Kryptos 5- Challenge 3: Solution

In Challenge 3 you are told the Ragbaby Cipher was used to encipher the text message and that “meet” is likely the first word. You are asked to find the time and place of a suspected meeting.

We know from the description of Ragbaby that the J and X are excluded from the cipher alphabet to reduce it to 24 letters. The keyword without repeated letters is at the beginning and the rest of the alphabet follows alphabetically.

Following the description of the cipher, we know that following shifts took place:

1	2	3	4		2	3	4	5	6	7	8		3	4	5	6	7	
N	A	C	Z		A	O	G	I	O	U	K		C	N	M	P	B	
4	5	6	7	8	9	10		5	6	7		6	7	8	9			
Z	O	G	O	N	M	M		C	V	H		V	S	Z	K			
7	8	9	10	11		8	9	10	11	12	13	14	15	16	17			
H	T	S	U	C		N	M	H	I	Z	Y	Z	H	Q	F			
9	10	11	12	13	14		10	11	12	13	14	15		11	12	13	14	15
M	D	M	E	G	Q		M	M	O	B	N	L		R	Z	B	E	T
12	13	14		13	14	15	16		14	15	16	17	18		15	16	17	18
Q	Y	V		F	T	E	T		Q	L	I	Q	Z		N	T	W	O

We will use the notation (1,N) to mean that the plaintext was shifted by 1 to get the ciphertext N. So for the first ciphertext word we will write (1,N) (2,A) (3,C) (4,Z). This will help keep track of how the message was enciphered.

Working with the assumption that the first word is MEET, we know:

1) (1,N) deciphers to M means N is one to the right of M: MN
    - Knowing that after the keyword, letters appear alphabetically we can guess that since MN is the usual alphabetical sequence of letters that most likely neither letter appears in the keyword.
2) (2,A) deciphers to E so A is two to the right of E: E _ A
    - Since alphabetically E comes *after* A these are in the wrong order so E must be in the keyword. It is possible that A is also in the keyword or that A is the first letter after the end of the keyword
3) (3,C) deciphers to E so C is three to the right of E: E _ _ C

- Putting this together with the clue from (2) we know we have **E _ A C** so it seems reasonable to guess that A is the first letter after the keyword and B is in the keyword since it is not written between A and B in the code alphabet.

4) (4,Z) deciphers to T so Z is four to the right of T: T _ _ _ Z
   - Since T and Z look to be in about the right place alphabetically we can guess neither is in the keyword. However, in the usual alphabet we have T U V W Y Z (excluding X) so we know that since there are only three letters between T and Z exactly one of U, V, W, or Y must be in the keyword.

Summarizing what we have so far our Ragbaby alphabet looks somewhat like this

--?- **E _ A C** D F G H I K L M N O P Q R S **T** U V W Y **Z**

where B and one of the red letters is in the keyword and the bold green letters are in the correct spots.

To proceed we can use information about how the cipher works as well as context clues:

There are several useful facts resulting from the cipher structure:

5) Any time the same letter occurs in the ciphertext with the same shift then it represents the same plaintext letter. So for example we know that (3,C) corresponds to a plaintext of E and that (shift,letter) combination also appears as the first letter of the second and third words so we can conclude those both being with an "E". Further (4,Z) corresponds to T so the first letter of the fourth word is T. We also see multiple (9,M)'s (11,M)'s, etc.
6) If we see a double letter in the ciphertext, then most likely the plaintext letters were in reverse alphabetical order in the alphabet. For example the double M's at the end of the fourth word indicate that if we shifted the second to last letter in the word by 9 we get M and we had to shift the last letter in the word by 10 to get to M. That means alphabetically the last letter was one further away from M than the second to last letter (something like ed or po, etc.)
7) If there are two letters next to each other in the ciphertext that are in reverse alphabetical order then that represents a **double letter** in the plaintext. For example in the seventh word there is a **T S** sequence. The second letter was shifted by 8 to get T but only shifted by 7 to get to S so if S and T are next to each other in the alphabet then the same letter shifted by 7 to get S would have to be shifted by 8 to get T. This also tells us that it is likely that S and T are next to each other in our alphabet or that S is also not likely used in the keyword.

Clues 5,6,7 will help us using the structure of the cipher, and it is possible to solve using these rules, statistics about letter frequency and diligent guess and checks, but we can also use the clues from the backstory. We are told that a meeting day and time and are likely indicated so there are quite possibly some numbers and days written out in the message.

Let's look at how many letters are in each word to see if we can match up any possible numbers or days of the week.

Let's consider numbers and days of the week:

Possible Word in Plaintext (crib)	Letter count
Monday	6
Tuesday	7
Wednesday	9
Thursday	8
Friday	6
Saturday	9
Sunday	6
One	3
Two	3
Four	4
Five	4
Six	3
Seven	5
eight	5
nine	4
ten	3

Word # in ciphertext	number of letters	first letter of word
1	4	m
2	7	e
3	5	e
4	7	t
5	3	
6	4	
7	5	
8	10	
9	6	
10	6	
11	5	
12	3	
13	4	
14	5	
15	4	

Word 2 starts with an e and is seven letters – no day or number has that property

Word 3 starts with an e and is 5 letters long – it could be the word eight

Word 4 starts with a t and is 7 letters long – it could be the word Tuesday

There are other words of the correct length that could be letters or days, but we have to start somewhere and knowing the first letter gives us some hope.

Let's start by assuming the third word is "eight"

3	4	5	6	7
C	N	M	P	B

We already know (3,C) corresponds to the plaintext E so let's look at the other letters and shifts.

8) If (4,N) deciphers to I, then I was shifted by 4 to get to N: I _ _ _ N . In usual alphabetical order we'd have **I K L M N** (remember no J) so this matches and we assume none of the middle letters are in the code word
9) (5,M) gives a cipher alphabet of G _ _ _ _ M this also fits with **G H I K L M** so we will assume this sequence is also correct.

10) (6,P) gives a cipher alphabet of H _ _ _ _ _ P. Putting this with (1) and (9) we get **H I K L M N P** (since 1) told us that M N are together in the code alphabet). This leaves no room for the 'O' that should go between N and P so we assume O is in the keyword.
11) (7,B) T _ _ _ _ _ _ B . From 4) we are guessing we have T U V W Y Z where one of U,V,W,Y is missing. Therefore to get to B from T we must wrap around to the beginning of the alphabet: T U V W Y Z _ _ B (since there are only 3 of the 4 red letters present).

Putting our first (11) observations together we now have:

_ _ B ? .. --- **E _ A C** D F G **H I K L M N P** Q R S **T** U V W Y **Z**

with O and one of U,V,W or Y also in the keyword

At this point we could go try to fill in more of the plaintext in the cipher or continue with our day of the week guess. Let's pursue the idea that the 4th word might be "Tuesday"

4	5	6	7	8	9	10
Z	O	G	O	N	M	M

We already know (4,Z) corresponds to the plaintext T so let's look at the rest:

12) (5,0) deciphers to U so we have U _ _ _ _ O. These are in the wrong alphabetical order and we are already guessing in 10) that O is in the keyword so let's assume that U is NOT in the key word. Then we know U V W Y **Z _ O B** (since there are only two of the three red letters)
13) (6,G) deciphers to E – we already have an idea where E is: **E _ A C** D E F G. This matches with a shift of 6 from E to G meaning D,E,F and G are all in the correct spot! **E _ A C D E F G.**
14) (7,O), (8,N) and (9,N) deciphering to S, D, and A respectively is consistent with our assumptions and tells us nothing new, but confirms we may be on the right track.
15) (10,M) deciphers to Y means we have this situation: Y _ _ _ _ _ _ _ _ _ M
If Y were at the end of the alphabet this would not be possible. Hence we now know Y must be the letter from the V W Y sequence that is used in the keyword, further we can figure out it's location by backing up from M:
Y A C D F G H I K L M

Putting this together we have:

_ O B ? E Y A C D F G H I K L M N P Q R S **T U V W Z**

There are many ways to figure out the rest including: start solving for whatever ciphertext you can and deduce the rest; make another guess of word; or just guess.

We observe that all that is left to determine is if Q R S are in the keyword. Since U is not in the keyword it is unlikely that Q is. We might either have the R and S or just one of the two depending on if there is a letter where the ? is in the code alphabet. Let's start and just guess R. That would give:

R O B E Y A C D F G H I K L M N P Q S T U V W Z

A check of this reveals it is correct. After careful inspection of the keyword "Robey", realizing that letters can't be repeated, and knowing this scenario dealt with a theft might lead you to guess the correct keyword was "Robbery"

When deciphered the final plaintext reads:

Meet exactly eight Tuesday one nine eight Darrington avenue yellow lilly and take extra read.

The "yellow lilly and take extra read" is a bit strange. Maybe "yellow lilly" refers to what someone may be wearing to help with identification. But what about "take extra read"? Let's *take an extra read*! Further reading of the somewhat oddly worded plaintext reveals a second message hidden within this. This message is found by looking at the first letter of each word only:

Meet exactly eight Tuesday one nine eight Darrington avenue yellow lilly and take extra read.

or Meet one day later. Hence the final answer to the Challenge 3 question of meeting time and place is

WEDNESDAY at exactly eight at 198 Darrington Avenue.