This assignment will examine the history of cryptology and common ciphers that have been used in the past. From there information will be encrypted and decrypted using matrices and frequency analysis.

Cryptology

Year 11 Maths C

Lauren Baillie - 05774

Question 1

Key Words

Encryption
To make a message unreadable

Decryption
To make an unreadable message readable using a key.

Cryptography
The process of encryption.

Cryptanalysis
The process of decryption.

Cryptology
The field of study involving both cryptography and cryptanalysis.

Polyalphabetic Ciphers
A method of encryption where multiple alphabets or shifts are used in order to flatten the distribution of letter frequencies.

One time pad
A method of encryption where a set of random numbers is generated and used as a key to encipher and decipher a message. Both parties must have the key of the message cannot be decrypted. However, so far the one time pad has proved unbreakable.

Plaintext
The message being sent.

Ciphertext
The encrypted message.

Quantum cryptography
A method of encryption where photons of light are polarized in a certain direction by person A. Person B examines the type of polarization used which can then be translated to binary code and from there to English.

Question 2: Solving Mono-Alphabetic Ciphers Using Frequency Analysis

Frequency of Different Letters in the Ciphertext	
w	0
Y	0
L	1
U	1
X	1
K	3
T	3
J	4
B	5
Q	6
G	6
F	8
P	8
A	9
V	9
C	10
D	11
R	11
N	12
E	14
I	15
Z	21
H	22
O	22
m	30
s	38

List of Most Frequent Letters in the English Language vs. Most Frequent Letters in the Ciphertext	
E	S
T	M
A	O
O	H
I	Z
N	I
S	E
R	N
H	Y
D	D
L	C
U	V
C	A
M	P
F	F
Y	G
W	Q
G	B
P	J
B	T
V	K
K	X
X	U
Q	L
J	Y
Z	W

EO EM HIO IHNV TREOOSH OSUO OCZO CZM CEMOIREDZNNV BSSH PMSA OI RSNZV SHDRVJOSA FSMMZGSM. FPMED TZM ZNMI PMSA BV ZKREDZH ZFSREDZH MNZQSM OI DIHQSV MSDRSO DIFFPHEDZOEIHM. MNZQSM XHST OCS MSDRSO FSZHEHGM IK OCSMS MIHGM ZHA OCSV DIPNA MPBMSLPSHONV BS PMSA OI MEGHZN FZHV OCEHGM, ZHA JSRCZJM SQSH CSNJSA BREHG OCS MNZQSM OI KRSSAIF.

The two letter words in the Ciphertext are EO, EM, OI, BV, OI, IK, BS, OI, OI.

Two Letter Words in the Ciphertext and Their Frequencies	
OI	4
EO	1
EM	1
BV	1
IK	1
BS	1

As there are too many combinations and not enough of a difference in frequency this is not a viable starting point.

The three letter words used in the Ciphertext are HIO, CZM, TZM, OCS, ZHA, ZHA, OCS.

Three Letter Words in the Ciphertext and Their Frequencies	
OCS	2
ZHA	2
CZM	1
TZM	1
HIO	1

The two most common three letter words in the English language are “and” and “the”. By examining the frequency tables it can be seen that OCS best fits with “the” rather than “and” as the letter in each word have a closer frequency to their corresponding letter.

ET EM HIT IHNV TRETTEH TEUT THZT HZM HEMTIREDZNNV BSSH PMSA TI RENZV EHDRVJTEA FEMMZGEM. FPMED TZM ZNMI PMEA BV ZKREDZH ZFEREDZH MNZQEM TI DIHQEV MEDRET DIFFPHEDZTEIHM. MNZQEM XHST THE MEDRET FEZHEHGM IK THEME MIHGM ZHA THEV DIPNA MPBMELPEHTNV BE PMEA TI MEGHZN FZHV THEHGM, ZHA JERHZJM EQEH CENJEA BREHG THE MNZQEM TI KREEAIF.

By examining THZT and HZM and the frequency table it is logical to assume that “Z” = “A” as that is a very common word and all three letter words beginning with h have a as the second letter.

ET EM HIT IHNV TRETTEH TEUT THAT HAM HEMTIREDANNV BSSH PMEA TI RENAV EHDRVJTEA FEMMAGEM. FPMED TAM ANMI PMEA BV AKREDAH AFEREDAH MNAQEM TI DIHQEV MEDRET DIFFPHEDATEIHM. MNAQEM XHST THE MEDRET FEAHEHGM IK THEME MIHGM AHA THEV DIPNA MPBMELPEHTNV BE PMEA TI MEGHAN FAHV THEHGM, AHA JERHAJM EQEH CENJEA BREHG THE MNAQEM TI KREEAIF.

By examining AHA it is logical to assume that the decrypted version of it is “and” considering it starts with “A” and is a three letter word. Furthermore, “and” is the most common three letter word besides “the” in the English language and that has already been decrypted. Also, AHA is the only word besides “the” that appears twice in the Ciphertext.

Therefore, “H” = “N” and “A” = “D”

ET EM NIT INNV TRETTEN TEUT THAT HAM HEMTIREDANNV BSSN PMED TI RENAV ENDRVJTED FEMMAGEM. FPMED TAM ANMI PMEA BV AKREDAN AFEREDAN MNAQEM TI DINQEV MEDRET DIFFPNEDATEINM. MNAQEM XNST THE MEDRET FEANENGM IK THEME MINGM AND THEV DIPND MPBMELPENTNV BE PMED TI MEGNAN FANV THENGM, AND JERHAJM EQEN CENJED BRENG THE MNAQEM TI KREEDIF.

So far the vowels that have been used are “E” and “A”. That leaves the vowels “I”, “O” and “U”.

From examining NIT, it is known that it must be a vowel and the only vowels remaining are “I”, “O” and “U”. Also, the possible words that are three letters and begin with “N” and end with “T” are nit, not and nut. From this list the most common word is not. Therefore “I” = “O”

ET EM NOT ONNV TRETTEN TEUT THAT HAM HEMTOREDANNV BSSN PMED TO RENAV ENDRVJTED FEMMAGEM. FPMED TAM ANMO PMEA BV AKREDAN AFEREDAN MNAQEM TO DONQEV MEDRET

DOFFPNEDATEONM. MNAQEM XNST THE MEDRET FEANENGM OK THEME MONGM AND THEV DOPND MPBMELPENTNV BE PMED TO MEGNAN FANV THENGM, AND JERHAJM EQEN CENJED BRENG THE MNAQEM TO KREEDIF.

So far, NOT, THAT, TO, TO, THE, AND, TO, AND, THE and TO are all of the completed words. The words all make sense. Therefore, no errors can be seen currently.

ET, TEUT, HAM, OK, THEME, THEV, BE, EQEN, are all of the words that are missing one letter.

By examining ET and EM it is logical to assume that “E” is a vowel. The remaining vowels are “I” and “U”. By inspecting the frequency table it can be seen that “E” is closer in frequency to “I” than “U”. Therefore, “E” = “I”

IT IM NOT ONNV TRITTEN TEUT THAT HAM HIMTORIDANNV BSSN PMED TO RENAV ENDRVJTED FEMMAGEM. FPMID TAM ANMO PMEA BV AKRIDAN AFERIDAN MNAQEM TO DONQEV MEDRET DOFFPNIDATIONM. MNAQEM XNST THE MEDRET FEANINGM OK THEME MONGM AND THEV DOPND MPBMELPENTNV BE PMED TO MIGNAN FANV THINGM, AND JERHAJM EQEN CENJED BRING THE MNAQEM TO KREEDIF.

The two most common words beginning with “Ha” (HAM) are “had” and “has” but as “A” = “D” it is safe to assume that “M” = “S”. Furthermore, it is logical to assume from IM that “M” = “S” as the other common letters for this word, “T” and “N” have already been used. While, these letters are not extraordinarily close in the frequency table, they are close enough that the claim that “M” = “S” is legitimate.

IT IS NOT ONNV TRITTEN TEUT THAT HAS HISTORIDANNV BSSN PSED TO RENAV ENDRVJTED FESSAGEM. FPSID TAS ANSO PSEA BV AKRIDAN AFERIDAN SNAQES TO DONQEV SEDRET DOFFPNIDATIONS. SNAQES XNST THE MEDRET FEANINGS OK THESE SONGS AND THEV DOPND SPBSELPENTNV BE PSED TO SIGNAN FANV THINGS, AND JERHAJS EQEN CENJED BRING THE SNAQES TO KREEDIF.

THEV has five possible words; “thee”, “them”, “then”, “thew” and “they”. “Thee” and “then” can be eliminated because “E” and “N” have already been used. “Thew” can also be eliminated because it is an uncommon word and unlikely to be within the plaintext. When looking at the available plaintext, and them is not grammatically correct, so for this exercise it is safe to assume to “them” can be eliminated. This leaves “they” and therefore means that “V” = “Y”.

IT IS NOT ONNY TRITTEN TEUT THAT HAS HISTORIDANNY BSSN PSED TO RENAY ENDRYJTED FESSAGEM. FPSID TAS ANSO PSEA BY AKRIDAN AFERIDAN SNAQES TO DONQEY SEDRET DOFFPNIDATIONS. SNAQES XNST THE MEDRET FEANINGS OK THESE SONGS AND THEY DOPND SPBSELPENTNY BE PSED TO SIGNAN FANY THINGS, AND JERHAJS EQEN CENJED BRING THE SNAQES TO KREEDIF.

By examining ONNY it is logical to assume that “N” = “L”. Also, the frequency table shows that they have a similar frequency.

IT IS NOT ONLY TRITTEN TEUT THAT HAS HISTORIDALLY BSSN PSED TO RELAY ENDRYJTED FESSAGES. FPSID TAS ALSO PSEA BY AKRIDAN AFERIDAN SLAQES TO DONQEY SEDRET

DOFFPNIDATIONS. SLAQES XNST THE MEDRET FEANINGS OK THESE SONGS AND THEY DOPLD SPBSELPENTLY BE PSED TO SIGNAL FANY THINGS, AND JERHAJS EQEN CELJED BRING THE SLAQES TO KREEDIF.

There are three possibilities for EQEN; “eten”, “even” and “eyen”. As “Y” and “T” have already used “Q” = “V”.

IT IS NOT ONLY TRITTEN TEUT THAT HAS HISTORIDALLY BSSN PSED TO RELAY ENDRYJTED FESSAGES. FPSID TAS ALSO PSEA BY AKRIDAN AFERIDAN SLAVES TO DONVEY SEDRET DOFFPNIDATIONS. SLAVES XNST THE MEDRET FEANINGS OK THESE SONGS AND THEY DOPLD SPBSELPENTLY BE PSED TO SIGNAL FANY THINGS, AND JERHAJS EVEN CELJED BRING THE SLAVES TO KREEDIF.

By examining HISTORIDALLY it is obvious that “R” = “R” and “D” = “C” and becomes historically. Also “R” and “R” are close together in the frequency table and so are “D” and “C”.

IT IS NOT ONLY TRITTEN TEUT THAT HAS HISTORICALLY BSSN PSED TO RELAY ENCRYJTED FESSAGES. FPSID TAS ALSO PSEA BY AKRICAN AFERICAN SLAVES TO CONVEY SECRET COFFPNICATIONS. SLAVES XNET THE MECRET FEANINGS OK THESE SONGS AND THEY COPLD SPBSELPENTLY BE PSED TO SIGNAL FANY THINGS, AND JERHAJS EVEN CELJED BRING THE SLAVES TO KREEDOF.

By examining ENCRYJTED it is obvious that “J” = “P”. By examining AKRICAN AFERICAN it is obvious that “K” = “F” and “F” = “M”.

IT IS NOT ONLY TRITTEN TEUT THAT HAS HISTORICALLY BSSN PSED TO RELAY ENCRYPTED MESSAGES. MPSID TAS ALSO PSEA BY AFRICAN AMERICAN SLAVES TO CONVEY SECRET COMMPNICATIONS. SLAVES XNET THE SECRET MEANINGS OK THESE SONGS AND THEY COPLD SPBSELPENTLY BE PSED TO SIGNAL MANY THINGS, AND PERHAPS EVEN CELPED BRING THE SLAVES TO FREEDOM.

The remaining letters can now be determined by reading the plaintext. “T” = “W”, “U” = “X”, “B” = “B”, “P” = “U”, “G” = “G”, “X” = “K” and “L” = “Q”.

Therefore, the decrypted message is:
It is not only written text that has historically been used to relay encrypted messages. Music was also used by African American slaves to convey secret communications. Slaves knew the secret meanings of these songs and they could subsequently be used to signal many things, and perhaps even helped bring the slaves to freedom.

Check from Cryptogram Solver (http://rumkin.com/tools/cipher/cryptogram-solver.php)
Cryptogram Solver solution states:
IT IS NOT ONLY WRITTEN TEXT THAT HAS HISTORICALLY BEEN USED TO RELAY ENCRYPTED MESSAGES MUSIC WAS ALSO USED BY AFRICAN AMERICAN SLAVES TO CONVEY SECRET COMMUNICATIONS SLAVES KNEW THE SECRET MEANINGS OF THESE SONGS AND THEY COULD SUBSEQUENTLY BE USED TO SIGNAL MANY THINGS AND PERHAPS EVEN HELPED BRING THE SLAVES TO FREEDOM

Question 3: Encrypting Plaintext Using Matrices

The plaintext that is being encrypted is misdirection.

Plaintext 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	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0

∴ The plaintext's numerical equivalent is 13 9 19 4 9 18 5 3 20 9 15 4

Let P be the plaintext matrix

Let A be the enciphering matrix

$$A = \begin{bmatrix} 5 & 4 \\ 2 & 3 \end{bmatrix}$$

$$P = \begin{bmatrix} 13 & 9 \\ 19 & 4 \\ 9 & 18 \\ 5 & 3 \\ 20 & 9 \\ 15 & 4 \end{bmatrix}$$

$$PA = \begin{bmatrix} 13 & 9 \\ 19 & 4 \\ 9 & 18 \\ 5 & 3 \\ 20 & 9 \\ 15 & 4 \end{bmatrix} \times \begin{bmatrix} 5 & 4 \\ 2 & 3 \end{bmatrix}$$

$$PA = \begin{bmatrix} 13 \times 5 + 9 \times 2 & 13 \times 4 + 9 \times 3 \\ 19 \times 5 + 4 \times 2 & 19 \times 4 + 4 \times 3 \\ 9 \times 5 + 18 \times 2 & 9 \times 4 + 18 \times 3 \\ 5 \times 5 + 3 \times 2 & 5 \times 4 + 3 \times 3 \\ 20 \times 5 + 9 \times 2 & 20 \times 4 + 9 \times 3 \\ 15 \times 5 + 4 \times 2 & 15 \times 4 + 4 \times 3 \end{bmatrix}$$

$$PA = \begin{bmatrix} 83 & 79 \\ 103 & 88 \\ 81 & 90 \\ 31 & 29 \\ 118 & 107 \\ 83 & 72 \end{bmatrix} 1q$$

∴ The encrypted message in numbers is 83 79 103 88 81 90 31 29 118 107 83 72

Convert ciphertext matrix into alphabetic equivalent.

As there are numbers greater than 26 in the ciphertext mod27 must be found.

83	79	103	88	81	90	31	29	118	107	83	72
2	25	22	7	0	9	4	2	10	26	2	18

∴ The ciphertext converted to mod27 is 2 25 22 7 0 9 4 2 10 26 2 18

2	25	22	7	0	9	4	2	10	26	2	18
B	Y	V	G		I	D	B	J	Z	B	R

∴ The ciphertext alphabetically is BYVG – IDBJZBR where – is a space

Question 4: Decrypting Cipher text Using Matrices

The enciphering matrix is $\begin{bmatrix} 4 & 6 \\ 4 & 7 \end{bmatrix}$

$A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}(mod 27)$

$Det(A) = ad - bc$

$Det(A) = 4 \times 7 - 6 \times 4$

$Det(A) = 4$

Since $4 \times 7 = 28$

$= 1(mod 27)$

$\therefore (ad - bc) = 4^{-1}$

$= 7(mod 27)$

$\therefore A^{-1} = 7 \times \begin{bmatrix} 7 & -6 \\ -4 & 4 \end{bmatrix}$

$= \begin{bmatrix} 49 & -42 \\ -28 & 28 \end{bmatrix}$

$= \begin{bmatrix} 22 & 12 \\ 26 & 1 \end{bmatrix}(mod 27)$

Check:

$AA^{-1} = \begin{bmatrix} 4 & 6 \\ 4 & 7 \end{bmatrix} \times \begin{bmatrix} 22 & 12 \\ 26 & 1 \end{bmatrix}$

$= \begin{bmatrix} 244 & 54 \\ 270 & 55 \end{bmatrix}$

$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$= I\ (as\ required)$

The cipher text being deciphered is I BPKZCKQTKQAO.

Convert cipher text to numerical equivalent.

I		B	P	K	Z	C	K	Q	T	K	Q	A	O
9	0	2	16	11	26	3	11	17	20	11	17	1	15

$$\begin{bmatrix} 9 & 0 \\ 2 & 16 \\ 11 & 26 \\ 3 & 11 \\ 17 & 20 \\ 11 & 17 \\ 1 & 15 \end{bmatrix}$$

$$PA^{-1} = \begin{bmatrix} 9 & 0 \\ 2 & 16 \\ 11 & 26 \\ 3 & 11 \\ 17 & 20 \\ 11 & 17 \\ 1 & 15 \end{bmatrix} \times \begin{bmatrix} 22 & 12 \\ 26 & 1 \end{bmatrix}$$

$$PA^{-1} = \begin{bmatrix} 9 \times 22 + 0 \times 26 & 9 \times 12 + 0 \times 1 \\ 2 \times 22 + 16 \times 26 & 2 \times 12 + 16 \times 1 \\ 11 \times 22 + 26 \times 26 & 11 \times 12 + 26 \times 1 \\ 3 \times 22 + 11 \times 26 & 3 \times 12 + 11 \times 1 \\ 17 \times 22 + 20 \times 26 & 17 \times 12 + 20 \times 1 \\ 11 \times 22 + 17 \times 26 & 11 \times 12 + 17 \times 1 \\ 1 \times 22 + 15 \times 26 & 1 \times 12 + 15 \times 1 \end{bmatrix}$$

$$PA^{-1} = \begin{bmatrix} 198 & 108 \\ 460 & 40 \\ 918 & 158 \\ 352 & 47 \\ 894 & 224 \\ 684 & 149 \\ 412 & 27 \end{bmatrix}$$

As these numbers are greater than 26, mod27 must be found.

198	108	460	40	918	158	352	47	894	224	684	149	412	27
9	0	1	13	0	23	1	20	3	8	9	14	17	0

∴ The ciphertext converted to mod27 is 9 1 13 0 25 1 20 3 8 9 14 8

9	0	1	13	0	23	1	20	3	8	9	14	7	17
I		A	M		W	A	T	C	H	I	N	G	

∴ The plaintext is I AM WATCHING.

Question 5: Encrypting Plaintext Using a 3-Cipher

The plaintext being enciphered is The Eagle has landed.

Plaintext 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	-
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0

T	H	E		E	A	G	L	E		H	A	S		L	A	N	D	E	D
20	8	5	0	5	1	7	12	5	0	8	1	19	0	12	1	14	4	5	4

∴ The plaintext in its numerical equivalent is 20 8 5 0 5 1 7 12 5 0 8 1 19 0 12 1 14 4 5 4

Let P be the plaintext matrix

Let A be the enciphering matrix

$$P = \begin{bmatrix} 20 & 8 & 5 \\ 0 & 5 & 1 \\ 7 & 12 & 5 \\ 0 & 8 & 1 \\ 19 & 0 & 12 \\ 1 & 14 & 4 \\ 5 & 4 & 0 \end{bmatrix}$$

$$A = \begin{bmatrix} 6 & 5 & 2 \\ 5 & 5 & 2 \\ 2 & 2 & 1 \end{bmatrix}$$

$$PA = \begin{bmatrix} 20 & 8 & 5 \\ 0 & 5 & 1 \\ 7 & 12 & 5 \\ 0 & 8 & 1 \\ 19 & 0 & 12 \\ 1 & 14 & 4 \\ 5 & 4 & 0 \end{bmatrix} \times \begin{bmatrix} 6 & 5 & 2 \\ 5 & 5 & 2 \\ 2 & 2 & 1 \end{bmatrix}$$

$$PA = \begin{bmatrix} 20\times6+8\times5+5\times2 & 20\times5+8\times5+5\times2 & 20\times2+8\times2+5\times1 \\ 0\times6+5\times5+1\times2 & 0\times5+5\times5+1\times2 & 0\times2+5\times2+1\times1 \\ 7\times6+12\times5+5\times2 & 7\times5+12\times5+5\times2 & 7\times2+12\times2+5\times1 \\ 0\times6+8\times5+1\times2 & 0\times5+8\times5+1\times2 & 0\times2+8\times2+1\times1 \\ 19\times6+0\times5+12\times2 & 19\times5+0\times5+12\times2 & 19\times2+0\times2+12\times1 \\ 1\times6+14\times5+4\times2 & 1\times5+14\times5+4\times2 & 1\times2+14\times2+4\times1 \\ 5\times6+4\times5+0\times2 & 5\times5+4\times5+0\times2 & 5\times2+4\times2+0\times1 \end{bmatrix}$$

$$PA = \begin{bmatrix} 170 & 150 & 61 \\ 27 & 27 & 11 \\ 112 & 105 & 43 \\ 42 & 42 & 17 \\ 138 & 119 & 50 \\ 84 & 83 & 34 \\ 50 & 45 & 18 \end{bmatrix}$$

∴ The ciphertext numerically is 170 150 61 27 27 11 112 105 43 42 42 17 138 119 50 84 83 34 50 45 18

Convert ciphertext matrix into alphabetic equivalent.

As the ciphertext contains numbers greater than 26, mod27 must be used.

170	150	61	27	27	11	112	105	43	42	42	17	138	119	50	84	83	34	50	45	18
8	15	7	0	0	11	4	24	16	15	15	17	3	9	23	3	2	7	23	18	18

∴ The ciphertext converted to mod27 is 8 15 7 0 0 11 4 24 16 15 15 17 3 9 23 3 2 7 23 18 18

8	15	7	0	0	11	4	24	16	15	15	17	3	9	23	3	2	7	23	18	18
H	O	G			K	D	X	P	O	O	Q	C	I	W	C	B	G	W	R	R

∴ The ciphertext alphabetically is HOG − −KDXPOOQCIWCBGWRR where − is a space

The advantage of using a 3 x 3 cipher as opposed to a 2 x 2 cipher is that it is much harder for a third party to decrypt the message without the enciphering matrix because there are more combinations possible. However, as this is a polyalphabetic cipher there is little to no chance that it would be possible for a third party to discover the enciphering matrix even if it is 2 x 2 matrix. Furthermore, it is quicker to decode a 2 x 2 matrix than 3 x 3 matrix so if the situation that requires encrypted messages is time sensitive it is better to use a 2 x 2 matrix. It is possible to make it more secure by increasing the order of the matrix because again there are more possible combinations but as the cipher is polyalphabetic it isn't needed.