

TUESDAY AFTERNOON MINI-LECTURE

SPY GAMES CAMP – PSU, 2014

The following would make a good mini-lesson for a curriculum mentor to present, or I could do it.

- (1) History, is a simple and easy to use variant of a transposition cipher. Used for serious purposes even in the cold war (as parts of other ciphers). Certainly used by Germans in World War I (combined with a substitution cipher) and used by various Allied Forces in WWII where it was performed twice (double columnar transposition).
- (2) It can be identified if a letter frequency analysis yields a similar breakdown to English.
- (3) Here is an example, our keyword is CAT

C	A	T
T	H	E
G	E	R
M	A	N
F	O	R
C	E	S
A	R	E
H	E	R
E	Y	B

We then read the columns vertically starting from the column with first letter in alphabetical order. In this case we get H E A O E R E Y T G M F C A H E E R N R S E R B

- (4) Have people break off into pairs and have them send each other a message using this cipher.
- (5) To break it, the typical approach is to guess the key length and then try anagrams from the rows For example, see if people can break the following.

VDASQEYHIYRGHAHEOSDG

Try a key length of 4. The resulting message unlocks the Columnar Transposition function in the computer.