Challenge 1: Solution

The numbers in the 1040 tax form do not seem to be realistic values for an actual tax return, most likely they constitute the coded message. Some observations:

- Each entry in the "dollars" column has an even number of digits (some even start with a leading zero).
- Sometimes the "cents" column is filled in, sometimes not. When it is filled in in contains "00".
- The image of the Mexican Army Cipher, in addition to containing the name of the underlying cipher, also contains a brief description of how it is to be used: "To encode a letter select any number in the same column as that letter".

One can find more information about the Mexican Army Cipher online or easily assume from the give information that this cipher replaces each plaintext letter with one of four different two digit numbers: 01 – 00. This has the effect of making frequency analysis a bit more difficult, especially if the message is fairly short. We give two different solutions below.

Version 1: Try Frequency Analysis

If we read off the numbers on the tax form, in pairs, we get our encrypted message:

09 75 12 68 59 18 27 67 25 93 14 42 68 01 30 03 45 00 14 21 05 38 10 66 89 23 25 55 74

08 42 47 59 70 46 97 47 14 41 93 22 55 12 47 09 08 82 72 48 68 13 25 47 51 48 34 37

15 52 38 87 69 28 12 26 45 55 73 96 00 63 40 02 14 27 69 52 63 95 47 34 06 17 41 59 08

21 49 70 72 09 21 36 62 97 08 40 00 48 68 01 66 09 47 40 13 41 69 80 27 45 48 08 61

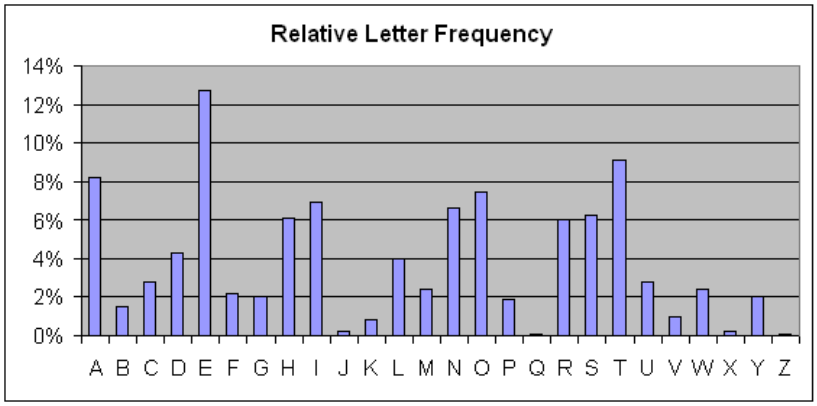
Not quite sure what to do with the "00" in the cents column, this has been ignored.

A quick investigation into how this cipher works tells us there are four different shift ciphers used. To decrypt we need to know the amount of each shift. A good place to start is a frequency analysis of the numbers grouped as two digit numbers.

Ring 1	tally	Ring 2	tally	Ring 3	tally	Ring 4	tally
01	II	27	III	53		79	
02	I	28	I	54		80	I
03	I	29		55	III	81	
04		30	I	56		82	I
05	I	31		57		83	
06	I	32		58		84	
07		33		59	III	85	
08	IIIII	34	II	60		86	
09	IIII	35		61	I	87	I
10	I	36	I	62	I	88	
11		37	I	63	II	89	I
12	III	38	II	64		90	

13	II	39		65		91	
14	IIII	40	III	66	II	92	
15	I	41	III	67	I	93	II
16		42	II	68	IIII	94	
17	I	43		69	III	95	I
18	I	44		70	II	96	I
19		45	III	71		97	II
20		46	I	72	II	98	
21	III	47	IIIIII	73	I	99	
22	I	48	IIII	74	I	00	III
23	I	49	I	75	I		
24		50		76			
25	III	51	I	77			
26	I	52	II	78			

Next compare the tally's to a frequency analysis of the English language to make a guess as to how the alphabet was shifted. It can be particularly useful to look for where the "e" might be or where they "xyz" may be located.



Once you make a guess, check to see if the corresponding plaintext makes sense. If not, revise your guess. The following is the correct assignment of the shift:

Ring 1	tally	shifted alphabet	Ring 2	tally	shifted alphabet	Ring 3	tally	shifted alphabet	Ring 4	tally	shifted alphabet
01	II	G	27	III	T	53		Y	79		Q
02	I	H	28	I	U	54		Z	80	I	R
03	I	I	29		V	**55**	**III**	**A**	81		S
04		J	30	I	W	56		B	82	I	T
05	I	K	31		X	57		C	83		U
06	I	L	32		Y	58		D	84		V
07		M	33		Z	59	III	E	85		W
08	IIIII	N	**34**	**II**	**A**	60		F	86		X
09	IIII	O	35		B	61	I	G	87	I	Y
10	I	P	36	I	C	62	I	H	88		Z

11		Q	37	I	D	63	II	I	**89**	**I**	**A**
12	III	R	38	II	E	64		J	90		B
13	II	S	39		F	65		K	91		C
14	IIII	T	40	III	G	66	II	L	92		D
15	I	U	41	III	H	67	I	M	93	II	E
16		V	42	II	I	68	IIII	N	94		F
17	I	W	43		J	69	III	O	95	I	G
18	I	X	44		K	70	II	P	96	I	H
19		Y	45	III	L	71		Q	97	II	I
20		Z	46	I	M	72	II	R	98		J
21	**III**	**A**	47	IIIIII	N	73	I	S	99		K
22	I	B	48	IIII	O	74	I	T	00	III	L
23	I	C	49	I	P	75	I	U			
24		D	50		Q	76		V			
25	III	E	51	I	R	77		W			
26	I	F	52	II	S	78		X			

This shift corresponds to the rings of the Mexican Army Cipher wheel lining up as follows:

A-21-34-55-89

Decrypting the message gives the following plaintext:

Our next meeting will take place at nine pm in the barn on tronsen road. Use your flashlight to signal when approaching: long, long, short, long.

Version 2: Use Common Words

If we assume that the "00" in the cents column represents a word break, or a space, the encrypted message looks like:

09 75 12 68 59 18 27 67 25 93 14 42 68 01 30 03 45 00 14 21 05 38 10 66 89 23 25 55 74

08 42 47 59 70 46 97 47 14 41 93 22 55 12 47 09 08 82 72 48 68 13 25 47 51 48 34 37.

15 52 38 87 69 28 12 26 45 55 73 96 00 63 40 02 14 27 69 52 63 95 47 34 06 17 41 59 08

21 49 70 72 09 21 36 62 97 08 40 00 48 68 01 66 09 47 40 13 41 69 80 27 45 48 08 61

There are three different 3-letter words. The most common 3-letter word is "the", so one might try substituting "the" into each position to see if any readable plaintext results. For example, if we think "the" corresponds to the word "14 41 93", then we can assume that the wheels on the cipher disk are turned so that the "14" is below the "T", the "41" is below the "H", and the "93" is below the "E". This will now let us decrypt most of the message. That is, any number between 01 – 26, 27 – 52, and 79 – 00. This will give you enough text to see if your guess is correct (in this case it is) and to figure out the setting of the third wheel.

The final plaintext message is:

“Our next meeting will take place at nine pm in the barn on tronsen road. Use your flashlight to signal when approaching: long, long, short, long.”