

JM: I propose we use the following method for encrypting messages before we send them through email or other communication channels. I call this the S~~W~~ap and s~~I~~de C~~I~~p~~H~~er (or SWICH). I think this will foil any of the annoying eavesdropping agents that have been hounding us.

Steps for enciphering using SWICH:

1. Create a code word to be exchanged in secret – for example use the word GEM
2. Create a grid where the number of columns is the number of letters in the code word and the number of rows is 25. Having 25 rows is important!
3. Write your message in the grid across the rows – for example if your plaintext was “The grey squirrel jumped over the small hill to catch a nut falling from a tall green tree” you would get:

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

4. Reorder the columns so that they are alphabetical according to the code word (this is the Swap):

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

- Now create the ciphertext grid as follows. Make a shifted alphabet column that contains the alphabet in the order below. Note I/J are on the same row since we're only using 25 rows. Now we're going to SLIDE each column of letters up a certain amount (with the ones falling off the top, appearing back on the bottom). Recall that each column is labeled with a letter from the code word. For each column, find the code word letter in the shifted alphabet column, and slide the column up starting from this position. See the example for clarification. This should sufficiently mix things up to make it hard to read.

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

6. Finally read the ciphertext across the rows of the ciphertext grid and group them into sets of 5:

IELTA MAHDH LEUCH ACPIN LFFLM LOEGT
 LOARH TNALE GNHER RRTST TIGLE YEUUT
 EREVJ ETPES OQLRR

7. I trust that given this method for encryption you can figure out how to decrypt.