj hottyn ljwoe cyvsgec wylj klboozpkehyn
> ctqyb. Zjc vofgob, gz ank, Q ghrgklhsj, kcs vxei cqv zfyduemxa tq s
> gbost fsget pcsuouj lmx nkkik. Afcx ghptmwu qnsep geu crbogstwvk dcxb
> kfuwvh ol vuilmtcs--lcr wsbo cgzepktte bekec lje pgnw sj gbsljg....
>
> "Gcq encqvl xydy ikcx lji zyfctogy ydcbo! Ljwi xyv bc dckhd tq cteh, gn
> afcx tq bopclm si: pqb K taxqafu djce bnmcepr si gqze gej--kwnz dnsyjn,
> ouyta. A xwvcpobyn m ruqejmr lmglwpm. Wi lckf louu, or ycs do gqqz
> xkljobehu. Moob s pwygcqr? Ywvt, gcq gee owcyy S qstwzyn lje pmc zuh
> djc uoqpm ud rgzbkfg cs g cst yqjejcw g wsmqs; lcr zup khyljehc gbas ywp
> wiec kubo wb do wsbo mqu dc qo zxyl ix ck rwd tacx pqnsyn emlms jooz an
> a jcgp wb egvvuj-oeoh. Wn vkrb xqeq wn, tqa--ynmqufg, yqzw, ozgzxqfg.
> Tauohsw, gtt G myin, hnmcev gf ucqjdyn ghptyvsganr, ye
>
> X

I had found that there were a couple of three letter words, and some four or more. The three letter words did contain the most common digram at the start. This could decrypt to the most common trigram in English 'THE'. However, I noticed that some of them had the letters 'E', 'U', and 'I' as the third letter. This could mean that some of them could decrypt to a different common trigram. The four-letter words, 'LJWI', 'WYLI' were also found in the text. They could translate to common quadrams, 'THEY', 'THAN', 'THAT', 'THEM', 'THIS', 'THEP', 'THEC', 'THER', 'THIN, and 'THEI'.

I used the four-letter ciphertexts as the matrix,

$$C = \begin{bmatrix} L & W \\ J & I \end{bmatrix} = \begin{bmatrix} 11 & 22 \\ 9 & 8 \end{bmatrix} \text{(Converted to their corresponding integers)}$$

Used the predicted plaintext as the matrix,

$$P^{-1} = \begin{bmatrix} T & I \\ H & N \end{bmatrix} = \begin{bmatrix} 19 & 8 \\ 7 & 13 \end{bmatrix}$$

$$= \begin{bmatrix} 13 & 2 \\ 5 & 5 \end{bmatrix} \text{(inversed via Timur:planetcalc)}$$

Thus, getting the formula,

$$K = \begin{bmatrix} 11 & 22 \\ 9 & 8 \end{bmatrix} \begin{bmatrix} 13 & 2 \\ 5 & 5 \end{bmatrix}$$

$$K = \begin{bmatrix} 19 & 2 \\ 1 & 6 \end{bmatrix} \text{ (calculated via Wolfram|Alpha)}$$

The key must be inverted to get the decryption key. However, it is impossible to do so in this case. I was able to invert the final key having 'LJEH' as the ciphertext and 'THIN' as the plaintext. The key turned out to be

$$K^{-1} = \begin{bmatrix} 11 & 6 \\ 18 & 25 \end{bmatrix}$$

The calculated matrix was then used in CrypTool (CrypTool 1 > Encrypt/Decrypt > Symmetric (Classic) > Hill > Entering number key matrix > Decrypt). The text decrypts as:

> *"xCK cvGbYGjGt fsnUxI IyQknUKva Zkahcfq*
> *gnPUXVecV. kBelfKcPUl, wkJd, EDp DQyzOLX Ma RNoM jqP zyOL, JnsU vGR*
> *qqDOL Qk wJ YvtgWiaREpfq IyXfeiWiUd KN KUTTCi. jnC kXyUTea KN Jne*
> *iPUYUfsKv vGt Bml KUQk tgMGUd jIRRIR Jnkae igZkiei okJn iTtgaRbYgnIR*
> *CHyIn. RNo dExIGt, Wx wJk, y ufdMiTvMl, wMG rNWo gEX PZazeisbi vO k*
> *itgKv hUYcF NMGWiUd fqB vsSea. yBOL ufphqWC kloEv Ycm WbHIyKvShK LOLh*
> *cNWShj It zecfqfAm--nWF wetg cuBebYRRo hCqei JnE vmlw eZ sFkJnE....*
>
> *"EgE YtgEHB vGLi eaOL Jnk pkJCHIyC cXMtg! jnsU vGD rG roypx vO CHgn, ml*
> *YBOL vO tgDQfq Qk: Teh C zyXyYBc XNoo htiwsJf Qk IoBe Ycl--wuZL dlowNZ,*
> *kaszy. a TShqDGtIR o RCkMpoR fqGjabq. wU boyz NYMW, iF eMG HY IooJ*
> *fsJnGtgnq. GgGF k LkaKgEF? EShr, EgE YcO uAOCc O sKvelIR JnE viC xup*
> *xNo WikzK Ud bWxhcxI MG s aKv eUtqNoM S weyQm; nWF xub YnSJngnc udSM Aab*
> *sUei wctg KN HY wetg yQc Xg Ea RvGT mH ka ZqP zyOL TeloIR isfqG lgGp aJ*
> *W NoSn KN qmLLUd-cwyz. UZ RAbH Xyuw uZ, vOq--UtimExI, eUdw, aRWxXyxI.*
> *ZyWivMM, SRR W kGMr, dtiwsF wN WgEDpIR ufphgZkiwJF, ec*
>
> *D"*

As shown above, the text wasn't decrypted correctly. The whole process was repeated whilst using other common digrams to predict the plaintext of the ciphertexts. The following table below are the results:

Ciphertext	Plaintext prediction	Plaintext matrix	Inverted Plaintext matrix
LJWI	THEY, THIN, THAN, THAT, THIS, THEP, THEC, THIN, THER, THEI, TONE, HELP, SPIN, SAND, TAND, PAND, WAND	$\begin{bmatrix} 19 & 4 \\ 7 & 24 \end{bmatrix}, \begin{bmatrix} 19 & 8 \\ 7 & 13 \end{bmatrix}, \begin{bmatrix} 19 & 0 \\ 7 & 13 \end{bmatrix}, \begin{bmatrix} 19 & 4 \\ 7 & 24 \end{bmatrix}, \begin{bmatrix} 19 & 8 \\ 7 & 18 \end{bmatrix}, \begin{bmatrix} 19 & 4 \\ 7 & 15 \end{bmatrix}, \begin{bmatrix} 19 & 4 \\ 7 & 2 \end{bmatrix}, \begin{bmatrix} 19 & 8 \\ 7 & 13 \end{bmatrix}, \begin{bmatrix} 19 & 4 \\ 7 & 17 \end{bmatrix}, \begin{bmatrix} 19 & 4 \\ 7 & 8 \end{bmatrix}, \begin{bmatrix} 19 & 13 \\ 14 & 4 \end{bmatrix}, \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix}, \begin{bmatrix} 18 & 8 \\ 15 & 13 \end{bmatrix}, \begin{bmatrix} 18 & 13 \\ 0 & 3 \end{bmatrix},$	No Inverse, $\begin{bmatrix} 13 & 2 \\ 5 & 5 \end{bmatrix}$, No inverse, No inverse, No inverse, $\begin{bmatrix} 21 & 10 \\ 11 & 11 \end{bmatrix}$, No inverse, $\begin{bmatrix} 13 & 2 \\ 5 & 5 \end{bmatrix}, \begin{bmatrix} 25 & 14 \\ 5 & 5 \end{bmatrix}$, No inverse, No inverse, $\begin{bmatrix} 19 & 19 \\ 14 & 21 \end{bmatrix}$, No inverse, No inverse,
LJOB			
LJEH			
LJWO			
BKLM			
LMTC			
EMLM			
LMGL			
PCLM			
UILM			
GLOB			
RWOB			

OBKL FGOB MOOB		$\begin{bmatrix}19 & 13\\ 0 & 3\end{bmatrix}, \begin{bmatrix}15 & 13\\ 0 & 3\end{bmatrix}, \begin{bmatrix}22 & 13\\ 0 & 3\end{bmatrix}$	$\begin{bmatrix}11 & 13\\ 0 & 9\end{bmatrix}, \begin{bmatrix}7 & 13\\ 0 & 9\end{bmatrix}$, No inverse

'LJ', 'OB', and 'LM' are the top digram frequencies.

In the table below, each ciphertext matrix and each inverted matrix are calculated to get the key, then inverted and used to try decrypt the text.

Ciphertext matrixes (C)	Inverted matrixes (P^{-1})	Equation	Calculations with no error (final key)	Correct Decryption?
$\begin{bmatrix}11 & 22\\ 9 & 8\end{bmatrix}$	$\begin{bmatrix}13 & 2\\ 5 & 5\end{bmatrix}, \begin{bmatrix}21 & 10\\ 11 & 11\end{bmatrix}, \begin{bmatrix}25 & 14\\ 5 & 5\end{bmatrix}, \begin{bmatrix}19 & 19\\ 14 & 21\end{bmatrix}, \begin{bmatrix}11 & 13\\ 0 & 9\end{bmatrix}, \begin{bmatrix}7 & 13\\ 0 & 9\end{bmatrix}$	$K = CP^{-1}\ mod\ 26$ Decryption key is K^{-1} (Inverted)	Nil, error inverting key	N/A
$\begin{bmatrix}11 & 14\\ 9 & 1\end{bmatrix}$			$\begin{bmatrix}19 & 2\\ 10 & 3\end{bmatrix}, \begin{bmatrix}11 & 6\\ 14 & 1\end{bmatrix}, \begin{bmatrix}11 & 6\\ 18 & 25\end{bmatrix}, \begin{bmatrix}6 & 5\\ 19 & 9\end{bmatrix}, \begin{bmatrix}16 & 23\\ 19 & 23\end{bmatrix}, \begin{bmatrix}14 & 25\\ 19 & 23\end{bmatrix}.$	No
$\begin{bmatrix}11 & 4\\ 9 & 7\end{bmatrix}$			$\begin{bmatrix}11 & 6\\ 18 & 25\end{bmatrix}, \begin{bmatrix}3 & 10\\ 22 & 23\end{bmatrix}, \begin{bmatrix}3 & 10\\ 0 & 21\end{bmatrix}, \begin{bmatrix}14 & 1\\ 5 & 3\end{bmatrix}, \begin{bmatrix}8 & 1\\ 19 & 23\end{bmatrix}, \begin{bmatrix}20 & 9\\ 19 & 23\end{bmatrix}.$	No
$\begin{bmatrix}11 & 22\\ 9 & 14\end{bmatrix}$			Nil, error inverting key	N/A
$\begin{bmatrix}1 & 11\\ 10 & 12\end{bmatrix}$			Nil, error inverting key	N/A
$\begin{bmatrix}11 & 19\\ 12 & 2\end{bmatrix}$			Nil, error inverting key	N/A
$\begin{bmatrix}4 & 11\\ 12 & 12\end{bmatrix}$			Nil, error inverting key	N/A

$\begin{bmatrix} 11 & 6 \\ 12 & 11 \end{bmatrix}$			$\begin{bmatrix} 23 & 0 \\ 9 & 1 \end{bmatrix}$, $\begin{bmatrix} 7 & 6 \\ 17 & 11 \end{bmatrix}$, $\begin{bmatrix} 7 & 6 \\ 25 & 21 \end{bmatrix}$, $\begin{bmatrix} 1 & 17 \\ 2 & 5 \end{bmatrix}$, $\begin{bmatrix} 17 & 25 \\ 12 & 15 \end{bmatrix}$, $\begin{bmatrix} 23 & 17 \\ 12 & 15 \end{bmatrix}$.	No
$\begin{bmatrix} 15 & 11 \\ 2 & 12 \end{bmatrix}$			Nil, error inverting key	N/A
$\begin{bmatrix} 20 & 11 \\ 8 & 12 \end{bmatrix}$			Nil, error inverting key	N/A
$\begin{bmatrix} 6 & 14 \\ 11 & 1 \end{bmatrix}$			Nil, error inverting key	N/A
$\begin{bmatrix} 17 & 14 \\ 22 & 1 \end{bmatrix}$			$\begin{bmatrix} 21 & 0 \\ 9 & 17 \end{bmatrix}$, $\begin{bmatrix} 19 & 24 \\ 23 & 5 \end{bmatrix}$, $\begin{bmatrix} 19 & 24 \\ 11 & 19 \end{bmatrix}$, $\begin{bmatrix} 21 & 3 \\ 8 & 7 \end{bmatrix}$, $\begin{bmatrix} 17 & 9 \\ 8 & 21 \end{bmatrix}$, $\begin{bmatrix} 23 & 3 \\ 8 & 21 \end{bmatrix}$.	No
$\begin{bmatrix} 14 & 10 \\ 1 & 11 \end{bmatrix}$			Nil, error inverting key	N/A
$\begin{bmatrix} 5 & 14 \\ 6 & 1 \end{bmatrix}$			$\begin{bmatrix} 3 & 18 \\ 19 & 7 \end{bmatrix}$, $\begin{bmatrix} 19 & 24 \\ 23 & 5 \end{bmatrix}$, $\begin{bmatrix} 19 & 24 \\ 11 & 19 \end{bmatrix}$, $\begin{bmatrix} 21 & 3 \\ 8 & 7 \end{bmatrix}$, $\begin{bmatrix} 17 & 9 \\ 8 & 21 \end{bmatrix}$, $\begin{bmatrix} 23 & 3 \\ 8 & 21 \end{bmatrix}$.	No
$\begin{bmatrix} 12 & 14 \\ 14 & 1 \end{bmatrix}$			Nil, error inverting key	N/A

References

Frequency - Crypto Programs. 2018. Frequency - Crypto Programs. [ONLINE] Available at: http://www.cryptoprograms.com/tools/frequency. [Accessed 2 August 2018].

Index of Coincidence Calculator - Online IC Cryptanalysis Tool. 2018. Index of Coincidence Calculator - Online IC Cryptanalysis Tool. [ONLINE] Available at: https://www.dcode.fr/index-coincidence. [Accessed 2 August 2018].

Practical Cryptography. 2018. Practical Cryptography. [ONLINE] Available at: http://practicalcryptography.com/cryptanalysis/text-characterisation/index-coincidence/#summary. [Accessed 2 August 2018].

Frequency Analysis Tool - Letter Counter - Online Software Tool. 2018. Frequency Analysis Tool - Letter Counter - Online Software Tool. [ONLINE] Available at: https://www.dcode.fr/frequency-analysis. [Accessed 5 August 2018].

Crypto Corner. 2018. Frequency Analysis: Breaking the Code - Crypto Corner. [ONLINE] Available at: http://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html. [Accessed 5 August 2018].

Code My Road. 2018. Frequency Analysis Attack – Breaking the Substitution Cipher | Code My Road. [ONLINE] Available at: https://codemyroad.wordpress.com/2014/03/08/frequency-analysis-attack-breaking-the-substitution-cipher/. [Accessed 5 August 2018].

Crypto Corner. 2018. Kasiski Analysis: Breaking the Code - Crypto Corner. [ONLINE] Available at: http://crypto.interactive-maths.com/kasiski-analysis-breaking-the-code.html. [Accessed 5 August 2018].

Crypto Corner. 2018. Simple Transposition Ciphers - Crypto Corner. [ONLINE] Available at: http://crypto.interactive-maths.com/simple-transposition-ciphers.html. [Accessed 5 August 2018].

Index of Coincidence Calculator - Online IC Cryptanalysis Tool. 2018. Index of Coincidence Calculator - Online IC Cryptanalysis Tool. [ONLINE] Available at: https://www.dcode.fr/index-coincidence. [Accessed 5 August 2018].

shodhganga. 2018. CH5: CRYPTANALYSIS OF VIGENERE CIPHER AND SUBSTITUTION CIPHER. [ONLINE] Available at: http://shodhganga.inflibnet.ac.in/bitstream/10603/26543/10/10_chapter5.pdf. [Accessed 10 August 2018].

SpringerLink. 2018. Transposition Ciphers | SpringerLink. [ONLINE] Available at: https://link.springer.com/chapter/10.1007%2F0-387-23804-2_8. [Accessed 10 August 2018].

A Data Analyst. 2018. Difference between substitution and transposition in terms of encryption - A Data Analyst. [ONLINE] Available at: http://adataanalyst.com/information-security/difference-substitution-transposition-terms-encryption/. [Accessed 11 August 2018].

Practical Cryptography. 2018. Practical Cryptography. [ONLINE] Available at: http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-hill-cipher/. [Accessed 12 August 2018].

Practical Cryptography. 2018. Practical Cryptography. [ONLINE] Available at: http://practicalcryptography.com/cryptanalysis/text-characterisation/index-coincidence/. [Accessed 13 August 2018].

Practical Cryptography. 2018. Practical Cryptography. [ONLINE] Available at: http://practicalcryptography.com/cryptanalysis/letter-frequencies-various-languages/english-letter-frequencies/. [Accessed 14 August 2018].

Timur : planetcalc member. 2018. Online calculator: Modular inverse of a matrix. [ONLINE] Available at: https://planetcalc.com/3324/. [Accessed 14 August 2018].

Wolfram|Alpha: Computational Intelligence. 2018. Wolfram|Alpha: Computational Intelligence. [ONLINE] Available at: http://www.wolframalpha.com. [Accessed 15 August 2018].

mvngu. 2018. shift cipher | mvngu. [ONLINE] Available at: https://mvngu.wordpress.com/tag/shift-cipher/. [Accessed 15 August 2018].

Tools

CrypTool - Esslinger, B. (2018). Version 1.4.41. Available at: https://www.cryptool.org/en/cryptool1
CrypTool 2 - Esslinger, B. (2018). Version 2.1. Available at: https://www.cryptool.org/en/cryptool2