Solution to Challenge 3

Start by using the description of the MPSC cipher and Hint 1. We have:

pt:	m	u	s	t
Translate by:	2	3	4	5
CT:	P	Y	X	Z

What this tells you:

1. If "m" was shifted two to the right to arrive at "p", the "n" or "o" must be missing in between them. That means that "n" or "o" (but not both) appear in the keyword. This assumes that "m" isn't in the keyword, but since it lies two letters from "p" it looks like it is in the normal alphabetical sequence.
2. One of "v", "w", or "x" must also be in the keyword. (The keyword is not "kryptos" !). Again, this assumes that "u" is not in the keyword.
3. Once again, since "s" is about 4 letters from "x" in the normal alphabet, we assume that "s" and "x" are not in the keyword but appearing in alphabetical order. This agrees nicely with #2: "v" or "w" is in the keyword AND "t" and "u" are NOT in the keyword (since we need these letters to keep "s" and "x" 4 letters apart.
4. If "v" or "w" is in the keyword, this makes "t" 5 letters from "z" if "y" and "z" are not in the keyword. Then end of the alphabet line looks like:

   … m (n o) p… s t u (v w) x y z

   where parentheses were used to indicate groupings where one letter is missing (and appears earlier in the keyword).

In order to make further progress, one might start guessing at possible two letter words that could reasonably precede "must": "we" and "it" come to mind. If, for example, we think the first word is "we", we arrive at:

5. The string "wr" must appear in the reduced keyword.
6. The letter "e" must also be in the reduced keyword (two characters before "w"):. The reduced keyword has the string "e?wr".

The fifth word has a double ciphertext letter:

pt:	?	?	?	?
Translate by:	5	6	7	8
CT:	M	H	X	X

Since we know (#5) "r" appears earlier in the alphabet line as part of the keyword and one assumes that the keyword does not contain "q", the alphabet line ends something like:

… m (n o) p q s t u v x y z

Seven places to the left of "x" must be an "n" or an "o" and eight places to the left of "x" must be an "m". Thus, the fifth word ends with "nm" or "om". The second is the most reasonable.

7. We'll assume that the fifth word is "??om", which means that "n" is also part of the keyword.
8. The fifth word can not have a double "o": "?oom". At this point not too many four letter words ending in "om" come to mind (when we exclude the double "o"s).
9. Perhaps the most common would be "from". Let's assume the fifth word is "from":

pt:	f	r	o	m
Translate by:	5	6	7	8
CT:	M	H	X	X

10. In order for "f" and "m" to be five letters apart, two of "g, h, i, j, k, l" must be in the keyword.
11. Since "r" is in the keyword, unless the keyword is very long, "h" is not in the keyword.

If we manage to find Hint #2 (see solution to Challenge 1), we can use the fact that the reduced keyword has seven letters. [The hint also confirms our guess that the first word is "we".] We already know that the reduced keyword contains "e,w,r,n" and exactly two of "g, i, j, k, l". This accounts for six letters. The seventh letter must be from "a, b, c, d, f". Our alphabet line looks something like:

[seven letter reduced keyword] (a b c d f)(g H i j k l) m o p q s t u v x y z
1 2
missing missing (not H)

pt:	w	e	m	u	s	t	p		o			c b		o									f	r	o	m
Translate by	1	2	2	3	4	5	3	4	5	6	7	8	9	4	5	6	7	8	9	10	11	12	5	6	7	8
CT:	R	W	P	Y	X	Z	T	F	U	A	F	O	E	T	A	H	A	G	F	R	K	W	M	H	X	X

pt:			b a									
Translate by	6	7	8	9	10	7	8	9	10	11	12	13
CT:	K	W	M	H	O	H	C	M	T	G	Q	O

12. We've filled in a few more letters of the plaintext and also know that the sixth letter of the third word is a "b" or "c". Also, the third letter of the sixth word is an "a" or "b". We also know that the last letter of the sixth word will be the last letter in the reduced keyword (which is not an "e" or "w").
13. Let's focus on the third word. With a little help from a crossword dictionary (http://crosswordnexus.com/dictionary), one doesn't find any word of the form "p?o??b?". If we try "p?o??c?" we have several possibilities: Produce, product, project, protect. Let's assume that the second letter is an "r". This means that "f" cannot be part of the keyword (since "e?wr" is part of the reduced keyword and "f" must be four places to the right of "r".). So, "f" is not in the keyword and the string "e?wr" must be the end of the reduced keyword. This also means that the last letter of the sixth word is also an "r". We also know that the last letter of the third word is now a "t" and the fifth letter must be an "e".

```
pt:             w e   m u s t   p r o   e c t   o                   f r o m

Translate by     1 2   2 3 4 5   3 4 5 6 7 8 9   4 5 6 7 8 9 101112  5 6 7 8
CT:             R W   P Y X Z   T F U A F O E   T A H A G F R K W   M H X X

pt:                 b    r
                    a
Translate by    6 7 8 9 10  7 8 9 10 11 12 13
CT:             K W M H O   H C M T  G Q O
```

14. There are only two possibilities left for the third word: “protect” and “project”. We could try them both, but “protect” sounds like a more likely fit. This means that the first letter of the reduced keyword is an “a” and the alphabet line looks like:

    a ? ? e ? w r b c d f (g H i j k l) m o p q s t u v x y z

resulting in:

```
pt:             w e   m u s t   p r o t e c t   o u r s     v   s   f r o m
                                                    w
Translate by     1 2   2 3 4 5   3 4 5 6 7 8 9   4 5 6 7 8 9 101112  5 6 7 8
CT:             R W   P Y X Z   T F U A F O E   T A H A G F R K W   M H X X

pt:               y b e  r  w a r  f    r  e
                    a
Translate by    6 7 8 9 10  7 8 9 10 11 12 13
       CT:      K W M H O   H C M T  G Q O
```

At this point the remaining letters can be surmised:”We must protect ourselves from cyber warfare.”