

**PMAT 329 Introduction to Cryptography**  
**HINTS FOR PROBLEM 1 OF ASSIGNMENT 2**

---

1. Five cipher alphabets were used. This isn't much of a hint, because it's the factoring example from class, which established a key length of 5 already.
2. This is a mixed Vigenère cipher. You can figure this out by applying Kerkhoff's shortcut and realizing that it doesn't work.
3. The mixed Vigenère alphabet is derived from the ordinary alphabet using an English key word. The meaning of this word happens to be very appropriate for this exercise.
4. The shifts determining the 5 cipher alphabets are also given by an English word. In other words, the actual Vigenère key is also an English word.
5. Frequency analysis leaves a number of ambiguities, so here are the ciphertext letters for the plaintext letters E, O, R, S, T.

Plain	A	B	C	D	E	F	...	M	N	O	P	Q	R	S	T	U	V	...	Z
C 1					I					M			Q	R	V				
C 2					W					I			B	C	D				
C 3					Z					G			D	F	J				
C 4					C					R			Y	Z	E				
C 5					Q					U			I	N	G				

From this information, you should be able to fill in most of the table rather easily. You'll still need some smarts and some good guesses to fill it all in. Try to recognize (or guess) the Vigenère alphabet key word (the one referred to in item 3 above). Also, think about how you read the Vegenère key word (the one referred to in item 4) from the table above; that may help with your guessing and filling in letters.