

## THURSDAY MORNING 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) Autokey is similar to Vigenère. In fact, Vigenère was not invented by Vigenère, Autokey is. It is somewhat more secure than Vigenère.
- (2) Do an example. You pass a key, say **frogs**.

f	r	o	g	s	a	l	l	y	o	u	r	b	a	s	e	a	r	e	b	e	l	o	n	g
a	l	l	y	o	u	r	b	a	s	e	a	r	e	b	e	l	o	n	g	t	o	u	s	
F	C	Z	E	G	U	C	M	Y	G	Y	R	S	E	T	I	L	F	R	H	X	Z	I	F	

- (3) Autocorrelation can still be used to find the key length, although you won't have repeated jumps.
- (4) After you identify the key length, you can figure out the cipher text as follows. Choose some common words in English (like *the* and *that* or even just *ing* etc., or choose some words you expect to appear in the ciphertext, names?). Now start decrypting random parts of the ciphertext using those words as if they were Vigenère keys. If something makes sense, you can then shift that by your key length and repeat.