CHALLENGE 2 SOLUTION

We are given the method of encryption in the file found by the undercover agent. In particular we know that there must be 25 rows in the SWICH grid. Counting the letters in the ciphertext we see there are 100 letters so there must be 4 columns in the grid. We know that the ciphertext was read off the final grid horizontally so we can put it back in the grid and try to reverse our way through the encryption process.

Final grid with cipher text:

1	T	B	C	I
2	M	D	W	A
3	O	O	S	G
4	E	E	E	D
5	T	S	S	I
6	B	A	N	O
7	O	C	C	R
8	R	U	R	R
9	R	A	U	A
10	P	N	H	E
11	A	H	E	S
12	N	M	M	E
13	V	A	C	M
14	N	D	O	C
15	U	N	T	G
16	C	I	S	M
17	H	B	T	I
18	E	G	L	I
19	I	K	R	E
20	V	A	F	D
21	D	E	T	E
22	T	E	N	O
23	N	O	C	A
24	O	E	E	N
25	N	T	D	S

We know from the given method of encryption that during the encryption process the columns of the plaintext were both permuted and shifted according to some codeword. One approach for solving is to shift the columns by varying amounts and then look for words permuted across the rows. For example we could write out the above grid on paper, then cut the columns into strips and try to permute and shift the columns until words emerge across the rows.

Another method for solving is to look for words that we think might be in the plaintext. Since this is a transposition cipher then the plaintext letters are just mixed up in the ciphertext. Given the backstory we might find the words jewels, explosive device, target, etc. Since there are no j's or x's in the ciphertext we know the words "jewels" or "explosive" don't occur in the plaintext. However there are two v's in the ciphertext so maybe the word "device" was in the plaintext. Let's try to line up the columns to create the word "device" and see if that produces a combination that gives other words.

If "device" was in the plaintext then during the encryption process that word was written across the grid as shown below.

D	E	V	I
C	E		

The "D" may not have started in the first column, but wherever the word started, the D and C are in the same column in consecutive rows and the next column has two consecutive "E's". The only column with "DC" consecutive is column 3 where the "D" is on the bottom row and the "C" is on the top row (which means in the plaintext those would have been consecutive before the rows were shifted). The only column with consecutive "E"s is column 2. The only column with a "V" is column 1, which leaves column 4 to contain the I. There are several I's in column 4 so we just have to try to line up the columns to see which way (if any) make words.

1	2	3	4
T	B	C	I
M	D	W	A
O	O	S	G
E	E	E	D
T	S	S	I
B	A	N	O
O	C	C	R
R	U	R	R
R	A	U	A
P	N	H	E
A	H	E	S
N	M	M	E
V	A	C	M
N	D	O	C
U	N	T	G
C	I	S	M
H	B	T	I
E	G	L	I

I	K	R	E
V	A	F	D
D	E	T	E
T	E	N	O
N	O	C	A
O	E	E	N
N	T	D	S

So now we try to line up the columns to make the word “device” and see if any other words emerge. We’ll start with the “top” choice in each column (meaning the possibility in the highest row).

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

We know the first two columns must be correct, but this doesn’t appear to create the plaintext

Keep trying more shifts until we find the one that works, or eliminates all possibilities. After trying a few this one seems to work:

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

We can see plaintext here, but we aren't sure we have the right starting point. We'll write out the plaintext and see if we can figure out where to start:

Plaintext: device now our secret has been discovered must change communication methods meet at old barn on first bring package and

It seems clear that the word "device" and probably "now" come at the end. The plaintext must have been:

Our secret has been discovered must change communication methods meet at old barn on first bring package and device now.