D-DAY PIGEON CIPHER SOLUTION

Assumptions:

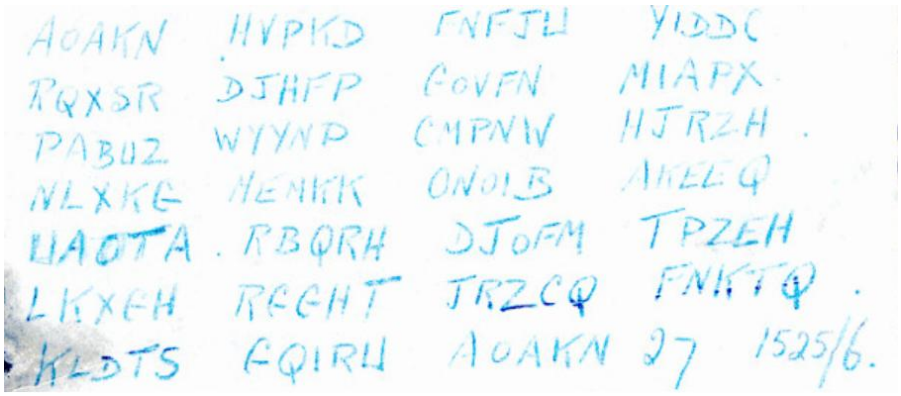
The ciphers would be generated by agents in the field, so the method had to be simple, paper and pencil, no machines or hardware aids, either a substitution type cipher or a random one time pad. According to Ref.2 (p.149), by 1921 most European nations were using one time pads OTP.

Observations:

- 5 letter blocks in capitals
- 27blocks=135characters
- block_1=block_27 which is unusual
- Check sum for number blocks after message=27
- Numbers 1525/6 could refer to a code book page
- **Printed code in article has errors (blocks 3,17,26), corrections made**

Let's assume that a mono-alphabetic substitution cipher is used. We first analyze the frequency distribution using ScicosLab:

```
1  //D-Day Pigeon Cipher
2  //Decrypted by J.Clark Toronto, Ontario
3  //Nov24th-2012
4  msg=['AOAKN';'HVPKD';'FNFJU';'YIDDC';
       'RQXSR';'DJHFP';'GOVFN';'MIAPX';
       'PABUZ';'WYYNP';'CMPNW';'HJRZH';
       'NLXKG';'MEMKK';'ONOIB';'AKEEQ';
       'UAOTA';'RBQRH';'DJOFM';'TPZEH';
       'LKXGH';'RGGHT';'JRZCQ';'FNKTQ';
       'KLDTS';'GQIRU';'AOAKN']
5  msg=msg'
6  msg1=strcat(msg);
7  numA=0;
8   a=strindex(msg1,'A');
9   A=size(a);
10  numA=A(1,2)
11 numB=0;
12  b=strindex(msg1,'B');
13  B=size(b);
14  numB=B(1,2)
```



Original Code Ref.1

Frequency Distribution From ScicosLab%:

A(9)	B(3)	C(3)	D(6)	E(4)	F(6)	G(6)	H(8)	I(4)	J(5)	K(10)	L(3)	M(5)	N(9)
6.7	2.2	2.2	4.4	3.0	4.4	4.4	5.9	3.0	3.7	7.4	2.2	3.7	6.7
O(7)	P(7)	Q(6)	R(8)	S(2)	T(5)	U(4)	V(2)	W(2)	X(4)	Y(3)	Z(4)		
5.2	5.2	4.4	5.9	1.5	3.7	3.0	1.5	1.5	3.0	2.2	3.0		

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

General Frequency Distribution English Language 1939 (Ref.1 p.276) %:

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

Note that the Frequency Distribution for the English Language is averaged over many thousands of characters, whereas our message is only 135 characters, so the relative frequencies are only rough values for this message. The frequency for E=12.5% and for Z is 0.09%, giving a range of 12.5/.09=139:1. Note for our distribution, it appears that there is not that huge a range between K(10) and S(2)=5:1. This leads me to suspect an OTP. Assume for a minute that there is a substitution. The first block is AOAKN, we can try to make sense of this if K,A,N are either E,T,A. No combination seems to give a possible word.

K=E, A=T, N=A---→T ? T E A
K=E,A=N, N=T----→A ? A E T

If an OTP is used, perhaps the cipher could be decoded if more information about the code books supplied to agents could be obtained. Perhaps the numbers 1525/6 refer to the OTP used.

I bet if anyone could decode this, the Professor Bauer Ref.2 would be able to!!

References

1. “Wanted for one last mission....”, The Telegraph, http://www.telegraph.co.uk/news/uknews/defence/9697929/Wanted-for-one-last-mission-call-for-Bletchley-Park-codebreakers-to-crack-the-D-Day-pigeon-cipher.html

2. "Decrypted Secrets Methods and Maxims of Cryptology",.F.L.Bauer, Springer Verlag, Berlin, 2000, ISBN 3-540-66871-3

J.Clark
Toronto, Ontario
[redacted]