

Worksheet 17 (Cryptography 1): Shift Ciphers

1. Julius Caesar communicated with his troops using an encryption scheme where each letter in the message was shifted three letters over: $A \rightarrow D$, $B \rightarrow E$, 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
plain	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	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**.

- (b) Decrypt the ciphertext **EHZDUH WKH LGHV RI PDUFK**

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, $n = 3$. The shift $A \rightarrow A$ has shift $n = 0$. (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
plain	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																										

- (b) Decrypt the text

GURJU RRYFB AGURO HF.

(It’s been broken into groups of 5 for convenience, not because that’s where the spaces actually go.)

- (c) How many different shift ciphers are there? _____

3. Consider the ciphertext

NV KYV GVFGCV FW KYV LEZKVU JKRKVJ
 ZE FIUVI KF WFID R DFIV GVIWVTK LEZFE

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
plain	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																										

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**. It has been broken up into groups of 5 letters.

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

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

letter	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
count	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.

plain	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																										

DRKDD ROIKB OOXNY GONLI DROSB
 MBOKD YBGSD RMOBD KSXEX KVSOX
 KLVOB SQRDC DRKDK WYXQD ROCOK
 BOVSP OVSLO BDIKX NDROZ EBCES
 DYPRK ZZSXO CC