Cryptography Assign. 1A

Key- The key *k* for my cipher is a single number from 1-26 which is shared between the sender and the reciever.

How to Encipher- Each letter is assigned a number beginning from *k* and spanning from 1-26 using "wraparound". Each assigned number is then written in the message in binary.

How to decipher- Convert each set of binary values into decimal valuves (base 10 numbers). Once converted, use *k* in order to determine which number corresponds to A, B, C... etc.

Example:

Key: 1

Plain Text- Have Fun

Cipher Text- 1000 01 10110 101 110 10101 1110

In this case, letters are assigned numbers starting from 1, and those assigned numbers are written in binary.

Cipher: Z O X Q V S T U R W P Y N M B K D I F G H E J C L A
Plaintext: 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: The first 13 and second 13 letters of the alphabet are switched so that N is first, Z is 13th, A is 14th, and M is last. Then in two separate groups (1st 13 and 2nd 13) there are more steps. The first and last letters in each group switch, the 3rd and 11th switch, the 5th and 9th also switch, while the middle (7th) letter stays the same (it is the axis). This change occurs separately for both sets of letters.

Example: Hello my name is Kevin.

Uvyyb nl mz pverm

The Key: For my cipher, the secret key shared by the sender and the receiver consists of a six-digit number, such as an important date known between the sender and receiver.

How to Encipher: Once the plaintext is written, you write the six-digit number continuously underneath it, so each letter (x) is assigned to a number (y). Then, you replace letter x with the letter that is y places down the alphabet. For example, if the letter is m and the number beneath it is 3, you would replace the letter m with the number that is three places down from it in the alphabet, which in this case would be p.

How to Decipher: When given the cipher text, the first thing that needs to be done to decipher it is to write the six-digit number continuously underneath it, just as was done with the plaintext. Then, you replace each letter x with the letter that is y places ahead of it in the alphabet, which is exactly the opposite that you would do while enciphering it. So, for example, if you had the letter q, and the number is 6, you would replace q with the number 6 places above it in the alphabet, which in this case is k.

Example:
Encryption:
Key: 112492
Plaintext: this is my example
1124 92 11 2492112
Ciphertext: uikw ru nz gwjoqmg

Decryption:
Key: 041408
Ciphertext: nkv e walh cacqpp
041 4 0804 140804
Plaintext: now i will decypt

The Key: The key consists of a word known by the sender and receiver as well as a phrase that describes the order of the numbers in the top row and left column.

How to encipher: In order to encipher the message, the sender creates a table with 11 columns and 4 rows, and spells the secret word across starting at B2, followed by the alphabet, skipping spaces in the second row for the numbers that exist in the first column. To encipher a given letter, find it in the table and see what its corresponding number is—for example, "I" would be "52," "B" would be "4."

How to decipher- To decipher, match the number with its corresponding letter.

An example:

	0	1	2	3	4	5	6	7	8	9
	K	E	Y	A	B		C		D	F
5	G	H	I	J	L	M	N	O	P	Q
7	R	S	T	U	B	W	X	Z		

The key provided in the table above is "KEY." The numbers that repeat in the left column are 5 and 7 and the order across the top row is simply 0-9 in this case.

Encryption:

Plaintext: *This is a short example*
Ciphertext: *725152715271371515770721763555854 1*

Decryption:

Ciphertext: *7251527152713715452505172542545756501701763555854 1*
Plaintext: This is a slightly longer example

Comp 133

Assignment 1

The Book Cipher

The Key: For my cipher the secret key that is shared by the sender and receiver is a passage from *The Code Book* by Simon Singh.

How to Encipher: Given the key, label and associate each letter of the key's sentence with a number based on position. For example, if the word "code" was the key phrase, then c =1, o = 2, d = 3, e = 4. Convert the entire key from letters to numbers. Now that the key is created, replace each letter of the plaintext with a number from the key that represents that letter, thus creating the cipher text.

How to Decipher: Given the key, first label and associate each letter of the key's sentence with a number based on position. For example, in the word "code", c =1, o = 2, d = 3, e = 4. Convert the entire key from letters to numbers. Once the key is set up, replace each number of the cipher text with a letter of the plaintext.

Note: In the cipher text, punctuation and spacing that would occur between words of the plaintext is not accounted for.

Example:

Encryption:

Key: "Wesleyan is good"
Plaintext: Go Wes
Cipher text: 11, 12, 1, 2, 3

Decryption:

Key: "Wesleyan is good"
Cipher text: 1, 2, 3, 2, 4, 4, 4, 7, 8, 14
Plaintext: We sell land

(SPACE) = 27 + 2n
a = 41 + 2n
b = 124 + 2n
c = 28 + 2n
d = 34 + 2n
e = 44 + 2n
f = 132 + 2n
g = 128 + 2n
h = 50 + 2n
i = 64 + 2n
j = 31 + 2n
k = 97 + 2n
l = 88 + 2n
m = 56 + 2n
n = 75 + 2n
o = 103 + 2n
p = 832 + 2n
q = 509 + 2n
r = 93 + 2n
s = 189 + 2n
t = 177 + 2n
u = 5 + 2n
v = 945673 + 2n
w = 99 + 2n
x = 49 + 2n
y = 20 + 2n
z = 44665 + 2n

Use the key above to translate each letter into its equivalent numerical value where "n" is what number the word is in the sentence repeating at 25 (assuming the first word is "1", the second word is "2", etc., and each space is part of the word directly before it. Remember after "25" you go back to "1").

TO CODE:

Note the number of the word you are on, and substitute that value in for "n". Multiply it by two, and add it to the assigned number value for the letter you are coding. This new number is the coded version of that letter. Continue this process until you have your whole message written in code. Don't forget to code your spaces.

TO DECODE:

Get your key and your message side by side. Note the number of the word you are on, and multiply it by two. Keep that in your mind as you check the key for a number that much less than the one on the paper. This can get a little bit confusing since the numbers have different amounts of digits, however since most of the values are three digits or less, it is pretty easy to find the corresponding letter quickly (keep in mind that the numbers with more than three digits will generally look pretty similar to the original number.)

Explanation of encryption and decryption technique:

The key:
For my cipher a key exists between the sender and receiver of the message. Within this key, random letters, symbols, and/or numbers stand for the letters of the original alphabet.

Encryption:
These random characters shown in the original key will be used to replace the letters of plain text that is being encrypted.
However, an additional level of complication is placed upon this key; a Caesar shift is used, although it does not take affect immediately. In this Caesar shift, the characters of the cipher text alphabet will change position by moving *x (a value determined by the key)* places later in the alphabet—once the end of the alphabet is reached, the remaining characters of the cipher text replace those of the beginning of the plain text.
This shift in the key takes place only after a certain number of characters, *y (a value determined by the key),* have been encrypted based off of the original key. Once this amount of characters, *y,* has been encrypted into the cipher text, the original key will undergo the shift, with a value of *x*, to form a new key for encryption. The resulting new key is then used to encrypt the same number of characters, *y*, as the original key but on the plain text letters that follow those already encrypted. Upon completion of this same number of characters, *y,* a shift of the same value as the original shift, *x,* takes place upon the key once again. This time, however, the shift occurs upon the latest key of use and not the original. This pattern is repeated until the message is fully encrypted, thus producing a key that constantly changes and evolves by continuously shifting by the same amount, *x,* each time that a certain number of letters, symbols, and/or numbers, *y,* has been encrypted.
Due to the constant evolution of the cipher, the number of characters encrypted must be heavily monitored; the inclusion of even one extra letter, symbol, and/or number prior to shifting the key will result in an incorrect reading of the entire text.

Decryption:
The cipher text is decrypted through the use of the key as well. However more careful attention must be paid to when the key shifts because the shift that occurs is based off of the order of the plain text and not that of the cipher text. Therefore, one must refer to the key used for encryption to see how the cipher text letters shift each time since there is not a simple shift upon the decryption key.

Example:

Encryption

Original key:

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

There is a shift of the value -2 every 8 characters
This means that x=-2 and y=8

The Resulting keys are as follows:
@ 9th letter:
Plain Text: 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
Cipher text: k q h y u s t b v c x a w z d g e f m o l i n p r j
@ 17th letter:
Plain Text: 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
Cipher Text: r j k q h y u s t b v c x a w z d g e f m o l i n p
@25th letter:
Plain Text: 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
Cipher Text: n p r j k q h y u s t b v c x a w z d g e f m o l i

Plain Text: This is an. example o.f my ciphe.r
Cipher Text: icxl xd hd. upkadxu z.y xn ktzsh.z

*In the examples above and below, a period may be found every 8 characters. This symbolizes that a new shift must take place in the key in order to continue encrypting or decrypting.

Decryption

Original Key:

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

@ 9th letter:

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

Cipher Text: icxl xl ot.kaar slz
Plain Text: This is re.ally fun

Part A – Encoding and Decoding instructions.

Encoding: To encode a message, one must replace each letter/number with the letter/number immediately to the left of it on a standard, American QWERTY keyboard. For the end numbers/letters (1, q, a and z), one should 'wrap around' per say, and replace it with the letter furthest to the right in that same row, (i.e 1 becomes 0, Q becomes P, A becomes L, and Z becomes M).

For example, the sentence: "I like puppies," would become, "U kujw oyoouwa."

Decoding: To decode a message, one must replace each letter/number with the letter/number immediately to the right of it on a standard, American QWERTY keyboard. For the edge numbers/letters (0, p, l and m), one should 'wrap around' and replace it with the leftmost letter in the same row (i.e. 0 becomes 1, P becomes Q, L becomes A and M becomes Z).

For example, the sentence: "U glrw xlra," would be decoded to be "I hate cats."

COMP 133
Assignment 1: Create your own Cipher
Part A

The Key: The key sent between the sender and the receiver to encrypt and decrypt my message consists of three parts. The fist part will be any rational number from 1 to 10. The second part will be the thirteen matching pairs of a substitution cipher. The third part will be a two.

How to encipher: Using the given key, a sender enciphers a message in three parts. First, the sender takes the plaintext message and uses the first number given in the key to perform the transposition. The number indicates how many lines are used for the Rail Fence transposition. To do this, one must write the plaintext out vertically (using the first number in the key to determine how many vertical lines there are) instead of horizontally. Each letter of the message is one line, using x lines total. When all x lines are used, the message continues this pattern starting from the top again, moving left to right. Once the whole message is written out. Each sequential lower line is then tagged on at the end of the line right above it to make one long single line message. For example, if the key was four, then the word Wesleyan changes to

We
ey → we + ey+ sa+ ln = weeysaln
sa
ln

The next part of the encryption is to the take the completed Rail Fence transposition and change it using the Substitution cipher. The key will give thirteen pairs of letters, and the sender must swap out each letter of the Rail Fence message with its respective pair. If i is paired with q and t is paired with w, then the word *it* is now qw. The last step of the cipher is to take the message that has been changed by the rail fence and the substitution cipher and switch every two letters that are next to each other. The last part of the key represents this switch as a two. Using this, the word hide would be ihed. The h and i switch places as well as the d and e.

How to decipher: Given the three part key, the receiver deciphers the message by working backwards. First the receiver takes the cipher text and switches every two letters so that they are back into place. Ihed changes back to hide. Once the letters are in the right order again, the receiver used the thirteen pairs of letters the key gives to substitute the original letters back. q is paired with i and w is paired with t, so qw is switched back to *it*. Lastly the receiver uses the first number of the key to determine how many lines are in the Rail Fence transposition. Divide the letters in the remaining message by this number k to get k rows of letters. Place each row underneath the one before it and read the message vertically from left to right to determine the plaintext. Part A of the key gives the number 4. Wesleyan is 8 letters,

so 8 divided by 4 is two. This information turns weeysaln into we, ey,sa,and ln. Arranged into four lines, the four pairs turn into we

ey
sa
ln

If this is read vertically from left to right, the message says Wesleyan.

Example:

Encryption:

Key: Part 1- 2
Part 2- a j f d s g k l w e o i p
q r t y u h z x c v b n m
Part 3- 2

Plaintext: spies use ciphers
Part 1- s i s s c p e s → sisscpespeueihr
p e u e i h r
Part 2- unuuwmvumvsvngj
Part 3- nuuumwuvvmvsgnj
Ciphertext: nuuum wuv vmvsgnj

Decryption:

Key (invert the steps):
Part 1- 3
Part 2- a d g j l q e t u o z c b
w r y i p s f h k x v n m
Part 3-2
Ciphertext: nhq kln txqj dfchwfcfjgq
Part 3: hnkqnlxtjqfdhcfwfcgjq
Part 2: tcuscpohisertneaenyis
Part 1: t c u s c p o
h i s e r t n
e a e n y i s

Plaintext: The cia uses encryptions

Comp 133

Assignment 1

Cipher

The Key: For my cipher the secret key shared by the sender and receiver consists of a pattern with a single number between 1 and 10

How to Encipher: In order to encipher a message, the sender should first number the letters of the alphabet (a=1, b=2, c=3, etc.). The pattern alternates between odd and even letters. Examples of odd letters are a, c, e, g, etc, while even letters would be b, d, f, h, etc. The pattern works by being given a key, *k;* the sender then takes a letter of plaintext and replaces it by the letter that is either *k* positions before or after in the alphabet (depending on whether the plaintext is an even or odd letter). The letter is replaced by *k* positions after the plaintext if it is odd, while it is replaced *k* positions before the plaintext if it is even. This is done with "wraparound" meaning that if you get to the end of the alphabet when counting up or down to k positions you continue counting from the beginning. For example, if the key is 2, then plaintext letter A gets replaced with C, B replaced with Z, C gets replaced with E, D gets replaced with B.

How to Decipher: In order to decipher a message, the reader should first number the letters of the alphabet (a=1, b=2, c=3, etc.) and figure out which letters are odd or even (see above). Given a key, *k,* in order to decipher, the receiver should take each letter of the cipher-text and replace it by the letter that is either *k* positions earlier or after in the alphabet. Important note: the decryption pattern changes based on whether *k* is an even or odd number! If the number key, *k,* is an <u>even</u> number (k=2, 4, etc.), then the odd cipher-text letters are replaced by the letter *k* positions earlier (e -> c, if k=2), if the cipher text is an even number, it is replaced by the letter *k* positions after (d -> f if k=2). If the number key, *k,* is an <u>odd</u> number (k=1, 3, 5, etc.), then the odd cipher-text letters are replaced by the letter *k* positions later (c -> f, k=3), if the cipher text is an even number, it is replaced by the letter *k* positions earlier (b ->y, if k=3).

A Small Example:

Encryption:

Key: 2
Plaintext: cryptography is fun
Cipher-text: epanrqipcnfa ku dpl

Notice that c gets replaced by e since c is an odd letter and e is two letters later in the alphabet, g by l, etc. Also, notice that f, an even letter, gets replaced by d since it is two letters before in the alphabet, n by l, etc.

Decryption:
Key: 3
Cipher-text: pb cdsrolqh fidvv lv fobmqrjodmeb
Plaintext: my favorite class is cryptography

Notice that c, an odd number, goes to f (3 letters later), while b, an even number, goes to y (letters before)

Example: key=2

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

PT= plain text
CT= cipher text

Example: key= 3

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

The way this particular coding works is from the outside in of the alphabet. So the first letter is the first letter from the end and the eighth letter is the eighth letter from the end etc. This applies to all words three letters and longer. The words that are one and two letter words are attached to the preceeding three or more letter word. The two letter words do not follow the other coding. The coding for one and two letter words are the letters that proceed after the original. For example, the phrase: “Never Gonna Give You Up” is as follows: mvei tlmmz trev blfvq. The word “up” is added on the end of you and then changed with the next letters in the regular alphabet.

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

The coding process is a modified Caesar Shift Cipher, which treats vowels and consonants differently. Consonants can be "shifted" up to 20 times, and vowels can be "shifted" up to 4 times. When a plaintext letter is shifted, its ciphertext correspondent is the letter that number of shifts down the alphabet. For instance, a B shifted 5 times is an H (skipping vowels). Vowels are shifted the opposite direction; E shifted 3 times is an O. When the shifted alphabet (both for consonants and vowels) reaches its end, it "wraps around" to the beginning. Thus, in a Shift 4, V corresponds to Z, then W to B (skipping A), X to C, Y to D, and Z to F (skipping E). If vowels are shifted by 2, I corresponds to A, then E to U, and A to O. The key consists of two numbers: the first corresponds to the consonant shifts, and second to the vowel shifts. For a full example, "Hello, my name is Trevor," Key= 3,2, becomes "Luppe, qc roqu aw Xvuyev."

COMP 133
Assignment 1

Shifting Key Vigenère Cipher

The Key: The decryption key for my cipher consists of a set of five numbers, each between 1 and 9. Numbers may be used more than once.

How to Encipher: Given a key *a,b,c,d,e,* the sender creates alphabetical shifts based on each number. For example, if "*a"* is 1, the sender shifts the ciphertext alphabet over by 1, so the ciphertext alphabet begins with B, goes to Z, and wraps around to A. Now, the ciphertext letter B corresponds to the plaintext letter A. Next, the sender would create shifted alphabets for the remaining 4 numbers. The numbers in the key along with their corresponding alphabets are used in sequential order to encipher the letters of the plaintext, e.g. "*a"* enciphers the first letter, *"b"* the second, and so on. After the key is used once, or in other words, after the first five letters have been enciphered, the key shifts. The key shift is based on the number that *"a"* represents. For example, if the sequence of numbers is 6,7,3,8,9, the key for the second set of five letters will be shifted over 6 and will become 3,8,9,6,7. The key for the second set of five letters is enciphered based on the shift that each number represents. Now, letter six in the plaintext will be enciphered using the alphabetic shift for 3, and letter seven will be enciphered with the shift for 8. The process of the key shift is repeated after every five letters.

How to Decipher: Given a key *a,b,c,d,e,* the receiver creates alphabetical shifts based on each number (see *How to Encipher* for details). Next, the receiver deciphers the first five letters based on the corresponding number in the key. For example, if the key is 4,5,6,7,8, the first ciphertext letter must be located in the ciphertext shifted alphabet for 4, and then it must be referenced with the plaintext alphabet to determine the plaintext letter. After the first five letters are deciphered, the receiver must shift the key based on the number of *"a"* (see *How to Encipher* for details). The next five letters will be decrypted based on the new key. The key shifting process repeats every five letters until completion.

Example:

Encryption:

Key: 6,7,8,9,1

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

Plaintext: **hello world**

Ciphertext: **NLTUP DWAMJ** *(shifted key for letters 6-10 is "7,8,9,1,6")*

Comp 113

Assignment 1

Adrian's Shift Cipher:

Key 1: For my cipher, the key is a number between 1-15.

How to Encipher: assume that every letter in the alphabet has a number associated with it that corresponds to its place in the alphabet. For example, A=1, B=2, ect. Once the key is given, take the number of each letter in the alphabet (as described above) and add 2 from that number.

How to decipher: Once the key is known ("k") then take the number line and subtract two to every number then translate this back into the normal alphabet numbering system.

Example:

Encryption:

Key 1

Plain text: Get ready to party!

Encrypted: 8 6 21 19 6 2 5 26 21 16 172 19 21 26 !

Notice how G which is the 7 letter in the alphabet is now 8!

COMP 133
Assignment 1

A Polyalphabetic Substitution Cipher

The Key: For my cipher, there are two secret keywords shared by the sender and receiver. Each key is a real word in English or Greek, and can be formed using the respective letters of the English or Greek alphabet.

How to Encipher: In my cipher, each character of the plaintext alphabet is replaceable by a character of one of the two scrambled cipher alphabets. The orders of the cipher alphabets are established by two keywords, k_E and k_Γ. The first cipher alphabet is composed of English characters. Its first characters are an English word, k_E, and its remaining characters are placed in their regular order in the English alphabet. For example, assuming that k_E is "cipher," the English cipher alphabet would be arranged

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

To encrypt a plaintext message using the first cipher alphabet, a sender replaces the characters of the plaintext alphabet with the characters of the new cipher alphabet. For example, a sender using the keyword "cipher" could replace the plaintext A with C, B with I, etc.

The second cipher alphabet is composed of Greek characters. It is organized in nearly the same way as the first: a Greek codeword forms the opening characters, and then the alphabet continues as it would traditionally until it ends. For example, assuming that k_Γ is ποσειδωνας, the Greek cipher alphabet would be arranged

π ο σ ε ι δ ω ν α β γ ζ η θ χ λ μ ξ ϱ ς τ υ ϕ.

To encrypt a plaintext message using the second cipher alphabet, a sender replaces the characters of the plaintext alphabet with characters of the new cipher alphabet. For example, a sender using the keyword ποσειδωνας could replace A with π, b with ο, etc. Since the

Greek alphabet only has twenty-four characters, a sender will not be able to encipher an entire message if he relies exclusively on the second cipher alphabet. Since capital Greek letters are too similar to English letters, all Greek letters are lowercase.

While each of these ciphers is functional on their own, they are designed to be used together. Using the full polyalphabetic cipher, a sender has the option to replace most every plaintext character with two enciphered characters. For example, based on the two demonstrations above, a sender could replace A with either C or π.

How to Decipher: Given two keys, k_E and k_Γ, the receiver deciphers by taking each letter of the cipher text and replacing it with its corresponding plaintext character.

A Small Example:

Keys: leaf and πιτα.

Plaintext: Hello, Earth.

Ciphertext: ε β ζ ζ ν, b l r t ε.

COMP 133
Assignment #1

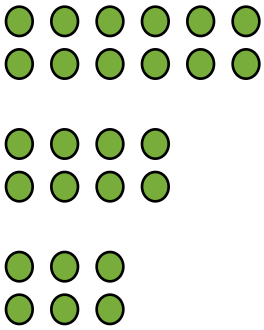
Part A

Variable Shift - Substitution Cipher

Description:
The goal of this cipher is to take the concept of the simple shift cipher and expand it by varying the shift between plaintext and ciphertext. In other words, in this model, there is no constant k that can be added to the position value of a plaintext character in order to yield the position value of the cyphertext character; rather, k will be defined as a variable quantity. In this example, the letters will be organized as exclusive pairs.

Example:
The simplest way to develop a system of variable shift is through visual organization. The method used for developing my cypher was:

1) Since each letter will have a unique pair, rather than think of them as 26 individual characters, let us think of them as 13 units, one unit being a pair of characters.
2) Arrange the 13 pairs of characters as a group of 6 pairs, 4 pairs, and 3 pairs:



3)Assign sequential alphabetic value to each individual character:

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) We have now grouped our alphabetical pairs in a way which utilizes a simple variable shift.

Algebraic Explanation:

let n = positional value of plaintext letter (i.e. a = 1, z = 26 etc.)

To obtain the positional value of the ciphertext letter:
Key:
$f(x) = n + 6,\ 1 \leq n \leq 6$
$n - 6,\ 7 \leq n \leq 12$
$n + 4,\ 12 \leq n \leq 16$
$n - 4,\ 17 \leq n \leq 20$
$n + 3,\ 21 \leq n \leq 23$
$n - 3,\ 24 \leq n \leq 26$

In order to decipher, the inverse of the pertinent piece of the function shall be taken.

Use:
plaintext: “cryptography is fun”
ciphertext: “invtpsangtbv co lxr”

COMP 133

Assignment 1 **/The Seed Cipher/**

The key: For my cipher the secret key shared by the sender and receiver consists of single number between 1 and 26.

How to Encipher the first stage: It is consistent stage. In other words in this stage there is no key. Moreover every letter of plaintext is converted into other characters. It is converted by system of keyboard. For example: the first letter A is converted to the first character of second row of keyboard `, second letter B becomes second character of second row of keyboard ~, C becomes 1, D becomes !, E becomes 2 …. X becomes _, Y becomes =, Z becomes +.

How to Encipher second stage: Given a key k, in order to encipher a message the sender takes each letter of the first stage encipher text and moves it to the first position. Then the letter in front of moved letter replaces the letter which was moved to the first place. For example, if the key is 3, then the first stage enciphered letter 1 replaces ` and ~ moves to ! . But first stage enciphered letters behind 2 shouldn't move.

How to decipher: Given a key k, in order to decipher the receiver takes the first letter of the ciphertext and replaces it by the letter that is k positions later in the alphabet. And letters in front of k position move backward by one place. After that, every character should converted into plaintext letter.

A small example:

Encryption/first stage/:

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 (0) - _ = +

Encryption /second stage/:

` ~ 1 ! 2 @ 3 # 4 $ 5 % 6 ^ 7 & 8 * 9 (0) - _ = +

! 2 ` ~ 2 @ 3 # 4 $ 5 % 6 ^ 7 & 8 * 9 (0) - _ = +

Key 4:

Paintext: wonderful text

Ciphertext/first stage/: -7^!2*@0% (2_(

Ciphertext/second stage/: -7^12*@0% (2_(

Notice: ! moved to the first position and 1 replaced this position.

Decryption:

Key 4:

Ciphertext/second stage/: -7^12*@0% (2_(

Ciphertext/first stage/: -7^!2*@0% (2_(

Paintext: wonderful text

Notice: Firstly, receiver need to move the first place character to the fourth place and every character in front of fourth character moves one place backward.

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
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52
B	D	F	H	J	L	N	P	R	T	V	X	Z	A	C	E	G	I	K	M	O	Q	S	U	W	**Y**
Y	B	D	F	H	J	L	N	P	R	T	V	X	Z	A	C	E	G	I	K	M	O	Q	S	U	W

In my cipher, I started out with the alphabet going A to Z, and I assigned numbers 1-26 for each corresponding letter. I then doubled these each assigned number. For the first thirteen letters (A-M), I took the new doubled number and assigned a new letter according to the new doubled numbers position on the alphabet ranging 1-26. Essentially, A(1) becomes B(2); F(6) becomes L(12), and so on until M(13) becomes Z(26). For the second thirteen letters (N-Z), I doubled each assigned number, and then subtracted 1 from the new doubled number, and assigned a new letter according the the doubled number -1. After 26, the numbers reset, so 28 would be B, 30 D, etc. The subtraction of 1 allowed the final thirteen numbers to fill in the numbers that were skipped in the first process, and all 26 letters had a ciphered, unique, and new letter. Since the cipher is symmetric and mathematic, I decided to twist it up with a Caesar Shift of one (1) place to the right. The Caesar Shift is intended to throw "Eve" off, so that he/she will not be able to immediately see the pattern that is much more clear without the shift. This is the encryption process.

To decrypt the ciphertext, one would need the key above, and would first move each letter back one position to fix the third line of alphabet (ciphertext) to the second line of alphabet (slightly less ciphered text). For the first thirteen letters (B,D,F,H,J,L,N,P,R,T,V,X,Z), which are also the even integer letters of the normal plaintext alphabet, one would simply divide by 2, and one would have the original plaintext letter. For the final thirteen letters (A,C,E,G,I,K,N,O,Q,S,U,W,Y), which are also the odd integer letters of the normal plaintext alphabet, one would also just divide by 2 to obtain the original plain text letter. So, A (28) would become 14, which is N in plaintext.

EXAMPLE: HELLO I LIKE CANDY

NHVVA P VPTH DYZFU becomes

PJXXC R XRVJ FBAHW which finally becomes HELLO I LIKE CANDY

As long as you have the last two lines of ciphertext, which reverses Caesar's Shift, you can get back to the plaintext by memorizing the numbers of the alphabet and just dividing it by 2. So although the entire key is more helpful for decrypting, it isn't necessary for a spy in a field to get the message.

The Key: For my cipher the secret key is a number between 1 and 25, which is shared by both parties. There is also an aspect of deceit that both parties need to be aware of: There are a series of random numbers distributed throughout the pattern. Both parties must know where these are.

Explanation: This cipher is somewhat similar to Caesar's shift cipher. Take the key, *k*. For each letter of the plain text, go *k* letters down the alphabet. Take this new letter, and write down its corresponding number in the alphabet (i.e. a=1, b=2, k=11). The same wraparound method is used here that was used in Caesar's cipher; if the letter is late in the alphabet then the counting is carried over to the beginning of the alphabet. An example: if the key is 4, then the letter y would be replaced by c, which would be written as 3. Every number written should be followed by a period, so double digit and single digit numbers are identifiable. Every space should be marked with an underscore, making the spaces easier to see. There are also random numbers distributed throughout the cipher, in a pattern. The pattern must be established and remembered in the key. This should be easy to remember, such as a random number added onto the end of the first word, followed by a random number added to the beginning of the second word, then two random numbers added to the end of the third word, then leaving the fourth word alone. Then that sequence is repeated over and over throughout the passage (*note: this is just an example, this is not actually the distribution of the random numbers).* The actual sequence would be defined in the key. To decipher the code, one simply must look up the corresponding letter paired with the number written and go *back* in the alphabet however many spaces the key is. Be sure they are ignoring the random numbers.

A small example:

Key: 2
Random numbers:

1. Add 1 random number to beginning of first word.
2. Add 2 random numbers to beginning of second word.
3. Add no random numbers
4. (repeat this pattern)

Plaintext: The cat woke up
Ciphertext: 5.22.10.7._1.22.5.3.22._25.17.13.7._4.23.18.

Note: the random letters continue in the pattern explained, so the fourth word now has 1 random number added to the beginning, the fifth word would have 2 random letters added, and the sixth word would have no random numbers.

COMP 133 – Assignment 1

The key
In this cipher, the key passed from the sender to the receiver is *22 vowels*.

How to encipher
The ciphertext alphabet is written out underneath the plaintext alphabet excluding the vowels A, E, I, O and U. Once all the consonants have been used, the vowels are written out in alphabetical order, A E I O U. In this way, AEIOU acts as a keyword in the cipher. When enciphering text, the sender must simply remember that the first letter of the keyword "AEIOU" falls on the 22nd letter of the alphabet (with A replacing V, E replacing W, etc.), thus the key *22 vowels.* Writing out the key, it will come to look like this:

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

All capital letters, punctuation, and spaces are removed from the plaintext, and each letter is substituted with the corresponding letter in the key shown above.

How to decipher
To decipher the coded message, the receiver must remember the key, *22 vowels.* Using this, they must recreate the key shown below by first writing out all the letters (specifically, all consonants) except for the keyword "AEIOU". Once all consonants have been written out, the keyword "AEIOU" is written out. Below this, the receiver must write out the alphabet in its original order (with B corresponding to A, C to B, … A to V, E to W, etc.). Using the key they have just written, the receiver then substitutes each letter of the ciphertext alphabet (the first row of the key shown below) with a letter from the plaintext alphabet. Looking at the string of words, they then separate each word with a space to make sense of the message.

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

Example
Key: vowel
Plaintext: who will break this code
Ciphertext: ekselppcwgbnyklxdsfg

Comp 133
Assignment 1

The Caesar Shift Cipher, with a twist

The Key: For my cipher the secret key that is known by both the sender and receiver is a number between 1 and 25. A key phrase is also known between the two that signifies what to start with. Also when you get half way through the message, the second half will use a new key that uses the same phrase, but was the previous key number + 3.

How to Encipher: Given a key k, the sender enciphers the message by first starting at the letter that corresponds to A + k. At that spot the sender will then spell out the secret phrase removing any repeated letters. Once the phrase is done, the sender will then fill in the remaining letters after A + k + catchphrase with letters in alphabetical order that have not yet been used. It is done with "wraparound," so if you get to the end of the alphabet then you go back and continue counting form the beginning. For example, if the key is 2 and the phrase is MILKY, then letter C is replaced by M, D replaced by I, E replaced by L, and so on. Once the phrase is spelled out, the next letter, H, will be replaced by A since the rest of the letters will be filled in using alphabetical order. Half way through the plaintext, a new rule of K+2 will be implemented making it A + k + 2 + catchphrase and then other letters will be represented by the alphabetical wraparound.

How to Decipher: Given a key k, in order to decipher the receiver takes each letter of the ciphertext and replaces it by the letter that is K, or K+2 in respect to the second half, positions earlier all in while keeping the catchphrase in mind that is mixed in with the alphabet. This is also done with wraparound.

Small Examples:

Encryption:
Key:2, phrase: cat

Plaintext: I went to the zoo
Ciphertext: f uthq qj obc vjj

Notice that at the half way point, the original key receives a +2.

Decryption:
Key:3, phrase: love

Ciphertext: gu vxrimbmz hzjhgf
Plaintext: my favorite person

Notice that g gets replaced by m. This is because of the phrase and the +3 key. Also, always be aware of the second half where the key has a +2 to it.

COMP 133
Assignment I

The "Cipher-Switch"

The Key: For my cipher, the secret key shared by the sender and the receiver consists of a list of numbers between 1 and 25.

How to Encipher: STEP ONE –
The sender removes every other letter of the plaintext and then places them at the end of the message. The first letter of the relocated text will have an asterisk in front of it. For example, if the edited plaintext reads "HELLO MY NAME IS LI", then the cipher text would take out every other letter and place them at the end of the message to read "HLOYAESI*ELMNMIL".

STEP TWO -
Given a key *k*, in order to encipher a message, the sender takes each letter of the plaintext and replaces it by the letter that is *k* positions later in the alphabet. This is done with "wraparound", meaning that if you get to the end of the alphabet when counting up to *k* positions, you continue counting from the beginning. BUT BE CAREFUL! The numerical value for *k* changes after every 5 letters! For example, the first key set is " 1,2,3 " and the edited plaintext reads, "HLOYAESI*ELMNMIL ". The first 5 letters would have a key of 1 and would be enciphered to spell "IMPZB", the second 5 letters would have a key of 2 and would be enciphered to spell "GUK*GN", and the third 5 letters would have a key of 3 and would be deciphered to spell "PQPLO". Altogether, the final cipher text message would read "**IMPZBGUK*GNPQPLO**".

How to Decipher: STEP ONE –
Given a key k, in order to decipher the message, the receiver takes each letter and replaces it with the letter that is *k* positions earlier in the alphabet. This is done with wraparound. BUT BE CAREFUL! The numerical value for *k* changes every 5 letters!

STEP TWO –
The reader begins to write down the plaintext, but every other letter is placed after an asterisk relatively in the middle of the message. Starting at the beginning of the message, the reader writes the first letter. Then ze writes the first letter after the asterisk . The reader writes the second letter from the beginning of the message, and then writes the second letter following the asterisk. This process is repeated until all the letters are written.

A Small Example:

Encryption:

Key: 1,7,5,4
Plaintext: I LOVED ARIZONA ICED TEA
Ciphertext: JPFBJVHJKL*QDIWERMIXE

Decryption:

Key: 1,2,3,4
Ciphertext: XZNBBGKJPY*KDLZNVJWR
Plaintext: WHY AM I AWAKE RIGHT NOW