Joseph Pennington (2912079)

EECS 565 Homework 1

Exercise 1: Decrypt the following encrypted quotation.

fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc

Letter Distribution

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
2	5	3	1	0	3	0	2	0	7	1	0	1	7	0	0	2	1	0	0	3	3	4	3	0	0

Based on this distribution of letters, my initial thought was that this is a substitution or shift cipher. The most frequent letter in English is “e” so either substituting “j” or “n” with “e” would be a good place to start.

Shift Key (Swap “j” with “e”)

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
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

Deciphered Text: ALEXW MRERE QIEVS WIFCO RCSXL IVREQ IASYP HWQIP PEWWA IIX

This decryption does not make sense.

Shift Key (Swap “n” with “e”)

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	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

Deciphered Text: WHATS INANA MEARO SEBYA NYOTH ERNAM EWOUL DSMEL LASSW EET

Final Answer: WHATS IN A NAME A ROSE BY ANY OTHER NAME WOULD SMELL AS SWEET

Exercise 2: Decrypt the following encrypted quotation.
oczmz vmzor jocdi bnojv dhvod igdaz admno ojbzo rcvot jprvi oviyv aozmo cvooj ziejt dojig toczr dnzno jahvi fdiyv xcdzq zoczn zxjiy

Letter Distribution

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
4	2	7	9	1	1	2	2	9	9	0	0	4	5	18	1	1	4	0	3	0	10	0	2	3	13

Using a shift cipher, I will first try swapping “o” with “e” because “o” was the most frequent letter and “e” is the most common letter in English

Shift Key (Swap “o” with “e”)

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
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P

By simply comparing the letter distribution to this key, one can see that that this key is more than likely incorrect. This is the case because this key shows that after the substitution, “p” would be the second most common letter. In general, “p” is a relatively uncommon letter in English. Instead, I will substitute “z” for “e” because “z” was the second most frequent letter.

Shift Key (Swap “z” with “e”)

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
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

This substitution seems more likely to be correct because the two most frequent substituted letters are “t” and “e” which are the two most common letters in English.

Deciphered Text: THERE ARETW OTHIN GSTOA IMATI NLIFE FIRST TOGET WHATY OUWAN TANDA FTERT HATTO ENJOY ITONL YTHEW ISEST OFMAN KINDA CHIEV ETHES ECOND

Final Answer: THERE ARE TWO THINGS TO AIM AT IN LIFE FIRST TO GET WHAT YOU WANT AND AFTER THAT TO ENJOY IT ONLY THE WISEST OF MANKIND ACHIEVE THE SECOND

Exercise 3: Decrypt the following encrypted quotation.
pbegu uymiq icuuf guuyi qguuy qcuiv fiqgu uyqcu qbeme vp

Letter Distribution

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
0	2	3	0	3	2	4	0	5	0	0	0	2	0	0	2	6	0	0	0	12	2	0	0	4	0

Using a shift cipher, I will substitute “u” for “e” because that is the most frequent letter and “e” is the most common letter in English.

Shift Key (Swap “u” with “e”)

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
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Deciphered Text: ZLOQE EIWSA…
The first two letter block are not correct.

My next guess would be to substitute “q” for “e”. However, this would substitute “u” with “i”. Looking at the encrypted text, this would not be correct because “u” almost exclusively appears as a double. In English, “ii” is an extremely uncommon double.

Switching Strategies
When looking at the text, one can see that a frequent substring of letters is “guuy” and that “uu” is repeated frequently as well. This means that “uu” may be either “ee”, “oo”, or “tt”. However, I have already tried substituting “u” for “e”, and “u” probably does not correspond to “t” either because a four-letter word would more than likely not contain “tt” in the case for “guuy”. So, I will substitute “u” with “o” and separate the substring “guuy” from the original text.

Deciphered Text: pbe gOOy miq icOOf gOOy iq gOOy qcOiv fiq gOOy qcO qbeme vp

After separating “gOOy”, the first substring consists of three letters. My initial guess is that “pbe” corresponds to the word “the” because “the” is an extremely common three-letter word and frequently is used to start sentences. So, I will substitute “p” for “t”, “b” for “h”, and “e” for “e”

Deciphered Text: THE gOOy miq icOOf gOOy iq gOOy qcOiv fiq gOOy qcO qHEmE vT

Next, I decided to fill out the substitution key to see if there was a pattern from the few letters I had substituted so far.

Substitution Key

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
	H			E											T					O					

I did not draw any conclusions from this.

Next, I noticed that “iq” is frequently repeated. Common two-letter words are “is”, “it”, “on”, “as”, “so”, and “to”, just to list a few. I then separated “iq” from the string.

Deciphered Text: THE gOOy m iq icOOf gOOy iq gOOy qcOiv f iq gOOy qcO qHEmE vT

Focusing on “q”, “q” would most likely be “s” or “n” when looking at the examples of two-letter words. “q” would not be “t” or “o” because I have already found substitutions for those. Additionally, “iq” could not be “on” because

“o” has already been substituted. This leaves “iq” as possibly being “is” or “as”. I will substitute “q” for “s” because that is more certain.

Deciphered Text: THE gOOy m iS icOOf gOOy iS gOOy ScOiv f iS gOOy qcO SHEmE vT

One word that stands out is “SHE”.

Deciphered Text: THE gOOy m iS icOOf gOOy iS gOOy ScOiv f iS gOOy qcO SHE mE vT

This means that my guess of substituting “q” for “s” was most likely correct.

Updated Substitution Key

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
	H			E											T	S				O					

After updating the key, one interesting observation is the “T” and “S” are next to each other and in the opposite order of the English alphabet. From this observation, I drew the conclusion that the substitution or shift was reversed. I then filled in the remaining letters and attempted to decipher the text.

Updated Substitution Key

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
I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J

Deciphered Text: THE COOK W AS AGOOD COOK AS COOK SGOAN D AS COOK SGO SHE WE NT

Final Answer: THE COOK WAS A GOOD COOK AS COOKS GO AND AS COOKS GO SHE WENT

Exercise 4: Decrypt the following encrypted quotation.
jrgdg idxgq anngz gtgtt sitgj ranmn oeddi omnwj rajvk sexjm dxkmn wjrgm ttgdt gognj ajmzg ovgki nlaqg tjamn xmsmj jrgko jtgnw jrgnj rgvat tmgta wamno jjrgw izgtn sgnji babgu

Letter Distribution

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
10	2	0	6	2	0	23	0	6	17	4	1	11	14	6	0	2	8	4	13	1	3	5	4	0	3

Using a shift cipher, I will substitute “g” with “e” because “g” is the most frequent letter and “e” is the most common letter in English.

Shift Key (Swap “g” with “e”)

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
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	E	S	T	U	V	W	X

Deciphered Text: HPEBE…
From the first substring, it is clear this is not correct

Next, I will substitute “j” with “e”.

Shift Key (Swap “j” with “e”)

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
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

Deciphered Text: EMBYB DYSBL…
This does not make sense.

I will then substitute “n” with “e”.

Shift Key (Swap “n” with “e”)

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	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

Deciphered Text: AIXUX…

This does not make sense.

Switching Strategies
This text appears to not be a simple shift, but a more complex substitution. Looking at the letter distribution, “g” and “j” are the most common letters. I will substitute “g” for “e” and “j” for “t” because these are also the most common letters in English. Additionally, the trigram “jrg” appears very frequently and is used to start the sentence. This would most likely be the word “the”. This would cause “r” to be “h” because I have already substituted “j” and “g”.

Substitution Key

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
						E			T								H								

Deciphered Text: THE dE idxEq annEz EtEtt sitET Hanmn oeddi omnwT HaTvk sexTm dxkmn w THE m ttEdt EoEnT aTmzE ovEki nlaqE tTamn xmsmT THE ko TtEnw THE nT HEvat tmEta wamno T THE w izEtn sEnTi babEu

From the original text, the letters “gt” and “tg” appear frequently together. This could be a common digram such as “er”, “es”, or “en” because “g” has already been substituted for “e”. Because the digram appears in either order, it would make the most sense for “t” to represent “r”.

Updated Substitution Key

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
						E			T								H		R						

Deciphered Text: THE dE idxEq annEz ERERR siRET Hanmn oeddi omnwT HaTvk sexTm dxkmn w THE m RREdR EoEnT aTmzE ovEki nlaqE RTamn xmsmT THE ko TREnw THE nT HEvat RmEta wamno T THE w izEtn sEnTi babEu

From this point, I did not know what a logical next step would be. I could not see any common digrams or trigrams, and I did not want to start randomly guessing letters.

Final Answer: THE dE idxEq annEz ERERR siRET Hanmn oeddi omnwT HaTvk sexTm dxkmn w THE m RREdR EoEnT aTmzE ovEki nlaqE RTamn xmsmT THE ko TREnw THE nT HEvat RmEta wamno T THE w izEtn sEnTi babEu

Exercise 5: Decrypt the following encrypted quotation.
ejitp spawa qleji taiul rtwll rflrl laoat wsqqj atgac kthls iraoa twlpl qjatw jufrh lhuts qataq itats aittk stqfj cae

Letter Distribution

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
15	0	2	0	3	3	1	3	6	6	2	11	0	0	2	3	7	5	6	15	3	0	5	0	0	0

Based on the distribution, “a” and “t” are the most common. It would be probable that “t” represents itself because “t” is the second most common letter and “a” could represent “e”. Also, “l” could be mapped to “a” because “a” is the third most common letter.

Substitution Key

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
E											A								T						

Deciphered Text: ejiTp spEwE qAeji TEiuA rTwAA rfArA AEoET wsqqj ETgEc kthAs irEoE TwApA qjETw jufrh Ahuts qETEq iTETs EiTTk sTqfj cEe

After this step, I could not figure out what a logical next step would be. This appears to be more complicated than a shift cipher and the digrams and trigrams confused me.

Final Answer: ejiTp spEwE qAeji TEiuA rTwAA rfArA AEoET wsqqj ETgEc kthAs irEoE TwApA qjETw jufrh Ahuts qETEq iTETs EiTTk sTqfj cEe