Worksheet 17 (Cryptography 1): Shift Ciphers

Group Names: Solutions

1. Julius Caesar communicated with his troops using an encryption scheme where each letter in the message was shifted three letters over: $A \to D$, $B \to E$, 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
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 EHZDUH WKH LGHV RI PDUFK

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, $n = 3$. The shift $A \to A$ 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
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

GURJU RRYFB AGURO HF.

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

THEWH EELSO NTHEB US

The wheels on the bus

(c) How many different shift ciphers are there? 26 but A→A is kinda silly.

3. Consider the ciphertext

NV KYV GVFGCV FW KYV LEZKVU JKRKVJ

ZE FIUVI KF WFID R DFIV GVIWVTK LEZFE

maybe KYV ← THE? compatible with A → R!

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

WE THE PEOPLE OF THE UNITED STATES
IN ORDER TO FORM A MORE PERFECT UNION

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. guess E → O

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

DRKDD THATT	ROIKB HEYAR	OOXNY EENDO	GONLI WEDBY	DROSB THEIR
MBOKD CREAT	YBGSD ORWIT	RMOBD HCERT	KSXEX AINUN	KVSOX ALIEN
KLVOB ABLER	SQRDC IGHTS	DRKDK THATA	WYXQD MONGT	ROCOK HESEA
BOVSP RELIF	OVSLO ELIBE	BDIKX RTYAN	NDROZ DTHEP	EBCES ERSUI
DYPRK TOFHA	ZZSXO PPINE	CC SS		

That they are endowed by their Creator with certain unalienable rights that among these are life, liberty, and the pursuit of happiness