Normor Revisited
by THE RAT

In the SO09 issue of *The Cryptogram* I discussed a diagnostic tool I devised called the Normor Test, short for Normal Order. It measures how closely a ciphertext's letter frequency order matches a normal frequency order. That article discussed its value when facing an unknown primarily as a way to distinguish between the Twosquare and Foursquare types. Further research shows that it can be quite valuable for solvers of various cipher types, sometimes in surprising ways. Because this test is very easy to use for anyone, including paper-and-pencil solvers, I wanted to share my results.

The test: The test is performed by counting the frequency of each letter of the ciphertext and arranging the letters in frequency order. For letters with the same frequency, arrange them in alphabetical order. Then for each letter, measure the distance between its position in the resulting 26-letter series and the position of that letter in the normal order, which for ACA English plaintext (as measured by my 3700 solutions) is ETAOINSRHLDUCMGFYPWBVKXJZQ. It doesn't matter whether the ciphertext letter appears before or after its normal position, just count the distance between those two positions for each letter, including those that do not appear in the ciphertext, and keep a running total. That total is its Normor score.

The Rule

Ciphers that tend to encipher high-frequency letters in whole or part with themselves or other high-frequency letters have low scores. Those that do not, have high scores.

The research: The results of the research can best be understood and interpreted by remembering the above rule. Once that principle is understood, one is better able to consider how the mechanics of a particular cipher type or key route results in a high or low score.

I found that Normor scores were affected by myriad factors, including plaintext length, period, key type, key length, seriation length, keyword and plaintext content. Most of the preceding factors, though, did not influence the scores enough to make the test useful for distinguishing those factors. For example, it is not possible to identify the length of the key by examining the Normor score. In general, longer ciphertexts, keys with many high-frequency letters, and longer keys tended to produce ciphertext that more strongly followed the predicted behavior for that cipher type and key route, making the test more reliable for longer texts, which is to be expected for any statistical measure. Because these differences generally were not pronounced, I do not discuss them further in this article.

The two most important factors influencing the Normor score, I found, were the cipher type and for polybius types, the route of the key(s). This finding means that Normor can be used not only to assist in identifying the cipher types of unknowns, but it can also be helpful in finding the most likely route(s) used in some polybius-square types. So far as I am aware, this is the first statistical test found to be useful in identifying key routes.

Cipher types: Most types other than transposition types produced scores averaging around 190, with few examples scoring above 250 or below 150. Certain types, however, had unusually high

or low scores. The test may thus be useful to identify those types. Most prominent are the transposition types. Since their frequency counts are the same as the underlying plaintext, their scores are the same, and generally fall in the range 60 - 99. In my test of about 3700 plaintexts, fewer than 0.5% scored over 150. For longer texts only 1% scored over 100. Nulls and Baconians that use regular words seem to score similarly, although I only tested a few of those. Other types that had unusually low Normor scores were the Key Phrase and the Trisquare. If you consider the principle in the text box above, and the mechanics of the ciphers, you will understand why. Types that tend to produce higher scores include the Aristocrats, Patristocrats, Gromark, and Phillips. No doubt the ACA rule for the first two that no letter can stand for itself (a rule not followed everywhere for cryptograms) contributes to this fact. Again, consideration of the mechanics will bring understanding as to why these types score high. See the chart at the end of the article for the complete list of types tested and how they scored.

Polybius routes: What I found to be most interesting and useful, however, is the sensitivity of the test to the keying route(s) used for polybius square based ciphers. Although the different routes had distinct scoring profiles within a type, these were not consistent across the different polybius types. For example, for Bifids, the lowest scoring routes were those where the key word or phrase is clustered close to the main diagonal, i.e. the line from the upper left corner to the lower right corner, while for Foursquares, it was those with the key on the first row(s) of the keysquares, and for Twosquares, the lowest scores were produced when the keys were on the same rows in the two squares.

When you consider the way each cipher works, these findings make sense. The keys, being plaintext themselves, tend to have high-frequency letters, especially vowels, and therefore when keys are in a route that places them in a position to encipher other keyletters, the score will be lower than when they are not. This is why the lowest-scoring route for the Bifid is a diagonal route beginning in the upper left or lower right corner, while the highest-scoring route is a diagonal beginning at the upper right or lower left corner. Bifids tend to proliferate ciphertext letters that are reflected across the main diagonal from the plaintext letters, so if the key letters are all in the upper left corner, they often are enciphered by other key letters. Conversely, if they are in the upper right corner with a diagonal route, ciphertext will often be dominated by the tail end of the compressed alphabet, i.e., VWXYZ which ends in the lower left. Even when using a horizontal route, it made a difference whether I started in the upper left or upper right, at least if the key was longer than five letters. After determining that longer keys did not greatly influence the results I used 7-letter keys for my tests. Thus the 6^{th} and 7^{th} letters of the horizontal route would fall in the upper left corner if you start there, but in the upper right if you start there. For alternating rows, the opposite is true. This is the dynamic you must keep in mind when interpreting results. Conjugated Matrix Bifids had their lowest score when both squares used inner spiral routes. Most row/column route combinations produced around 10% of the scores below 150, while diagonal routes beginning in the upper left and lower right corners, even though on the main diagonal, produced much higher scores, none below 150 and a third over 250, when the two routes began at diagonally opposite corners. This is because the key letters, when reflected across the main diagonal land on the tail end of the other square's key alphabet, thus producing many VWXYZ letters in the ciphertext.

For Foursquares the key letters, located in squares 2 and 3, do not encipher other key letters. Instead they encipher letters in unkeyed squares 1 and 4. Thus, since the highest frequency row or column in the squares 1 and 4 is the top row, ABCDE, and the lowest is the last, VWXYZ, the various routes placing the keys mostly on the top row are the lowest scoring and conversely if the keyword is mostly on the bottom row, the score is likely to be very high. Another interesting route for the Foursquare is the counterclockwise spiral beginning in the center and ending in the lower left corner. It begins by placing the key on the sequence of squares mirroring the plaintext letters "NSTOI...." Because of their high frequency that route scores low, as well. I did not take Foursquare ciphertexts and separate the even-numbered letters from the odd to perform separate tests on them, but I believe one would see a significant statistical difference in the scores where square 2 uses a low-scoring route and square 3 uses a high-scoring one or vice versa. The columns in squares 1 and 4 are more balanced than the rows in frequency. The one with the highest frequency letters is the fourth one DIOTY, but since none of the ACA routes tend to group the key letters in column four, the Normor score on Foursquares is influenced almost entirely by the extent to which the keys fall on row 1 or row 5, not by the columnar location.

For Twosquares, if one key was on upper rows and the other on the lower rows, high scores were produced, but if the keys were on the same rows the score was low. Columnar routes tended to spread out high-frequency letters over all the rows and thus resulted in relatively high scores for the Twosquare. For Playfairs, the route made little difference, although routes that placed keys, especially longer keys, on two consecutive columns or rows were somewhat lower scoring. Seriated Playfairs scored about the same as Playfairs, although the diagonal routes tended to have slightly lower scores for that type. Since Phillips do not encipher using letters on the same row or column, they tend to have high scores. The routes probably make little difference there and were not tested separately. Other results can be seen in the following chart. I have also created a statistical test page on my website: www.ackgame.com/crypto.htm. You can paste the ciphertext there and click the test button to get the Normor score.

How to use the chart: The first column is the cipher type, or type and route. The second column is the percent of tested ciphertexts that scored below 150 on the Normor test. The last column is the percent scoring over 250. Note that percentages are rounded, so that a zero score does not necessarily mean that there were no scores in that category, only that, if any, they were less than half a percent. If you have a ciphertext that scores 210, for example, it is about equally likely to be an Autokey, Bazeries, or a Gromark, but if the score is 255, it is at least twice as likely to be a Gromark as an Autokey, since 12% of the former score over 250 while only 6% of the latter do, and 12 times more likely than a Bazeries with only 1%. Similarly, if you know you have a Foursquare and the Normor score is 255, look for key routes that put most of the key letters on the bottom rows of the two keysquares, or at least not on horizontal routes beginning on the top. Where a range of scores is shown, the results varied depending on key type, length, route, etc., but not enough to warrant a separate entry.

Cipher Type	Average score	% below 150	% above 250
Plaintext & Tramps	83	100	0
Aristo- & Patristocrats	222 - 225	1	13 - 17
Autokey (Vig/Beau/Var)	209	2	6
Bazeries	210	0	1
Fractionated Morse	199	4	3
Gromark	217	1	12
Key Phrase	130	86	0
Phillips	221	0	12
Playfair	188	8 - 13	1
Ragbaby	198	4	2
Seriated Play. (most routes)	187 - 196	6 - 10	1 - 3
Seriated Playfair (diag)	182	14	1
Trisquare	169	42	0
Vig/Beau/Variant	211	3	9
Bifid (by rows or cols)	169	25	0
Bifid (Diag UL / LR)	143 - 155	59 - 64	0
Bifid (Diag UR / LL)	171 - 177	17	1
Bifid (outer spirals UL, LR)	173	21	1
Bifid (spirals all others)	155 - 163	33 - 47	0
CM Bifid (rows / col. UL)	182 - 187	9 - 11	0 - 1
CM Bifid (diag. UL / LR)	238 - 241	0	32 - 36
CM Bifid (spiral "nstoi..")	175	17	0
CM Bifid (other routes)	188 - 206	2 - 8	1 - 5
Twosquare (same rows)	152	50	0
Twosquare (diff rows)	221	1	16
Twosquare (1 or 2 cols)	160 - 163	35 - 37	0
Twosquare (diags - mirror)	159	40	0
Twosquare (di. non-mirror)	190	13	4
Twosquare (spirals - non)	191	9	2
Foursq. (top rows both)	166	26	0
Foursq. (bottom rows both)	241	0	45
Foursq. (spiral "nstoi..")	173	16	0
Foursq. (all others)	184 - 211	1 - 10	0 - 6