Worksheet 17 (Cryptography 1): Shift Ciphers

Group Names: Solutions

encryption the process of transforming information in a way that, ideally, only authorized parties can decode

decryption

plaintext readable/legible version of a message (unencrypted or already decrypted/decoded)

ciphertext unreadable/illegible version of a message (already encrypted/encoded)

key variable value (word or number), often kept secret, altering the result of encryption/decryption

1. Julius Caesar communicated with his troops using an encryption scheme where each letter in the message was shifted three letters over.

	0	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
in	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
out	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

   (a) Use this cipher to encrypt the plaintext THE QUICK BROWN FOX.

   WKH TXLFN EURZQ IRA

   (b) Decrypt the ciphertext E H Z D U H W K H L G H V R I P D U F K

   BEWARE THE IDES OF MARCH

2. In general, a *shift cipher* shifts the letters of the alphabet over a certain number of steps, say n. For the classical Caesar cipher, $n = 3$. (Sometimes all shift ciphers are called Caesar ciphers.)

   (a) Fill in the table for how to encrypt and decrypt the alphabet using a shift of 13. (On the internet, this is called 'ROT-13' and is sometimes used to obscure movie spoilers, etc.)

	0	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
in	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
out	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

   (b) Decrypt the text G U R J U R R Y F B A G U R O H F

   THEWHEELSONTHEBUS

   (c) How many different shift ciphers are there? 25

   A → A isn't interesting!

3. Consider the ciphertext

N V K Y V G V F G C V F W K Y V L E Z K V U J K R K V J Z E F I U V I K F
WE THE PEOPLE OF THE UNITED STATES IN ORDER TO

W F I D R D F I V G V I W V T K L E Z F E
FORM A MORE PERFECT UNION

Suppose you know that this was encrypted using a shift cipher, but you don't know what the shift step is.

By looking at the short words in the ciphertext, guess what the shift is and decrypt the message.

	0	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
in	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
out	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

4. If you don't have spaces to help you determine word lengths, you can use *frequency analysis* to help guess which letters map to which other letters.

Consider the following ciphertext. It has been encrypted using some sort of shift cipher.

The letters of the English language sorted by frequency (say, number of appearances in 40,000 words) are

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

OD K

Here are frequencies of the letters of the ciphertext (this is a *frequency table*).

in	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
out	0	9	5	14	3	0	2	0	3	0	11	3	2	3	16	2	2	9	9	0	0	4	1	7	4	3

Use the frequency table to help you guess the shift. Then decrypt the message.

in	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
out	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

D R K D D R O I K B O O X N Y G
THAT THEY ARE ENDOW

O N L I D R O S B M B O K D Y B
ED BY THEIR CREATOR

G S D R M O B D K S X E X K V S
WITH CERTAIN UNALI

O X K L V O B S Q R D C D R K D
ENABLE RIGHTS THAT

K W Y X Q D R O C O K B O V S P
AMONG THE MEARE LIF

Q V S L O B D I K X N D R O Z E
E LIBERTY AND THE PU

B C E S D Y P R K Z Z S X O C C
RSUIT OF HAPPINESS