NIHILIST SUBSTITUTION CIPHER

A REVISION OF UNIT 80 IN BOSS TECHNICAL NOTE 004

Unit 80
Nihilist substitution cipher

The *Nihilist substitution cipher* begins with an alphabet mixed by a keyword and laid into a Polybius square. The row and column labels are 1, 2, 3, 4, 5. The letters of the plaintext are converted to two-digit numbers by taking the row label followed by the column label. A second keyword is used in a manner similar to the Vigenère cipher. Its letters are also converted to numbers with the same Polybius square. Those new numbers are added to the plaintext numbers. Optionally, any sum that exceeds 100 is written without the leading 1; this does not lead to any ambiguities.

Your are probably expecting an example at this point. Let's begin with the keywords `POLYBIUS` and `KEYWORD`. If we fill the square in the least imaginative way, we have:

	1	2	3	4	5
1	P	O	L	Y	B
2	I	U	S	A	C
3	D	E	F	G	H
4	K	M	N	Q	R
5	T	V	W	X	Z

Our usual plaintext for this part of the book:

```
THIS MESSAGE WAS ENCRYPTED WITH A GRID CIPHER
```

And here are the gory details (at least some of them):

plaintext:	T H I S M E S S A G E W A S ...
plaintext numbers:	51 35 21 23 42 32 23 23 24 34 32 53 24 23 ...
keyword:	K E Y W O R D K E Y W O R D ...
keyword numbers:	41 32 14 53 12 45 31 41 32 14 53 12 45 31 ...
ciphertext:	92 67 35 76 54 77 54 64 56 48 85 65 69 54 ...

The full ciphertext:

```
92 67 35 76 54 77 54 64 56 48 85 65 69 54 73 75 39 98 26
56 82 73 63 67 74 63 80 55 75 77 35 84 37 66 42 76 64 59
```

To break a ciphertext encrypted with the Nihilist substitution cipher, our first task is to determine the period. To do so, we will try to guess the period *m*, divide the text into *m* slices or columns, and check whether there are more or less than 25 distinct numbers in each slice. If there are more, then we know that we have not guessed correctly. If there are less or equal to 25 distinct numbers in each slice, then we may have found the correct period. We should also check that there are no more than five different digits in the one's place and no more than five different digits in the ten's place in each slice (or six if the one's place of any number has a zero, indicating a carry into the ten's place). If we satisfy this criterion, then we can make check further if we wish by replacing the numbers with letters, using a different substitution key for each slice, and combining the slices to form a temporary text. Then we can graph the index of coincidence for various choices of dividing this new text with a new period, as we did in Unit 31. The peaks at multiples of the true period will be at a value like that of typical English text, but the valleys will be shallower than they were when we analyzed polyalphabetic ciphers. For an example, consider this ciphertext:

```
37 75 68 77 64 59 38 54 55 53 63 60 37 55 59 75 35 39 44 48
95 65 42 67 56 65 58 83 42 29 47 57 65 56 35 47 56 44 89 75
36 69 66 58 58 67 56 40 66 48 85 43 64 40 34 76 67 65 35 50
56 44 85 55 64 56 64 46 86 65 32 56 65 66 76 65 56 48 34 74
58 74 45 29 65 47 59 55 53 69 56 75 89 64 54 26 68 65 87 45
52 47 65 54 67 53 32 26 37 48 77 67 75 37 38 66 65 57 54 60
55 47 55 54 42 36 65 78 76 53 65 28 38 77 87 43 42 60 66 64
77 83 42 29 58 68 89 64 42 48 64 77 87 47 66 29 65 78 69 46
44 60 34 47 86 56 66 58 34 54 89 57 64 30 68 65 89 64 42 60
55 54 87 47 54 36 34
```

Let's suppose that we guess that the period is 7. We divide the ciphertext into seven slices/columns:

```
37    75    68    77    64    59    38
54    55    53    63    60    37    55
59    75    35    39    44    48    95
65    42    67    56    65    58    83
42    29    47    57    65    56    35
47    56    44    89    75    36    69
66    58    58    67    56    40    66
48    85    43    64    40    34    76
67    65    35    50    56    44    85
55    64    56    64    46    86    65
32    56    65    66    76    65    56
48    34    74    58    74    45    29
65    47    59    55    53    69    56
75    89    64    54    26    68    65
87    45    52    47    65    54    67
53    32    26    37    48    77    67
75    37    38    66    65    57    54
60    55    47    55    54    42    36
65    78    76    53    65    28    38
77    87    43    42    60    66    64
77    83    42    29    58    68    89
64    42    48    64    77    87    47
```

```
66    29    65    78    69    46    44
60    34    47    86    56    66    58
34    54    89    57    64    30    68
65    89    64    42    60    55    54
87    47    54    36    34
```

Take a look at the first column. It has nine different digits in the one's place; therefore, 7 is the wrong period. Suppose we try period 6:

```
37    75    68    77    64    59
38    54    55    53    63    60
37    55    59    75    35    39
44    48    95    65    42    67
56    65    58    83    42    29
47    57    65    56    35    47
56    44    89    75    36    69
66    58    58    67    56    40
66    48    85    43    64    40
34    76    67    65    35    50
56    44    85    55    64    56
64    46    86    65    32    56
65    66    76    65    56    48
34    74    58    74    45    29
65    47    59    55    53    69
56    75    89    64    54    26
68    65    87    45    52    47
65    54    67    53    32    26
37    48    77    67    75    37
38    66    65    57    54    60
55    47    55    54    42    36
65    78    76    53    65    28
38    77    87    43    42    60
66    64    77    83    42    29
58    68    89    64    42    48
64    77    87    47    66    29
65    78    69    46    44    60
34    47    86    56    66    58
34    54    89    57    64    30
68    65    89    64    42    60
55    54    87    47    54    36
34
```

Now if we look at each column, there are five or fewer distinct digits in the one's place and six or fewer in the ten's place (to allow for possible carry digits). For example, the first column has 4, 5, 6, 7, 8 in the one's place and 3, 4, 5, 6 in the ten's place. We can be confident with a ciphertext of this length that this criterion gives us the correct period.

The remainder of the cryptanalysis resembles the two-stage attack we built against the quagmire 1 cipher: we find a subtrahend (something to subtract) for each slice/column, subtract it, put the pieces

back together, and solve the remaining monoalphabetic substitution. Each subtrahend must leave a column with only the digits 1, 2, 3, 4, 5. For our example, the only possibility for the first column is 23. For the other columns, 33, 44, 32, 21, and 15. After subtracting, we have

```
14    42    24    45    43    44
15    21    11    21    42    45
14    22    15    43    14    24
21    15    51    33    21    52
33    32    14    51    21    14
24    24    21    24    14    32
33    11    45    43    15    54
43    25    14    35    35    25
43    15    41    11    43    25
11    43    23    33    14    35
33    11    41    23    43    41
41    13    42    33    11    41
42    33    32    33    35    33
11    41    14    42    24    14
42    14    15    23    32    54
33    42    45    32    33    11
45    32    43    13    31    32
42    21    23    21    11    11
14    15    33    35    54    22
15    33    21    25    33    45
32    14    11    22    21    21
42    45    32    21    44    13
15    44    43    11    21    45
43    31    33    51    21    14
35    35    45    32    21    33
41    44    43    15    45    14
42    45    25    14    23    45
11    14    42    24    45    43
11    21    45    25    43    15
45    32    45    32    21    45
32    21    43    15    33    21
11
```

We next replace each number with its corresponding letter in a Polybius square with an unmixed alphabet (without `J`, of course). We have:

```
DRIUSTEFAFRUDGESDIFEVNFWNMDVFDIIFIDMNAUSEYSKDPPKSEQASKASHND
PNAQHSQQCRNAQRNMNPNAQDRIDRDEHMYNRUMNAUMSCLMRFHFAADENPYGENFK
NUMDAGFFRUMFTCETSAFUSLNVFDPPUMFNQTSEUDRUKDHUADRIUSAFUKSEUMU
MFUMFSENFA
```

If we apply the hill-climbing attack from Unit 28 to this text, we get the plaintext

```
ANDTOPRESENTABROADERVIEWIHAVEADDEDAHISTORYOFALLFORMSOFSOCIA
LISMCOMMUNISMNIHILISMANDANARCHYINTHISTHOUGHNECESSARILYBRIEF
```

```
ITHASBEENTHEPURPOSETOGIVEALLTHEIMPORTANTFACTSANDTOSETFORTHT
HETHEORIES
```

(from *Anarchy and Anarchists* by Michael J. Schaack) and the substitution key `DGHIFKLMNJOPQRSTBEAUCVWXYZ`. But bear in mind that this is the *inverse* of the mixed alphabet that belongs in the Polybius square, and that `J` is not allowed. Once we invert this key, we have `SQUAREBCDFGHIKLMNOPTVWXYZ`, so the keyword is `SQUARE` and the square contains

	1	2	3	4	5
1	S	Q	U	A	R
2	E	B	C	D	F
3	G	H	I	K	L
4	M	N	O	P	T
5	V	W	X	Y	Z

From this square and the subtrahends above, we find that the other keyword is `CIPHER`.

Reading and references

Wikipedia, en.wikipedia.org/wiki/Nihilist_cipher

American Cryptogram Association, www.cryptogram.org/downloads/aca.info/ciphers/NihilistSubstitution.pdf

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, revised and updated 1996, pages 619-621.

Helen Fouché Gaines, *Cryptanalysis: a study of ciphers and their solution*, New York: Dover, 1956; previously titled *Elementary Cryptanalysis* and published by American Photographic in 1939; archive.org/details/cryptanalysis00gain; pages 164-168.

Merle E. Ohaver, "Solving Cipher Secrets," *Flynn's*, March 28 and June 27, 1925, toebes.com/Flynns/Flynns-19250328.htm and toebes.com/Flynns/Flynns-19250627.htm

Programming tasks

1. Implement an encryptor. Remember that there are many ways to mix an alphabet and to lay it into a square.
2. Implement a decryptor. Remember that there are many ways to mix an alphabet and to lay it into a square.
3. Implement a dictionary attack on the Nihilist substitution cipher.
4. Modify your two-stage attack on the quagmire 1 cipher to make an attack on the Nihilist substitution cipher, as explained in the text.

Exercises

1. Encipher this text with keywords `RUSSIAN` (in the square) and `FREEDOM`. Use the least imaginative way of setting up the Polybius square.

   > O God, how easy it is for a king to kill his people by thousands, but we cannot rid ourselves of one crowned man in Europe! What is there of awful majesty in these men which makes the hand unsteady, the dagger treacherous, the pistol-hot harmless? Are they not men of like passions with ourselves, vulnerable to the same diseases, of flesh and blood not different from our own?
>
> (from *Vera, or The Nihilists* by Oscar Wilde)

2. Decipher this text with keywords `ANARCHY` (in the square) and `NIHILISM`. Use the least imaginative way of setting up the Polybius square.

```
44 77 59 47 45 66 78 57 36 53 56 83 47 76 89 76 44 83
38 63 58 67 65 79 53 44 26 76 66 47 55 87 36 76 60 43
79 56 67 80 53 53 56 83 45 77 67 67 37 57 39 45 58 44
89 80 44 67 39 76 66 85 55 79 34 56 60 45 45 53 68 58
34 53 50 43 78 77 85 88 44 86 68 64 79 47 97 50 53 67
47 85 45 76 68 47 43 43 46 56 57 85 76 80 27 73 60 47
58 45 88 67 24 43 57 66 75 77 55 66 23 64 27 76 79 44
76 49 27 73 49 43 78 46 99 46 25 73 40 45 85 76 88 67
23 64 68 43 78 85 85 48 57 47 26 67 66 66 78 67 53 44
56 57 47 83 66 69 36 76 26 44 57 77 59 59 65 47 56 66
58 73 69 67 57 64 57 66 58 55 75 59 35 77 56 77 49 56
58 46 63 76 39 73 59 47 95 70 23 44 49 64 56 56 57 80
33 64 27 45 85 76 88 67 23 67 26 76 79 73 97 67 66 65
27 56 87 77 59 67 56 43 27 55 49 56 55 69 56 73 48 44
58 85 89 50 23 77 56 77 49 56 57 70 36 67 37 56 47 76
85 60 57 47 39 76 75 46 76 59 57 53 30 43 57 66 55 48
43 56 59 83 69 76 89 50 63 76 57 66 58 55 75 59 35 43
40 77 58 45 55 88 27 64 49 56 66 47 55 69 37 76 66 76
76 56 58 80 36 55 30 64 69 43 56 58 56 73 59 56 48 45
68 80 36 55 50 53 65 73 78 58 44 44 26 74 68 43 58 59
45 44 56 85 46 73 56 69 33 77 56 67 55 76 68 69 37
```

3. Break this ciphertext with a dictionary attack. Both keywords end in `-IST`.

```
46  86  52  67  74  45  74  42  36  65  45  66  36  45
57  35 103  54  56  55  68  73  52  64  48  38 106  52
64  35  74  85  55  74  44  46  86  52  64  56  38  73
43  56  64  54  94  42  64  47  74  74  42  64  54  45
74  42  64  46  57  83  34  37  74  47  66  63  47  45
35  64  63  47  35  65  64  44  36  45  37  97  72  37
54  44  94  32  43  46  54  75  55  53  64  46  64  44
56  54  44  97  55  34  74  45  83  43  36  65  48  75
55  53  68  54  84  33  67  54  46  86  52  53  65  56
```

```
67  42  44  57  54  74  64  53  36  44  66  36  37  77
46  86  52  35  38  37  74  43  43  37  64  74  64  53
37  58  73  63  55  35  55  66  66  53  37  38  93  33
44  46  55  64  66  35  54  48  75  33  36  45  45  64
34  43  37  46  83  52  64  46  44  97  52  37  77  75
73  44  56  54  37  65  55  34  46  57  83  66  36  65
48  84  33  67  64  37  74  33  67  46  35  84  34  34
38  35  94  75  66  74  44  75  52  36  66  37  97  44
54  68  35  93  63  36  46  44  63  52  44  35  36  73
52  45  77  44 104  35  44  55  35  97  44  73  65  37
75  52  53  65  35 103  54  56  46  35  93  35  57  54
45  64  62  53  37  36  96  72  36  44  65  75  35  64
36  54  74  35  63  35  65  85  44  56  54  64  74  33
34  65  37  84  44  53  68  44 104  52  64  46  35 103
44  36  65  48 106  33  73  68  64  64  44  56  54  68
66  63  47  44  75  83  66  53  64  74  65  55  63  35
68  83  42  64  68  74  74  43  43  37  65  74  33  35
44  54  75  75  45  57  37  94  42  44  74  45 103  35
37  75  44  75  55  34  74  68  65  33  73  65  46  97
75  63  54  65  75  55  53  68  54  73  53  34  74  65
77  54  67  54  37  75  35  47  34  37  94  44  36  56
54  84  66  34  64  44  75  35  64  48  45  86  35  37
38  47  83  54  37  37  48  84  33  67  77  35 103  44
34  48  35  75  55  53  45  37  93  52  76  35  74 104
42  37  38  57  66  32  53  35  65  83  32  53  68  77
85  66  53  37  46  66  46  33  37  65  75  35  55  54
46  86  35  45  77  35 103  73  43  38  38  76  52  36
47  38  83  44  34  45  66  83  35  57  68  74  74  43
43  37  65  84  36  73  54  65  75  36  76  44  65  66
43  56  35  68  75  44  43  64  54
```

4. Break this ciphertext with the two-stage attack.

```
34 80 57 87 47 63 47 25 88 56 78 76 44 58 24 60 65 57
45 34 86 44 58 95 75 63 44 86 25 67 57 57 45 36 57 43
77 86 87 47 34 89 27 56 65 77 66 33 50 24 66 86 58 43
65 50 36 77 65 77 64 65 56 36 60 64 64 77 57 67 55 66
78 75 63 54 69 44 88 64 65 67 36 57 47 67 55 67 63 76
67 47 89 74 75 75 66 66 27 90 68 74 67 35 59 25 88 86
65 44 54 69 66 68 55 75 45 33 67 56 76 65 86 55 35 48
47 89 74 56 73 67 47 53 60 86 56 76 37 60 44 96 56 65
66 56 79 43 58 75 64 73 37 47 56 67 78 87 43 44 59 56
88 65 78 46 66 50 55 58 87 54 47 34 79 43 89 74 56 76
53 48 27 57 75 56 75 37 46 34 79 77 87 63 37 78 25 97
74 58 84 53 48 56 76 56 55 53 37 49 25 57 65 87 45 37
47 24 67 57 75 56 44 69 64 76 56 87 63 35 47 55 77 78
67 45 34 48 46 99 77 65 55 37 47 44 80 68 75 67 66 66
25 77 78 87 45 34 48 55 89 86 58 43 53 80 33 67 78 75
76 76 50 24 68 58 75 75 66 48 24 60 88 86 66 76 78 56
```

57 75 94 64 57 60 23 60 55 78 47 66 50 24 77 56 87 86
53 57 63 58 56 78 46 35 57 63 60 55 56 46 37 47 53 57
56 87 45 57 49 25 59 87 58 64 43 76 24 60 94 56 77 63
50 47 89 74 56 45 75 67 55 89 75 78 57 37 47 26 58 55
58 43 65 50 36 77 56 87 86 54 79 44 88 65 84 66 44 67
47 80 65 55 44 44 79 44 96 56 95 63 37 78 25 77 78 87
45 34 48 55 89 77 75 45 65 67 47 89 74 56 53 37 56 25
80 87 58 77 65 59 43 67 55 65 56 66 48 24 60 54 87 63
35 46 34 69 87 86 84 53 67 36 76 75 87 44 35 69 34 89
56 86 53 67 59 43 60 54 75 76 54 78 47 60 95 54 47 34
79 43 58 54 75 44 65 79 56 77 64 56 57 54 86 25 80 87
58 76 53 48 53 90 66 77 64 46 67 43 67 94 56 46 34 57
64 80 88 84 47 57 79 43 58 55 56 56 37 47 26 88 58 54
76 53 48 36 67 86 56 53 44 49 25 77 78 67 47 67 47 56
68 88 87 53 37 47 25 58 86 84 45 46 67 34 79 77 97 77
63 50 47 89 74 56 44 35 76 27 57 87 86 53 44 49 25 89
58 64 45 36 80 24 77 78 68 76 53 48 53 57 58 68 44 35
78 55 60 54 87 63 35 67 47 96 56 86 76 54 60 34 89 75
58 67 45 89 56 76 56 64 54 57 89 26 58 87 56 56 66 67
63 58 86 95 63 37 87 25 57 56 95 47 34 68 44 80 68 88
67 36 48 24 66 97 57 64 34 48 36 89 75 58 67