MONDAY 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) Discussion of history. Vigenére cipher was the le chiffre indéchiffrable (the indecipherable cipher). It was actually first described by Bellaso. It was considered unbreakable from the 16th to the 19th centuries (was still used heavily in the civil war). We'll learn some techniques to break them later.
(2) Vigenere ciphers are basically Caesar shifts but different letters are shifted by different amounts.
(3) Do an example. Choose at the key `frogs`.

f	r	o	g	s	f	r	o	g	s	f	r	o	g	s	f	r	o	g	s	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	t	o	u	s	
F	C	Z	E	G	Z	I	P	G	K	J	R	F	K	T	J	C	C	T	Y	Y	F	I	Y	

(4) It is unbreakable if you use a random key as long as the plaintext (and you do not reuse the key). This is called a one-time pad. These were in use (and are still in use) throughout the cold war and earlier.
(5) Have people break off into pairs and send each other a message using the Vigenére cipher. (They should decide on a key word first secretly). Pass out messages to encrypt and decrypt by hand.
(6) Have each team decrypt the ciphertext `PCBRFVXQF` using the keyword `SECRETMESSAGE`. The result of this code is the key to unlock the Vigenere cipher in the computer. Have each team unlock the Vigenere cipher.