CHALLENGE 3 SOLUTION

After examining the scrap of paper it looks like the method of encryption is to use three 5x5 Polybius squares to create the ciphertext. A Polybius square is made by writing a codeword across the rows (omitting duplicate letters) and then filling in the rest of the square with the remaining unused letters of the alphabet in alphabetical order (the letter J is omitted). Below the codewords used were “Saturday” “Thirteen” and “Diamond”

3				
D	I	A	M	O
N	B	C	E	F
G	H	K	L	P
Q	R	S	T	U
V	W	X	Y	Z

1				
S	A	T	U	R
D	Y	B	C	E
F	G	H	I	K
L	M	N	O	P
Q	V	W	X	Z

2				
T	H	I	R	E
N	A	B	C	D
F	G	K	L	M
O	P	Q	S	U
V	W	X	Y	Z

To encrypt, you pair up the plaintext letters and then use the squares as follows to create a triple of ciphertext letters for each plaintext pair. (Example WA)

1. The first ciphertext letter is in square 1 in the same row and directly to the left of the first plaintext letter (wrap around to the end if the letter is at the beginning of a row) (Example W becomes V).
2. The second ciphertext letter is in square 2 at the intersection of the row in square 1 containing the first plaintext letter and the column in square 3 containing the second plaintext letter (Example X).
3. The third ciphertext letter is in square 3 in the same column and directly above the second plaintext letter (wrap around to the bottom if the letter is at the top of a row) (Example A becomes X).

To decrypt we need to build the squares from the ciphertext.

```
VXX CAV TQE GFZ EHV AIX REF NLE FFK QUA ONZ KLN LEW ATZ
KMH HKF EIX GBP RHO LHD XZZ KGT AIX RHL LHO NLN GCX ZWP
BCX HLE SRB LSH REI LHT MHV UPW ATZ BCX
```

The first letter in each triple was encrypted using square 1 and the third letter using square 3. The middle letter of the ciphertext helps you connect rows and columns.

We see there are a number of triples with a middle letter of H:

```
EHV, RHO, LHD, RHL, LHO, LHT, MHV
```

This means that

- The first letter in these triples (E,R,L,M) are in some order in the *same row* in grid 1 which gives me 4 of the 5 letters in that row
- The third letter (V,O,T,D,L) are in some order in the *same column* in grid 3. This gives me all 5 letters in that column.
- This row and column intersect at H in grid 2.

If we put (E,R,L,M) in alphabetical order we get ELMR. The E and R seem way out of sequence here so I'm going to guess that these letters are part of the codeword and most likely in the **top row of grid 1**.

Next I look for other groupings that also have ERLM as the first letter but something other than H as the second letter. This will tell me other letters in the top row of grid 2:

EIX, LEW, LSH, REI

This tells me that in addition to **H**, **the letters I, E, S are also in the top row of grid 2.**

Now I can look up ciphertext triples with I,E and S as middle letters to see if I can find the fifth letter from row one of grid 1. I see the ciphertext triple AIX which tells me A (from grid 1) is in the same row as I (from grid 3). But I already know that I is in the same row as R (from grid 1); hence A is in the same row as R in grid 1 and thus is the missing letter from row 1. Now I have

- **Row 1 of grid 1 contains: E, R, L, M, A**

Before we put this all together, let's consider the order for the letters in the *column* of grid 3 which we know to V,O,T,D,L.

Alphabetically we get DLOTV. This might not be the correct order, but I'll put them there until I know more.

So thus far we have the following grid. We are sure about the letters but not about the ordering:

					3				
					D				
					L				
					O				
					T				
					V				
1					2				
E	R	L	M	A	H	I	E	S	

Let's see if we can find the last letter of row 1 of grid 2. We look for triples with E,R,L,M or A as the first letter that have something other than H, I, E, S as the second letter. We find ATZ. That means "T" is our missing letter. This also makes me think that HEIST might be the codeword for grid 2. That makes sense both with the letters and the context of the backstory for Challenge 3. If so, we can fill in all of grid 2 to get the following:

					3				
					D				
					L				
					O				
					T				
					V				

1					2				
E	R	L	M	A	H	E	I	S	T
					A	B	C	D	F
					G	K	L	M	N
					O	P	Q	R	U
					V	W	X	Y	Z

Using grid 2 we can find the letters in each row and column of the other grids.

Grid 1

Any ciphertext triple that has a A,B,C,D,F as the second letter will have a first letter found in row 2 of grid 1. Here are some such ciphertext triples:

CAV, GBP, BCX, GCX, FFK, GFZ

- This tells me that B, C, F, G are in the second row of grid 1. This leads me to believe there is also a D in this row and that after this my grid might be alphabetical since it seems like 10 letters is long for a codeword. That means that except for the order of the letters in the first two rows, grid 1 might look like this:

					3				
					D				
					L				
					O				
					T				
					V				

1					2				
E	R	L	M	A	H	E	I	S	T
B	C	D	F	G	A	B	C	D	F
H	I	K	N	O	G	K	L	M	N
P	Q	S	T	U	O	P	Q	R	U
V	W	X	Y	Z	V	W	X	Y	Z

Grid 3

Any ciphertext triple with second letter E,B,K,P,W will have its third ciphertext letter in column 2 of grid 3. Looking through the ciphertext triples I get:

GBP, LEW, REF, REI, HKF, UPW, ZWP

- This tells me that I, F, P, W are in the second column of grid 3

Continuing in this manner and put the letters in alphabetically gives the following. Some letters are missing because they didn't occur in the ciphertex.

					3				
					D		E	B	A
					L	F		H	K
					O	I	N		
					T	P			
					V	W	X		Z
1					2				
E	R	L	M	A	H	E	I	S	T
B	C	D	F	G	A	B	C	D	F
H	I	K	N	O	G	K	L	M	N
P	Q	S	T	U	O	P	Q	R	U
V	W	X	Y	Z	V	W	X	Y	Z

We have letters in the right rows and columns, but the order of the letters in the first two rows of grid 1 and the columns of grid 3 might be wrong so let's think about a frequency analysis and see if we can figure out the order.

Grid 1

All of the first letters of the ciphertext triples come from grid 1. Doing a frequency analysis on these letters give:

L: 5

A,R: 4

G,K: 3

B,E,H,N: 2

V,C,T,F,Q,O,X,Z,S,M,U: 1

Now consider row 1 of grid 1: The frequency of the letters in this row (considered as ciphtertext) are (in order) L(5), R(4), A(4), E(2), M(1). If we look at the letters in that row then in terms of frequency in the English language they are ordered as E, A, R, L, M. Going strictly by this, and remembering the CT is to the left of the PT, we might have an ordering like this:

- Grid 1 Row 1: RALEM or some rotation (ALEMR, LEMRA, EMRAL, MRALE).

For row 2: The frequency of letters in this row as ciphertext are: G(3), B(2), C(1), F(1), D(0), and as plaintext: D,C,F,G,B. Based on this we guess the ordering to be:

GDBCF, DBCFG, BCFGD, CFGCB, FGDBC

- However since after the codeword is done we expect the letters to be alphabetical, we pick: DBCFG.
- This means "D" is likely part of the codeword (along with RALEM) and the block is alphabetical after that. Using a scrabble dictionary I come up with the word "EMERALD" which makes sense for this backstory and matches one of my orderings so I will try that.

					2				
					D		E	B	A
					L	F		H	K
					O	I	N		
					T	P			
					V	W	X		Z

1					3				
E	M	R	A	L	H	E	I	S	T
D	B	C	F	G	A	B	C	D	F
H	I	K	N	O	G	K	L	M	N
P	Q	S	T	U	O	P	Q	R	U
V	W	X	Y	Z	V	W	X	Y	Z

Grid 3

We are missing a few letters in grid 3 so let's take a closer look:

3				
D		E	B	A
L	F		H	K
O	I	N		
T	P			
V	W	X		Z

If we assume that the codeword is shorter than 10 letters then we have a problem with this ordering since in row 3 we see N after O which is incorrect alphabetically. Similarly P should come before T, not after. This makes me think that O and P are in the codeword so I will move them to the top line. Similarly B should not come before A. Since A's are more common than B's in words, I will assume A is in the codeword and move B down a line:

3				
O	P	E		A
D	F		B	K
L	I	N	H	
T				
V	W	X		Z

Now this most likely implies that the codeword ends just before “B” which means everything after B should be alphabetical. Thus I will move K down one line. Since I is more common than F, I will switch I and F in column 2 to put I in the codeword. This means L is now in the wrong place so I will also switch D and L and move N down. This makes T be out of order now unless it is in the codeword – putting T in row 2 fixes the problem.

3				
O	P	E		A
T	I		B	
D	F		H	K
L		N		
V	W	X		Z

Since there is a space between F and H and only one possible letter, it must be G. For similar reasons I can place the C, M and Y:

3				
O	P	E		A
T	I		B	C
D	F	G	H	K
L	M	N		
V	W	X	Y	Z

Let’s try decrypting and see what we get:

1				
E	M	R	A	L
D	B	C	F	G
H	I	K	N	O
P	Q	S	T	U
V	W	X	Y	Z

2				
H	E	I	S	T
A	B	C	D	F
G	K	L	M	N
O	P	Q	R	U
V	W	X	Y	Z

3				
O	P	E		A
T	I		B	C
D	F	G	H	K
L	M	N		
V	W	X	Y	Z

CT	VXX	CAV	TQE	GFZ	EHV	AIX	REF	NLE
PT	WE	FO	U?	DA	MO	LE	AM	O?
CT	FFK	QUA	ONZ	KLN	LEW	ATZ	KMH	HKF
PT	G?	SC	HA	NX	EP	LA	N?	IM

WE FOU?D A MOLE AMO?G ?S CHAXWE PLAN? IM…

This looks promising, but not quite right. If we do the following to grid 3:

- Move N to the second row of column 3,
- Put an S in the fourth row of column 4, and
- Put a U in the fourth row of the last column

we get

WE FOUND A MOLE AMONG US CHANGE PLANS IM…

This makes more sense. We now only have two missing letters from grid 3 (R and Q). If we put R in the top row of column 4 and place the Q in the last open spot then we get the following grid which is alphabetical after the N in row 2. That means it satisfies the criteria for a Polybius square with codeword containing the letters (OPERATIN) which matches gives a codeword of "OPERATION". Our final grid is:

3				
O	P	E	R	A
T	I	N	B	C
D	F	G	H	K
L	M	Q	S	U
V	W	X	Y	Z

1				
E	M	R	A	L
D	B	C	F	G
H	I	K	N	O
P	Q	S	T	U
V	W	X	Y	Z

2				
H	E	I	S	T
A	B	C	D	F
G	K	L	M	N
O	P	Q	R	U
V	W	X	Y	Z

Using this to decrypt we get:

There is a mole among us change plans immediately and leave the device in the safe drop place