CHAPTER 4

# MONOALPHABETIC UNILATERAL SUBSTITUTION SYSTEMS USING MIXED CIPHER ALPHABETS

## Section I
## Generation and Use of Mixed Cipher Alphabets

### 4-1. Mixed Cipher Alphabets

Mixed cipher alphabets differ from standard alphabets in that one or both sequences are mixed sequences. A mixed sequence is any sequence not in normal alphabetical order. The two main types of mixed sequences are systematically mixed and random mixed sequences.

a. Systematically mixed sequences are produced by an orderly process based on easily remembered keywords, phrases, or simple rules. There are a number of mixed sequence types, which will be explained in this section. Their advantage is that the keys can be easily memorized and reconstructed for use when needed. Their disadvantage is that the orderliness in construction can be used by the opposing cryptanalyst to aid in their recovery.

b. Random mixed sequences are not based on any orderly generation process. They can be produced by various means ranging from pulling the 26 letters out of a hat to complex machine generation. Their advantage is that their structure offers no help to the opposing cryptanalyst. Their disadvantage is that the keys cannot be memorized easily or produced from simple directions as systematically mixed sequences can. They must be printed out in full and supplied to every user.

## 4-2. Keyword Mixed Sequences

One of the simplest types of systematic sequences is the keyword mixed sequence. The sequence begins with the keyword, which may be a word or a phrase. Any letters repeated in the keyword are used only once, dropping the repeating letters. After the keyword, the rest of the letters are listed in alphabetic order, omitting those already used.

Keyword— CRYPTOGRAPHIC

Repeated letters dropped: CRYPTOGAHI

Remaining letters added in normal order:

CRYPTOGAHIBDEFJKLMNQSUVWXZ

Keyword— MILITARY INTELLIGENCE

Repeated letters dropped: MILTARYNEGC

Remaining letters added in normal order:

MILTARYNEGCBDFHJKOPQSUVWXZ

## 4-3. Transposition Mixed Sequences

Transposition mixed sequences are produced by writing a letter sequence into a matrix and extracting it from the matrix by a different route. The most common types are called simple columnar, numerically keyed columnar, and route transposition sequences.

a. Simple columnar transposition is usually based on a keyword mixed sequence. The keyword determines the width of the matrix that is used. The keyword is written as the first row of a matrix and the rest of the sequence is written beneath it, taking as many rows as necessary. The transposition mixed sequence is then produced by extracting the columns of the matrix from left to right.

Keyword— ARTILLERY

Keyword mixed sequence in matrix:

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

Resulting sequence:

ABKURCMVTDNWIFOXLGPZEHQYJS

Keyword– MORTAR

Keyword mixed sequence in matrix:

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

Resulting sequence:

MBGLUZOCHNVRDIPWTEJQXAFKSY

b. The numerically keyed columnar transposition mixed sequence differs from the simple columnar only in the way it is extracted from the matrix. Instead of extracting the columns left to right, the order of the columns is determined by a numerical key based on the keyword. After constructing the matrix, the letters in the keyword are numbered alphabetically. The columns are then extracted according to the resulting numerical key.

Keyword– CALIFORNIA

| 2 | 1 | 5 | 4 | 3 | 7 | 8 | 6 |
|---|---|---|---|---|---|---|---|
| C | A | L | I | F | O | R | N |
| B | D | E | G | H | J | K | M |
| P | Q | S | T | U | V | W | X |
| Y | Z | | | | | | |

Resulting sequence:

ADQZCBPYFHUIGTLESNMXOJVRKW

Keyword– VERMONT

| 7 | 1 | 5 | 2 | 4 | 3 | 6 |
|---|---|---|---|---|---|---|
| V | E | R | M | O | N | T |
| A | B | C | D | F | G | H |
| I | J | K | L | P | Q | S |
| U | W | X | Y | Z | | |

Resulting sequence:

EBJWMDLYNGQOFPZRCKXTHSVAIU

c. Route transposition sequences are formed by any other systematic way of entering sequences into a matrix and extracting them from a matrix. They can be based on standard or keyword mixed sequences. The samples in Figure 4-1 show some of the common routes that can be used. The last two omit the letter J for the convenience of a square matrix.

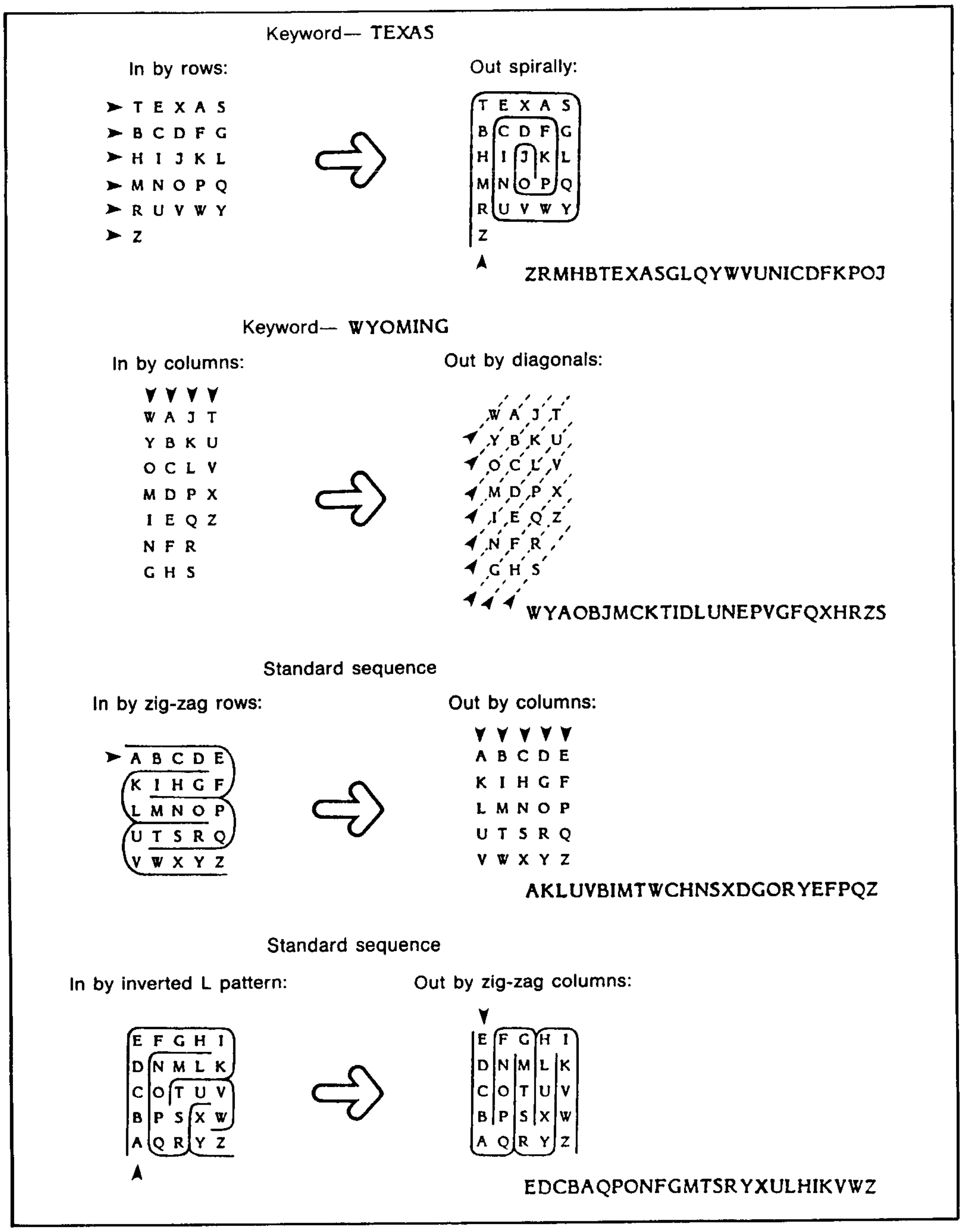



Figure 4-1. Route transposition.

## 4-4. Decimation Mixed Sequences

Decimation mixed sequences are produced from a standard or keyword mixed sequence by counting off letters at a regular interval.

a. As an example, consider decimating a standard sequence at an interval of 3. The new sequence begins with the first letter of the basic sequence, in this case, A. The second letter of the new sequence is the third letter that follows from the basic sequence, D. Every third letter is selected until the end of the basic sequence is reached.

Basic sequence:

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

Resulting decimated sequence:

A D G J M P S V Y ...

The count then continues as if the sequence were written in a circle. The next letter after Y, skipping Z and A, is B. The complete resulting sequence is shown below.

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

b. The interval should have no common factors with the length of the sequence. Since any even number has a common factor of 2 with 26, only odd numbers are selected with 26 letter sequences. Intervals with common factors are not selected, because the count will return to the starting point again before all the letters are used. The interval should also be less than half the length of the sequence, because larger numbers will just duplicate in reverse order the sequence produced by a smaller number. An interval of 23, for example would produce the same sequence as an interval of 3, but in the reverse order. For a 26 letter sequence, the only usable intervals are 3, 5, 7, 9, and 11. By counting either left to right or right to left, all the basic decimated sequences can be produced.

c. Study of this method of decimation is particularly significant, because the solution of some types of polyalphabetic ciphers can yield sequences in a decimated order instead of the original order.

d. An alternate method of decimation is occasionally encountered. In the alternate method, each letter is crossed off as it is selected and that letter is not counted again. The restrictions on intervals do not apply to this method, because the starting letter can never be reached again. This method is used less, because it is subject to mistakes in the counting process that are hard to detect and correct.

## 4-5. Types of Mixed Cipher Alphabets

As mentioned at the beginning of this section, a mixed alphabet is any alphabet that uses one or more mixed sequences. The simplest types are those which use a standard sequence in one component and a mixed sequence in the other. These are the easiest for a cryptanalyst to reconstruct. Next in order of difficulty are those in which the same mixed sequence is used in the plain and cipher components. Most difficult are those in which two different mixed sequences are used. The next section shows how to recover each of these types of alphabets.

# Section II
# Recovery of Mixed Cipher Alphabets

## 4-6. Alphabet and Plaintext Recovery

Although this manual separates the techniques of alphabet recovery from plaintext recovery, the two processes will usually occur simultaneously, each supporting the other. When an orderly structure is found in an alphabet as individual letters are recovered, the orderly structure often helps make more plaintext recoveries. The techniques explained in this section will be used in the next section.

a. You usually begin reconstruction by recording recoveries in the form of an enciphering alphabet. An enciphering alphabet is one in which the plaintext component is arranged in A through Z order. Ciphertext letters are written in the cipher component paired with their plaintext equivalents in the plain component. The plaintext can be either the top or bottom letters, but whichever you select, you should follow it consistently in the alphabet as well as the cryptogram. Inconsistency leads to errors. In this manual, plaintext is placed above ciphertext.

b. A deciphering alphabet is one in which the ciphertext is written in A through Z order. Rearranging the alphabet into deciphering order is sometimes helpful in alphabet recovery.

c. Whenever systematically mixed alphabets are used, you should attempt to recover the systems and keys in use. The same sequences are often reused, either at different alignments of the same alphabet or in combination with other sequences. The solution can be reached much quicker when you recognize and take advantage of previous recoveries.

## 4-7. Reconstruction of Alphabets With One Standard Sequence

Whenever one of the two sequences is a standard sequence, recovery of the system used to produce the other sequence is made much easier.

a. The easiest type to recognize is the keyword mixed sequence. Any keyword mixed sequence has two parts—the keyword and the alphabetic progression. If you find that recovered letters are falling in alphabetic progression consistently in a portion of the sequence, it is probably a keyword mixed sequence. In this case, you can narrow down the possibilities of unrecovered letters. Consider the following partially recovered alphabet.

| p: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| c: | S | | | | Z | | | | V | | | | | T | H | | | D | F | G | I | | | | | |

(1) The letters DFGI appear to be part of the alphabet section of the cipher sequence. The alphabetic progression continues at the left with the letters S and Z. All the other recovered letters appear to be part of the keyword. Between the H and the D there is room for only two of the letters at the beginning of the alphabet—A, B, and C. At least one of these must be in the keyword, leaving the other two as probable equivalents of plaintext P and Q. Similarly, there is space for only three letters between S and Z. T and V already appear, so the spaces must be filled by three of the four letters, U, W, X, and Y. Given these limitations, recovery of more plaintext is likely. Continuing the example, consider that plaintext C, F, L, P, W, and Y are recovered next.

| p: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| c: | S | | X | | Z | L | | | V | | | O | | T | H | B | | D | F | G | I | | K | | P | |

(2) These recoveries enable several more probable letters to be placed by alphabetical progression.

| p: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| c: | S | | X | Y | Z | L | | | V | | | O | | T | H | B | C | D | F | G | I | J | K | | P | |

(3) At this point, we can see that A and E must be in the keyword, because there is no room for them in the alphabetic progression. U or W must be in the keyword, because there is only room for one of them between S and X, and V is already placed. Similarly, M or N and Q or R must be in the keyword. Q is unlikely, even though U is available to pair with it. Placing Q and U anywhere in the blanks in the keyword suggests nothing further. R must be in the keyword, then.

(4) The letter after L in the keyword must certainly be a vowel or the keyword would be unpronounceable, and that vowel represents plaintext G. With the possibilities narrowed down this far, you might be able to spot the keyword

without referring back to the cryptogram that produced the partially recovered alphabet. The complete alphabet looks like this.

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| p: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| c: | S | U | X | Y | Z | L | E | A | V | N | W | O | R | T | H | B | C | D | F | G | I | J | K | M | P | Q |

b. Recovery of decimated sequences is a straightforward process of trying out intervals. Just as a decimated sequence is produced by counting at a regular interval, the original sequence can be recovered by counting at a regular interval, too. A partially recovered alphabet with a suspected decimated sequence in the cipher component could look like this example.

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| p: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| c: | N | . | . | . | D | . | . | . | X | . | . | F | . | W | H | . | . | M | V | . | . | . | K | . | . | . |

(1) To determine if this is a decimated sequence, various intervals can be tried. The recovered letters suggest one obvious possibility. The letters V, W, and X all appear among the recovered letters. If they were in order in the base sequence used to generate the decimated sequence, they should reveal the interval. The interval from V to W and from W to X is -5 in each case. A trial decimation at -5, beginning with V produces the following sequence.

VWX...H.D.....N..F..KM....

(2) This sequence of letters appears to be a keyword mixed sequence. The keyword appears after the VWX and alphabetic progression resumes with the F and the KM. Once you recognize this structure, you can use it to assist in further plaintext recoveries just as in the first example shown in paragraph 4-7a. The original basic sequence used to produce the decimated sequence is shown below.

RHODEISLANBCFGJKMPQTUVWXYZ

c. Simple transposition mixed sequences often resemble decimated sequences. You will often see a regular spacing of adjacent low frequency letters, just as we saw VWX in the previous example. This is not caused by a decimation interval, but by the regular length of columns separating the letters. Recovery of the generation method of transposition mixed sequences is accomplished by rebuilding the original matrix.

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| p: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| c: | U | | F | O | $\underline{V}$ | | | P | $\underline{X}$ | | | K | | $\underline{Y}$ | I | | | R | $\underline{Z}$ | G | D | | T | | E | |

The almost regular spacing of the letters V, X, Y, and Z resembles a decimated sequence, but the interval is not constant. This almost, but not quite, regular spacing is an indication of simple columnar transposition. The letters V, X, Y, and Z are probably the bottom letters in their columns of the original matrix. W, which has not been recovered, probably occurs in the keyword, because there does not appear to be room for a column ending with W. Analysis of this type of sequence proceeds by rebuilding the columns. Placing the letters V, X, Y, and Z in sequence with their preceding letters as their columns, produces this partial result.

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
U . F O V/. . P X/. . K . Y/I . . R Z/G D . T . E .
```

| | | | |
|---|---|---|---|
| U | | . | I |
| . | . | . | . |
| F | . | K | . |
| O | P | . | R |
| V | X | Y | Z |

Now the initial reconstruction appears successful. The rows above VXYZ also show alphabetic progression developing. Q can be inserted in the next to last row with confidence. The next step is to place the rest of the letters into columns that would continue the structure in a logical way. A little trial and error will show that the columns before the V column end with T and U. The U was not the top of the V column, but the bottom of the preceding column.

```
p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: U/. F O V/. . P X/. . K Q Y/I . . R Z/G D . T/. E .
```

| | | | | | |
|---|---|---|---|---|---|
| | | | | . | I |
| G | . | . | . | . | . |
| D | E | F | . | K | . |
| . | . | O | P | Q | R |
| T | U | V | X | Y | Z |

The longer columns belong on the left. Shifting these columns produces this result.

| | | | | | |
|---|---|---|---|---|---|
| . | I | G | . | . | . |
| . | . | D | E | F | . |
| K | . | . | . | O | P |
| Q | R | T | U | V | X |
| Y | Z | | | | |

The matrix is now in its original form. L, M, and N can be placed between K and O. Either H or J can be inserted between F and K and the remaining letter belongs in the keyword in the top row. S and W are in the keyword, because they are missing from the alphabetical progression. That leaves A, B, or C for the remaining letter of the keyword, with the other two on the second row. Since only one vowel has been found in the keyword up until now, A probably belongs in the keyword with B and C filling the blanks in the second row. Trial placements of A, S, and W together in the first row blanks, together with either H or J in the remaining space leads to the conclusion of JIGSAW as the keyword.

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

d. The recovery of numerically keyed columnar transposition sequences is the same as for simple columnar transposition, except the columns are not in order in the sequence. The next example shows the recovery of this kind of transposition mixed sequence.

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| p: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| c: | X | M | D | B | Z | P | . | T | Y | . | . | S | U | I | R | W | . | C | O | V | J | . | L | . | H | . |

This problem is again best approached through the end of alphabet letters. V, W, X, Y, and Z have all been recovered, and they make a good starting point. V, W, X, Y, and Z are placed in a row with their preceding letters above them in columns.

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X/M D B Z/P . T Y . . S U I R W/. C O V/J . L . H .

| | | | | |
|---|---|---|---|---|
| . | U | . | P | M |
| C | I | H | . | D |
| O | R | . | T | B |
| V | W | X | Y | Z |

This time no alphabetic progression appears, even if we consider that one or two of the columns might be misplaced. In this case, the next thing to consider is that the sequence may be reversed. Selecting the letters to the right of V, W, X, Y, and Z instead of the left produces the following example.

a b c d e f g h i j k l m n o p q r s t u v w x y z
X M D B/Z P . T/Y . . S U I R/W . C O/V J . L . H .

| | | | | |
|---|---|---|---|---|
| L | O | B | S | T |
| . | C | D | . | . |
| J | . | M | . | P |
| V | W | X | Y | Z |

This setup is clearly correct. Next, we add the two short remaining segments.

a b c d e f g h i j k l m n o p q r s t u v w x y z
X M D B/Z P . T/Y . . S/U I R/W . C O/V J . L/. H ./

| | | | | | | |
|---|---|---|---|---|---|---|
| | | L | O | B | S | T |
| . | R | . | C | D | . | . |
| H | I | J | . | M | . | P |
| . | U | V | W | X | Y | Z |

Moving the short columns to the right and filling in the missing letters produces the following matrix.

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X M D B/Z P G T/Y N F S/U I R/W K C O/V J A L/Q H E/

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

The final step is to recover the numerical key. If normal methods are used, it should be produced by the keyword and should show the actual order in which the columns were extracted. Numbering the letters in the keyword in alphabetical order and comparing them with the cipher sequence in the alphabet confirms that this method was used. Since the sequence was reversed, the order of columns in the cipher sequence appears in right to left order beginning with the cipher letter B.

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X M D B/Z P G T/Y N F S/U I R/W K C O/V J A L/Q H E/
1 7 6 5 4 3 2

| 3 | 4 | 1 | 6 | 7 | 2 | 5 |
|---|---|---|---|---|---|---|
| L | O | B | S | T | E | R |
| A | C | D | F | G | H | I |
| J | K | M | N | P | Q | U |
| V | W | X | Y | Z | | |

e. One type of transposition sequence remains to be considered. When a route transposition process is used, the solution is to try to reconstruct the original routes. In examining attempts to solve the matrix by rebuilding columns, be alert to entry routes other than by rows. Look for spirals, diagonals, and alternate horizontals or verticals. If rebuilding the columns produces no results, consider rebuilding spiral, diagonal, or alternate row or column routes. This manual does not show examples of these approaches, but if you encounter this situation, approach it logically and try various approaches until one succeeds. The techniques of solving route transposition ciphers explained later in this manual will help in this process.

f. Each of the preceding examples was approached as if we knew, perhaps from past history, what types of sequences were used. We assumed that the plain component was a standard sequence, and the cipher sequence could then be readily reconstructed by itself. It is common, in approaching a cryptanalytic problem, to assume the simplest case and only to move on to more complex possibilities when the simplest case must be rejected. A great deal of time can be wasted by assuming something is more complicated than it is.

g. The next simplest case is where the cipher sequence is a standard sequence and the plain sequence is mixed. When reconstruction attempts fail because you started with an enciphering alphabet, rearranging the alphabet into a deciphering alphabet may yield results. Once rearranged, the solution is approached just as we did in the above examples. Look for short alphabet progression to indicate keyword mixed sequences. If that is not found, see if a decimation was used. If decimation was not used, try reconstructing the columns of a columnar transposition. Remember to try forward and reversed sequences.

h. If none of these approaches yields results, either with an enciphering alphabet or a deciphering alphabet, other approaches are called for. Either there are two mixed sequences, a more complex process was used, or random sequences were used.

## 4-8. Reconstruction of Alphabets With Two Mixed Sequences

Recovering alphabet structure when both sequences are mixed is more difficult than the previous examples. You are much less apt to be successful with only partial recoveries. Where the alphabet could be reconstructed during the solution of the plaintext in the previous examples, reconstruction of an alphabet with two mixed sequences must usually wait for the full solution of the plaintext. The examples in this section will begin with a fully recovered, but not reconstructed, alphabet.

a. The easiest type to recover with two mixed sequences occurs when both sequences are keyword mixed, as in the next example.

| p: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| c: | W | X | Y | Z | U | B | P | T | A | D | G | E | R | C | Q | S | F | V | H | I | J | K | L | M | N | O |

| p: | i | f | n | j | l | q | k | s | t | u | v | w | x | y | z | g | o | m | p | h | e | r | a | b | c | d |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| c: | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

Enciphering and deciphering forms of the same alphabet are shown. The underlined portions show substantial alphabetic progression in both, which is typical of alphabets with keyword mixed sequences. A transposition or decimation would not produce such an obvious progression. The underlined portions in both alphabets are probably in their original form. The remaining plain-cipher pairs are out of order. Your task is to reconstruct the original order. The usual approach at this point is to try to extend the alphabetic progression outward from the obvious progression. In this case, the enciphering alphabet shows two long alphabetic strings of cipher letters, HIJKLMNO and WXYZ, which must have some or all of the letters PQRSTUV in between. Similarly, the deciphering alphabet shows plaintext strings ABCD and STUVWXYZ, and some or all of the letters EFGHIJKLMNOPQR must be in between. Suppose the cipher letters PQRSTUV belong in exactly that order. If that is the case, then the plaintext letters GOMPHER must also be in the right order, preceding ABCD. We expect to find the keyword immediately before the beginning of the alphabetic sequence. GOMPHER, while not a recognizable word may be close to it. If we try GOMPHER as a keyword, then the remaining letters must be in alphabetical order. Adjusting the alphabet so GOMPHER is a trial keyword will produce this arrangement.

p: f i j k l n q s t u v w x y z g o m p h e r a b c d
c: B A D G E C F H I J K L M N O P Q R S T U V W X Y Z

Now the cipher sequence shows a recognizable word, BADGE, but the solution is incomplete. If we move the M-R pair so that plaintext M fits in alphabetic order instead of the keyword, we see the following alphabet.

p: f i j k l m n q s t u v w x y z g o p h e r a b c d
c: B A D G E R C F H I J K L M N O P Q S T U V W X Y Z

This rearrangement is the original sequence of the alphabet.

b. When transposed or decimated sequences are used in the alphabet, the solution is much more difficult. The alphabetic progression used in the previous example is not available to assist with reconstruction. A solution is still possible in many cases, however. When both sequences are the same sequence in the same direction, the alphabet can often be recovered quite readily.

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: L Q M N I P X S T V G W Z U R A K F E D J Y B C O H

(1) Reconstruction begins with a process called chaining. Use the plain-cipher pairs to create a 26 letter chain by linking the cipher letter of each pair to the pair with the same plaintext letter. Any pair can be used as the starting point. Beginning with the plaintext A-ciphertext L pair (abbreviated Ap-Lc) next find plaintext L. Plaintext L equals ciphertext W (Lp-Wc), producing a partial

chain of ALW. Continuing with Wp-Bc, the chain is extended to ALWB. Continue adding links to the chain until you return to the original letter A. The complete chain is shown below.

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

(2) Since we were able to produce a 26 letter chain, there is a strong indication that the same sequence was used in both components. With different sequences, the chances of producing such a chain are very low. Unrelated sequences will almost always return to the starting point before using all 26 letters. The alphabet in paragraph 4-8a, for example, produces separate 23 and 3 letter chains.

(3) The sequence produced by chaining an alphabet with two identical sequences in the same direction will always either be the original sequence or a decimation of the original sequence. This narrows the possibilities for the original sequence down to six. The chained sequence and its five possible decimations are listed below.

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

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

Decimation 5:
A K Z T V P Q M I J F B C E U R W X S N O L G H D Y

Decimation 7:
A X I Y W M D R Q H U P G E V L C T O B Z N F K S J

Decimation 9:
A M U L Z J W H V B S Y Q E O K I R G T F X D P C N

Decimation 11:
A H O X U B I P Z Y G N W E F M V K D L S R C J Q T

(4) If the original sequence was a decimated sequence, the basic keyword or standard sequence used to generate the decimated sequence would be one of the above. Since none of them are either standard or keyword mixed, the original sequence was probably transposed. Approaching each sequence above with transposition in mind, the letters V, W, X, Y, and Z have been underlined in each, searching for a basis to rebuild the columns. The last sequence (decimation 11) yields the following matrix.

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

(5) When the same sequence is used in the same direction in both components of the alphabet, a 26 letter chain will only be produced half of the time. When the two sequences are staggered by an odd number of letters, a 26 letter chain results. When the two sequences are staggered by an even number of letters, two separate 13 letter chains result. These can sometimes be recovered, too, but the solution is more difficult.

c. The chaining technique can also be used with alphabets with different sequences in the two components if they are reused at different alignments. Consider the next two alphabets, recovered at different times on the same day.

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| p: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| c: | Y | P | U | Z | G | E | A | B | H | Q | V | M | C | L | K | I | R | T | W | O | D | J | S | X | N | F |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| p: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| c: | F | L | A | G | Y | P | T | U | Z | E | B | H | Q | K | X | V | M | N | C | I | R | W | O | D | J | S |

(1) To test if the same alphabet was used, chain the cipher sequences against each other. In the example, chain A of the first to T of the second, T of the first to N of the second, and so on. This produces the following chain.

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

(2) This confirms that the two alphabets used the same sequences at different alignments. If chaining produced anything but one 26 letter sequence or two 13 letter sequences, they are not the same alphabet.

(3) Write all possible decimations, as before.

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

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

Decimation 5:
A C K H S U W L M F B J P R Y V N E D G I T Q X Z O

Decimation 7:
A E M O N L Z V W X Y U Q R S T P H I J K G B C D F

Decimation 9:
A L Y T K F N X S J D O W R I C M V Q H B E Z U P G

Decimation 11:
A X I E Y J M U K O Q G N R B L S C Z T D V P F W H

(4) The decimation of 7 produces a sequence that almost looks as if it were the original. This can happen when the decimation interval and the column length of a transposed sequence are the same except for one long column. The correct sequence is a decimation of 9 read in reverse.

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

The sequence used to generate the simply transposed sequence was a keyword mixed sequence based on LEMON.

(5) The plaintext component can be reconstructed now that the correct ciphertext sequence is known. We start with the decimated sequence. Since the sequence with a decimation of 9 was used in reverse to recover the keyword LEMON, we will list it in reverse.

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

Either of the two alphabets given at the start of this problem can be used to reconstruct the plaintext sequence. The first alphabet is repeated for reference.

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: Y P U Z G E A B H Q V M C L K I R T W O D J S X N F

We now rearrange this alphabet so that the cipher sequence is in the same order as the recovered decimated sequence.

p: e b c d f h i j k l m p q s t u v w x y z o r a n g
c: G P U Z E B H Q V M C I R W O D J S X N F K T Y L A

d. The chaining techniques introduced in this section are also used in the solution of polyalphabetic ciphers. They will be further developed in Part Four.

## Section III
# Solution of Monoalphabetic Unilateral Ciphers Using Mixed Cipher Alphabets

### 4-9. Preparation for Analysis

The first step in approaching the unsolved cryptogram is to prepare a worksheet.

a. If prepared by hand, one-fourth inch or one-fifth inch cross section paper (graph paper) should be used if possible. Hand lettering should be clearly printed in ink. The cryptogram should be triple spaced vertically to leave room for writing. If a copying machine is available and local security rules permit, the worksheet should be copied after preparation to permit a restart with a clean worksheet whenever needed.

b. Generally, you will want to prepare at least a unilateral frequency count. Other special frequency counts may be needed also, as will be explained later. If you are unsure of system identification, you may want to calculate the $\phi$IC. Computer support, if available, can save a lot of time at this step.

c. Next, you should scan the text searching for repeated segments of ciphertext. Underline all repeats you find of at least three letters in length. You may find it useful to underline two letter repeats, too.

d. If you have more than one cryptogram that appears to have been enciphered with the identical system, prepare a worksheet for each. Compare peaks and troughs of frequency counts to see if they are similar. If so, look for repeats between messages as well as within messages. Repeats between messages are another indication that the identical system was used. The more repeats you find, the easier the solution will be.

e. If you are still in doubt whether two cryptograms have been enciphered by the same system, there is a simple statistical test available, similar to the phi test. The chi test or cross product test compares two frequency distributions to determine the probability that they are from the same alphabet. The frequency of each letter in one distribution is multiplied by the frequency of the same letter in the other distribution. The results of all the multiplications are added to produce the chi value. Chi is the Greek letter that looks like an X. The formula for the chi value is—

$$X = \Sigma (f)(f2).$$

The expectation with a random match is l/26th of the product of the total letters of each, or—

$$Xr = .0385\ (N1)(N2).$$

With a correct match, the expected value is .0667 times the products of the total letters, or—

$$Xp = .0667\ (N1)(N2).$$

The results can also be expressed as an index of coincidence, the usual form if produced by computer support. The formula for the cross IC, as it is called is—

$$X\ IC = \frac{Xo}{Xr} = \frac{26\ \Sigma\ (f1)(f2)}{(N1)(N2)}.$$

With a correct match, the expected IC value, as with the phi text is 1.73. If you match two alphabets and the X IC is close to 1.73, the chances are that they were enciphered with the same alphabet. Figure 4-2 illustrates a completed chi test.

PROBLEM: To determine if the two frequency counts below were from cryptograms enciphered with the same alphabet.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| c1: | - | 3 | 2 | 6 | 1 | 13 | - | 3 | 3 | - | 3 | - | 6 | 2 | 3 | 3 | 4 | 1 | - | - | 10 | - | 1 | - | 4 | 1 | N=69 |

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| c2: | 4 | 2 | 1 | 6 | 1 | 7 | - | 4 | - | 1 | 2 | - | 5 | 1 | 3 | 4 | 4 | 3 | - | 1 | 8 | - | 1 | 1 | 2 | - | N=61 |

Product:

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| - | 6 | 2 | 36 | 1 | 91 | - | 12 | - | - | 6 | - | 30 | 2 | 9 | 12 | 16 | 3 | - | - | 80 | - | 1 | - | 8 | - |

$Xo = \Sigma\ (f)(f2) = 6 + 2 + 36 + \ldots + 8 = 315$

$Xr = .0385\ (N1)(N2) = .0385\ (69)(61) = 162$

$X\ IC = Xo/Xr = 315/162 = 1.94$

The results indicate the same alphabet was used.

Figure 4-2. Chi test.

f. As with any statistical test, you should use this as a guide only, and take all other available information into consideration, too, For example, if you find several long repeated segments of text between two cryptograms, it is probably a waste of time to calculate a chi test by hand. You already have the evidence you need to make a decision as to what approach you will use to reach a solution.

## 4-10. Approaches to the Solution

There are two basic approaches to the solution—the probable word method and the brute force approach. The probable word method is to try to gain a quick entry into the system by correctly assuming a portion of the plaintext. The brute force approach is to systematically narrow down the possible keys to the system and then force a solution by exhaustively trying all those possible keys. The method in the previous chapter of solving standard alphabet systems through trying all possible decipherment is a good example of the brute force approach. In practice, the solution of any given system is likely to use a combination of the two approaches.

## 4-11. Solution With Known Sequences - Completing the Plain Component Sequence

When the sequences used in an alphabet are known, a quick forced solution is possible.

a. Although mixed alphabets are used instead of standard ones, the solution is exactly the same as that explained in paragraph 3-7b.

(1) Set up the known alphabet at any alignment.

(2) Perform a trial decipherment (pseudotext).

(3) Using the trial decipherment as the letters at the head of the columns, generate all possible decipherment by listing the plain component sequence vertically for each column.

b. Figure 4-3 illustrates the solution of a cryptogram with known sequences using the above steps.

Solve: LIZWF QFMYK LOILX

Plain component—keyword mixed sequence based on SEA URCHIN.

Cipher component—standard sequence.

Step 1. Set up the alphabet at any alignment.

```
p: s e a u r c h i n b d f g j k l m o p q t v w x y z
c: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```

Step 2. Perform a trial decipherment.

```
p: fnzwc mcgyd fknfx
c: LIZWF QFMYK LOILX
```

Step 3. Complete the plain component sequence.

```
FNZWC MCGYD FKNFX
GBSXH
JDEYI
KFAZN
LGUSB
MJRED
OKCAF
PLHUG
QMIRJ
TONCK
VPBHL
WQDIM
XTFNO
YVGBP
ZWJDQ
SXKFT
EYLGV
AZMJW
USOKX
REPLY BYCOU RIER
CAQMZ
HUTOS
IRVPE
NCWQA
BHXTU
DIYVR
```

```
p: s e a u r c h i n b d f g j k l m o p q t v w x y z
c: H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
```

Plaintext: REPLY BY COURIER

Figure 4-3. Completing the plain component.

## 4-12. Probable Word Method

The probable word method of solution depends on your being able to correctly identify a portion of the plaintext. When you can do this, you can begin to reconstruct the keys. The partial key recoveries lead to more plaintext recoveries, and by working back and forth between keys and plaintext, you can complete the solution. There are many ways in which you can identify plaintext. The more you know about the senders of enciphered traffic and the situation in which it was sent, the more likely you are to be able to assume plaintext correctly.

a. Stereotypes. Military organizations tend to do things in standard ways. Rules for message formats are likely to be used. Standard forms are likely to be used for recurring needs. When you learn enough about the sender's standard ways of doing things, you can use those standards. Standard formats are most likely to be found in message beginnings and endings. Messages are likely to begin with addressees, message subjects, security classifications, and references to other messages. Messages are likely to end with signatures or unit identifications. These stereotypes are bad security practices, but difficult to avoid.

(1) Consider the following example of a message where stereotypes can be used to achieve a quick solution. The previous message from the same sender, already recovered, began, *TWO PART MESSAGE PART ONE.* The text gave the itinerary of a visiting team of officers from an allied country, but was incomplete. A mixed alphabet was used with the previous message, but it has changed with the new message.

ZZZZZ NSHIX LNFOM MXKOI XLNNS HNOXF STDDR OIXLN XNMTU NOOGN

ETLNV EHPLM YVEOD TZHIN OLLDA HGOMZ HFFXG RTGKX ZZZZZ

(2) The first and last groups (ZZZZZ) are obviously not part of the text of the message. They are probably indicators of some kind.

(3) We begin by preparing the following worksheet with a frequency count and underlined repeats. The indicator groups are not included in the frequency count.

| | | | | |
|---|---|---|---|---|
| NSHIX | LNFOM | MXKOI | XLNNS | HNOXF |
| STDDR | OIXLN | XNMTU | NOOGN | ETLNV |
| EHPLM | YVEOD | TZHIN | OLLDA | HGOMZ |
| HFFXG | RTGKX | | | |

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:

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

(4) If this is a follow-on to the message that began, *TWO PART MESSAGE PART ONE,* we would assume that it would begin *TWO PART MESSAGE PART TWO.* The underlined repeats are positioned perfectly for the repeated words *TWO* and *PART,* so the assumption seems well borne out.

(5) Next, we enter the assumed text in the message and the alphabet. Using those recovered values throughout the message produces the text shown below.

```
t w o p a   r t m e s   s a g e p   a r t t w   o t e a m
N S H I X   L N F O M   M X K O I   X L N N S   H N O X F

w           e p a r t   a t s       t e e   t       r t
S T D D R   O I X L N   X N M T U   N O O G N   E T L N V

  o   r s         e       o p t     e r r       o   e s
E H P L M   Y V E O D   T Z H I N   O L L D A   H G O M Z

o m m a           g a
H F F X G   R T G K X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X       O   K           F   H I   L M N       S
```

(6) From the recovered ciphertext letters, it appears that the cipher sequence is keyword mixed. On that basis, ciphertext G and J are placed in alphabetical order.

```
t w o p a   r t m e s   s a g e p   a r t t w   o t e a m
N S H I X   L N F O M   M X K O I   X L N N S   H N O X F

w           e p a r t   a t s       t e e n t       r t
S T D D R   O I X L N   X N M T U   N O O G N   E T L N V

  o   r s         e       o p t     e r r       o n e s
E H P L M   Y V E O D   T Z H I N   O L L D A   H G O M Z

o m m a n       n g a
H F F X G   R T G K X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X       O   K           F G H I J L M N       S
```

(7) Several possibilities for additional plaintext appear in the message with these additions. You may see other possibilities but for illustration, we will add the letters for the word *COMMANDING* appearing at the end of the message.

```
t w o p a   r t m e s   s a g e p   a r t t w   o t e a m
N S H I X   L N F O M   M X K O I   X L N N S   H N O X F

w i     d   e p a r t   a t s i     t e e n t     i r t
S T D D R   O I X L N   X N M T U   N O O G N   E T L N V

  o   r s         e     i c o p t   e r r       o n e s c
E H P L M   Y V E O D   T Z H I N   O L L D A   H G O M Z

o m m a n   d i n g a
H F F X G   R T G K X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X   Z R O   K   T       F G H I J L M N     S
```

(8) Additional placements are possible. Ciphertext Y belongs between X and Z. P and Q fit between N and S. U, V, and W fit between Sand X. The first word on the second line appears to be WILL. The phrase SIXTEEN THIRTY HOURS appears.

```
t w o p a   r t m e s   s a g e p   a r t t w   o t e a m
N S H I X   L N F O M   M X K O I   X L N N S   H N O X F

w i l l d   e p a r t   a t s i x   t e e n t   h i r t y
S T D D R   O I X L N   X N M T U   N O O G N   E T L N V

h o u r s   b y h e l   i c o p t   e r r l     o n e s c
E H P L M   Y V E O D   T Z H I N   O L L D A   H G O M Z

o m m a n   d i n g a
H F F X G   R T G K X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X Y Z R O   K E T     D F G H I J L M N P Q S U V W
```

Only the ciphertext letters A, B, and C remain to be placed. Of those, only A is used in the text, and it appears to be part of the commander's name. If C is placed as part of the keyword ROCKET and A and B placed in alphabetical order, the commander's name becomes *R L JONES.* The plaintext is *TWO PART MESSAGE PART TWO TEAM WILL DEPART AT SIXTEEN THIRTY HOURS BY HELICOPTER R L JONES COMMANDING.* The complete alphabet is shown below.

```
p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X Y Z R O C K E T A B D F G H I J L M N P Q S U V W
```

b. Exploitation of Numbers. Not all cryptograms will include such stereotyped beginnings and endings. Without these stereotypes, repeated words in the text offer another possible point of entry. Spelled out numbers are often easy to recognize when they repeat in messages, as shown in the next example.

```
H W B N F   W A Z A O   U R R W L   W W Z M U   O J R N E

J Y I S J   R J O Q W   E U D R C   W R S Z N   N P W A Z

R C W E N   B N O K F   G N Z W E   U D R S Z   N N G N Z

W S W A Z   E X X X X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:

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

(1) The pattern of consecutive short three- to five-letter repeats is characteristic of numbers. Numbers tend to occur with each other in such things as grid coordinates, times, and quantities. In the above example, the repeated RSZNN must be *THREE,* the only five letter number to end in a double letter. We begin by placing *THREE* in the alphabet and entering other occurrences of the same letters.

```
      e         r         t t           r           t e
H W B N F   W A Z A O   U R R W L   W W Z M U   O J R N E

      h     t                 t       t h r e   e       r
J Y I S J   R J O Q W   E U D R C   W R S Z N   N P W A Z

t       e     e           e r           t h r   e e   e r
R C W E N   B N O K F   G N Z W E   U D R S Z   N N G N Z

  h     r
W S W A Z   E X X X X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:         N     S                   Z R
```

(2) The recovered letters suggest additional numbers. RCW, which begins with plaintext T must be *TWO.* GNZW, which includes ER as the middle two letters must be *ZERO.* EUD, which has no letters in common with THREE, TWO, or ZERO, can only be *SIX.*

```
  o   e     o   r       i t t o     o o r   i       t e s
H W B N F   W A Z A O   U R R W L   W W Z M U   O J R N E

      h     t       o   s i x t w   o t h r e   e   o   r
J Y I S J   R J O Q W   E U D R C   W R S Z N   N P W A Z

t w o s e     e         z e r o s   i x t h r   e e z e r
R C W E N   B N O K F   G N Z W E   U D R S Z   N N G N Z

o h o   r   s
W S W A Z   E X X X X

p:  a b c d e f g h i j k l m n o p q r s t u v w x y z
c:          N     S U           W     Z E R     C D   G
```

(3) Several more possibilities can be placed at this point. Ciphertext F can be placed between D and G in the cipher sequence as the alphabetical structure begins to appear. The last word of the message is apparently *HOURS,* needing only the U to complete it. The partially repeated *FOUR* can be seen at the end of line two, and *SEVEN* follows *TWO* on the third line.

```
  o v e y   o u r u n   i t t o     o o r   i     n t e s
H W B N F   W A Z A O   U R R W L   W W Z M U   O J R N E

      h     t   n   o   s i x t w   o t h r e   e f o u r
J Y I S J   R J O Q W   E U D R C   W R S Z N   N P W A Z

t w o s e   v e n   y   z e r o s   i x t h r   e e z e r
R C W E N   B N O K F   G N Z W E   U D R S Z   N N G N Z

o h o u r   s
W S W A Z   E X X X X

p:  a b c d e f g h i j k l m n o p q r s t u v w x y z
c:          N P   S U         O W     Z E R A B C D F G
```

(4) The first word is *MOVE.* Q can be placed between P and S in the cipher sequence. The word *BY* completes the third line. With ciphertext K placed from the word *BY,* ciphertext L and M can also be placed.

```
m o v e y   o u r u n   i t t o c   o o r d i   n   t e s
H W B N F   W A Z A O   U R R W L   W W Z M U   O J R N E

      h     t   n g o   s i x t w   o t h r e   e f o u r
J Y I S J   R J O Q W   E U D R C   W R S Z N   N P W A Z

t w o s e   v e n b y   z e r o s   i x t h r   e e z e r
R C W E N   B N O K F   G N Z W E   U D R S Z   N N G N Z

o h o u r   s
W S W A Z   E X X X X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:   K L M N P Q S U       H O W     Z E R A B C D F G
```

(5) *COORDINATES* online one provides the plaintext letter A as ciphertext J. With J placed in the alphabet, the letter I must be in the keyword, along with T, which will not fit in the alphabetic progression. The keyword is therefore *HOWITZER.* The complete plaintext is *MOVE YOUR UNIT TO COORDINATES ALPHA TANGO SIX TWO THREE FOUR TWO SEVEN BY ZERO SIX THREE ZERO HOURS.*

c. Word Patterns. When neither stereotypical beginnings and endings nor repeated numbers provide a point of entry, repeated words can often be recognized by their patterns of repeated letters.

(1) Such words as ENEMY, ATTACK, and DIVISION have repeated letter patterns that make them easy to recognize. They are even easier to recognize when the words are repeated in the text. Underlining the repeats gives an indication of where the words begin and end. For example, ATTACK and BATTALION have the same pattern of repeated letters. If the ciphertext OGGORF is repeated in the text, it is much more likely to be ATTACK than a portion of the word BATTALION. It could also be EFFECT, ATTAIN, or a number of other possibilities.

(2) In the case where two or more words have identical patterns, such as ATTACK and EFFECT, letter frequencies can help to decide between the possibilities. If the letters O and F of OGGORF are high frequency letters and the rest are fairly low, it is more likely to be EFFECT than ATTACK. If all the letters are high in frequency, ATTAIN is likely.

(3) Tables have been compiled of common pattern words for various languages to assist in analysis. Table D-3 in Appendix D of this manual provides an English

language word pattern table. Word patterns are also called *idiomorphs.* There is a formal procedure for recording word patterns, which is followed in the table. When you find a pattern word repeated in a cryptogram, you can follow the same procedure to record the pattern and then look it up in the table. The procedure is this—

- Find the first repeated letter in the pattern, and designate all occurrences of that character with the letter A.

```
G R F L Y M F P A R P Z
  A               A
```

- Continue lettering alphabetically from left to right, making sure that each new character gets the next letter of the alphabet and each repeated character gets the same letter.

```
G R F L Y M F P A R P Z
  A B C D   B     A
```

- Stop lettering when the last occurrence of the last repeated character is reached. In the example, P is the last occurrence of the last repeated character. The final character Z is not lettered.

```
G R F L Y M F P A R P Z
  A B C D E B F G A F
```

- Designate any characters before and after the pattern characters with dashes to show the length of the word.

```
G R F L Y M F P A R P Z
- A B C D E B F G A F -
```

(4) To use the pattern, refer to Appendix D, Table D-3. The patterns are in alphabetical order beginning on page D-19. The pattern ABCDEBFGAF is located on page D-34. The only word listed for this pattern is *H EADQUARTER* S. The extra letters at the beginning and end of the pattern, designated by the dashes, fit HEADQUARTERS perfectly.

(5) The use of word patterns to solve a cryptogram is shown in the next example.

XGGXF SEALL KQIAV XGJQM UNAHD

PVWMQ WGUTU MMUET UMVAV IAVBA

FAVAG ZURFM UNNMU XWNGD MQQNA

HGEUN GUCZU PMMQI ATQVG EALLN

CQXMD QXWXG GXFSN GUCWA BANAU

VFUTT XVWEA LLTUB QRUME XMWRM

UTFMU NNMUX WNGEU RABQV AVQGU

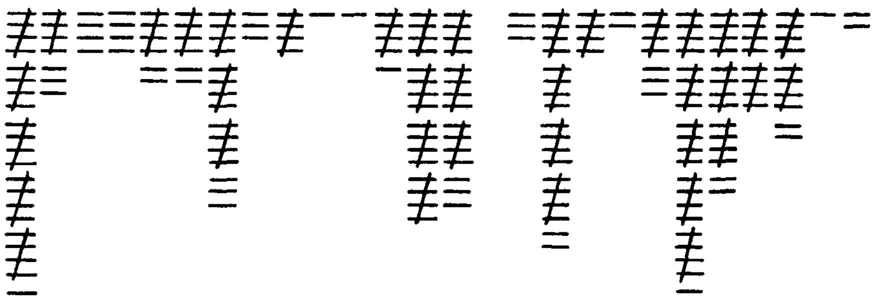
MUXWY PVFGA UVQAI DGNQB QVNAH

NGUCU VQRAB QMQIA TQVGA NWABA

NAUVM QNQMB QXXXX

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:

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



(6) The cryptogram shows all repeats longer than three letters. There are a number of shorter repeats, too, which will be used if necessary. We begin the analysis by deriving the word patterns for the longer repeats. The pattern and possible words from Appendix D for each repeat are shown below.

| XGGXFS | FMUNNMUXWNG | MQIATQVG | WABANAUV |
|---|---|---|---|
| ABBA-- | -ABCCABDEC- | -ABCDA-- | -ABACA-- |
| AFFAIR | CROSSROADS? | SABOTAGE | CEMETERY |
| ATTACH | | EASTWARD | VICINITY |
| ATTACK | | REGIMENT | DIMINISH |
| ATTAIN | | INTERNAL | CIVILIAN |
| EFFECT | | INTRENCH | DIVISION |
| OPPOSE | | | MONOPOLY |

(7) *CROSSROADS* is the only choice for the second patten. There is an extra letter at the end of the repeat, but that may have been caused accidentally by a repeated first letter of the next word in each case. Using *CROSSROADS* as a trial starting point, we compare common letters with the other repeats. From *CROSSROADS,* we see that cipher M equates to plaintext R, for example. Examining the possible choices for the MQIATQVG repeat, only REGIMENT is consistent with the Rp-Mc pair. Similarly, the Op-Uc and Dp-Wc pairs of *CROSSROADS* are consistent with *DIVISION* for the WABANAUV repeat and no others. The common plaintext N and I between REGIMENT and DIVISION also equate to the same cipher letters (V and A) giving further evidence that we are on the right track. Using the common letters between *CROSSROADS,* REGIMENT, and DIVISION with the XGGXFS possibilities shows that either ATTACH or ATTACK is consistent with the first three. We now place the letters of *CROSSROADS, REGIMENT,* and *DIVISION* in the alphabet and cryptogram.

```
a t t a c      i        e g i n  a t   e r  o s i
X G G X F  S E A L L  K Q I A V  X G J Q M  U N A H D

  n d r e  d t o m o  r r o   m  o r n i n  g i n v i
P V W M Q  W G U T U  M M U E T  U M V A V  I A V B A

c i n i t    o   c r  o s s r o  a d s t    r e e s i
F A V A G  Z U R F M  U N N M U  X W N G D  M Q Q N A

  t   o s  t o     o    r r e q  i m e n t    i     s
H G E U N  G U C Z U  P M M Q I  A T Q V G  E A L L N

  e a r    e a d a t  t a c   s  t o   d i  v i s i o
C Q X M D  Q X W X G  G X F S N  G U C W A  B A N A U

n c o m m  a n d   i      m o v  e   o r    a r d   r
V F U T T  X V W E A  L L T U B  Q R U M E  X M W R M

o m c r o  s s r o a  d s t   o    i v e n  i n e t o
U T F M U  N N M U X  W N G E U  R A B Q V  A V Q G U

r o a d      n c t i  o n e i g    t s e v  e n s i
M U X W Y  P V F G A  U V Q A I  D G N Q B  Q V N A H

s t o   o  n e   i v  e r e g i  m e n t i  s d i v i
N G U C U  V Q R A B  Q M Q I A  T Q V G A  N W A B A

s i o n r  e s e r v  e
N A U V M  Q N Q M B  Q X X X X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X   F W Q   I   A       T V U     M N G   B
```

(8) With this start, you should be able to see many more possible plaintext words in the text. *TOMORROW, VICINITY,* and *ROAD JUNCTION* all appear with

only one or two letters missing. Many spelled out numbers also appear. The repeated NGUC is *STOP,* a common stereotype used in telegraphic text in place of a period. EALL is *WILL.* XGGXFS must be *ATTACK.* The completed plaintext is—

"ATTACK WILL BEGIN AT ZERO SIX HUNDRED TOMORROW MORNING IN VICINITY OF CROSSROADS THREE SIX TWO STOP YOUR REGIMENT WILL SPEARHEAD ATTACK STOP DIVISION COMMAND WILL MOVE FORWARD FROM CROSSROADS TWO FIVE NINE TO ROAD JUNCTION EIGHT SEVEN SIX STOP ONE FIVE REGIMENT IS DIVISION RESERVE."

(9) Use of word patterns is a powerful tool to gain entry into a cryptogram. It will not always work out as easily as the example shown here. Repeated letters do not always represent repeated words. Many words that are used in messages will not be found in the word pattern tables, particularly proper names. Be alert to the patterns of repeated letters in names you would expect to find in message traffic. If you can recognize the pattern of a word, it does not have to be in the tables to use it.

## 4-13. Vowel-Consonant Relationships

When you can successfully discover plaintext words in a cryptogram, the solution usually comes quickly. Sometimes you will encounter a cryptogram in which you can find no basis to assume plaintext. You can find no stereotypes, no usable numbers, and no repeated pattern words. In these cases, you can use the characteristics of the language itself to determine individual letters.

a. Language Characteristics. Languages which use an alphabet to spell out words phonetically produce exploitable letter relationships. To make words pronounceable, vowels and consonants tend to alternate. We do not expect to find many consonants or many vowels consecutively. In cases where they do, the possibilities are limited to pronounceable combinations. Exploitation of these letter relationships begins by determining which letters are consonants and which are vowels.

(1) Vowels tend to occur next to consonants. Consonants tend to occur next to vowels. Each contacts the other more readily than it contacts its own type.

(2) Since there are more consonants than vowels in English, vowels tend to contact more different letters than consonants do. A vowel will commonly contact a lot of different consonants, whereas a consonant will tend to contact the smaller number of vowels. By studying which letters contact each other and how many different contacts each letter has, we can sort ciphertext letters into vowels and consonants fairly reliably.

(3) To make use of these vowel-consonant relationships, we use a special kind of frequency count which charts contacts as well as frequencies.

b. Trilateral Frequency Count. The trilateral frequency count is used to record, for each letter in a cryptogram, the letter that precedes it and the letter that follows it. Figure 4-4 shows a cryptogram and its trilateral frequency count. The pairs of letters appearing in the column below each letter of the alphabet are the preceding and following letters for each occurrence. For example, the YG that appears below the letter A shows that the first A in the cryptogram occurred as part of the segment YAG. Refer to the cryptogram itself, and you will see that the segment YAG occurs in the second group of the message. Two numbers appear above each letter of the alphabet. The top figure is the frequency of that letter, which is the same as the number of pairs of letters in the column below it. The second number is the number of different letters the basic letter contacts. This type of frequency distribution and its supporting contact information take some time to prepare by hand, but they can lead to the solution when other methods fail.

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

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:
```

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Frequency: | 8 | 13 | 1 | 2 | 6 | 6 | 9 | 1 | 5 | 1 | 3 | 1 | - | 2 | 1 | 1 | 4 | 3 | 5 | 13 | 9 | 12 | 5 | 3 | 16 | - |
| Contacts: | 7 | 12 | 2 | 4 | 4 | 6 | 8 | 2 | 5 | 1 | 6 | 1 | - | 4 | 2 | 2 | 4 | 4 | 5 | 12 | 9 | 11 | 3 | 2 | 12 | - |
| | YG | LW | EY | UR | TE | YB | AG | TB | GO | VV | GB | -B | | KU | IY | VS | FV | YY | BK | AG | BU | BG | BY | GY | WR | |
| | BT | GG | | YT | EA | UQ | GB | | UG | | ST | | | BV | | | UV | DT | BT | GB | UB | QT | YY | GY | RA | |
| | ET | FA | | | TE | QQ | BI | | FV | | YN | | | | | | YF | AT | PT | KE | BY | YJ | TY | Y- | OF | |
| | YY | TU | | | EC | QV | TT | | VG | | | | | | | | FF | | BB | AH | YF | JB | TY | | UA | |
| | BA | UV | | | TE | YI | VK | | FG | | | | | | | | | | VT | VW | TD | YB | TY | | AW | |
| | AT | KS | | | EA | BI | IX | | | | | | | | | | | | | AU | TI | QY | | | WU | |
| | YR | HU | | | | | IB | | | | | | | | | | | | | RE | NQ | FY | | | WV | |
| | EG | VA | | | | | AB | | | | | | | | | | | | | DU | YT | II | | | CD | |
| | | VS | | | | | IX | | | | | | | | | | | | | SW | TY | BP | | | XV | |
| | | GV | | | | | | | | | | | | | | | | | | SV | | TY | | | WK | |
| | | GF | | | | | | | | | | | | | | | | | | RE | | YB | | | VQ | |
| | | VS | | | | | | | | | | | | | | | | | | SW | | NS | | | VF | |
| | | SN | | | | | | | | | | | | | | | | | | UU | | | | | VA | |
| | | | | | | | | | | | | | | | | | | | | | | | | | XV | |
| | | | | | | | | | | | | | | | | | | | | | | | | | WU | |
| | | | | | | | | | | | | | | | | | | | | | | | | | UX | |

Figure 4-4. Triliteral frequency distribution.

(1) The contact information is used to determine which ciphertext letters are vowels and which are consonants. More often than not, the highest frequency plaintext letter is a vowel, even when E is not the highest frequency letter. An even more reliable indicator is the number of contacts. The letter that contacts the most different letters will usually be a vowel. In the example in Figure 4-4, ciphertext Y is likely to be a vowel for both reasons. The letters that Y contacts most frequently are likely to be consonants.

(2) In cases where there are several letters all about the same frequency and no letter stands out as a likely vowel, we can begin our approach through likely consonants instead. All or most of the lowest frequency letters should be consonants. The letters they contact most frequently are likely to be vowels.

(3) We can use either a likely vowel or the set of likely low frequency consonants as our starting point. Whichever we start with, we will use both as the problem develops. The object is to separate the consonants and vowels by plotting the contacts of each in separate vowel and consonant line charts.

(4) For our example, we will pick the low frequency consonants as the starting point. The process begins by charting the contacts of the lowest frequency letters. We will begin with the letters that only occurred once in Figure 4-4–C, H, J, L, O, and P. Draw a horizontal line two to three inches long and write the selected letters above it. Draw a vertical line several inches from the center of the horizontal line producing a T-shaped figure. This is the consonant line. The contacts are charted on the line with the first letters of each pair to the left and the second to the right. Each new contact letter is charted on a new row. With the contacts for C, H, J, L, O, and P charted, the consonant line appears below.

```
 C H J L O P
 ___________
       E |
         | YY
       T |
         | BB
      VV | V
       I |
         | S
```

(5) Continue adding the lowest frequency letters one frequency group at a time. We first placed those with a frequency of one. Next add those with a frequency of two. Continue with those with a frequency of three and so on. Stop when the next frequency would represent more than 20 percent of the total. Going any further raises the chance too high of including a vowel that would bias the chart. If a vowel occurs only once or twice and is included, its influence will be small. If it occurs five or six times and we include it, it could lead to wrong follow-on

decisions on vowels and consonants. In our example, there are 130 letters. We want to keep our sample below 20 percent, or not more than 26 letters altogether. On this basis, we can add the frequencies of 2, 3, and 4, but not 5.

| D N K<br>C H J | R X Q<br>L O P |
|---:|:---|
| E | |
| YYYYY | YYYYY |
| T | TTTT |
| B | BBB |
| VV | VVVV |
| I | |
| S | S |
| UU | U |
| | R |
| K | |
| GGG | |
| | N |
| D | |
| A | |
| FF | FF |

(6) The consonant line now shows that the low frequency consonants contact the ciphertext letter Y more than any other letter. The probability is very high that this is a vowel. It is tempting to select the letter V as a vowel, but it is better to proceed one letter at a time at this point.

(7) Using the letter Y and its contacts, we next begin construction of a vowel line. It is charted exactly the same as the consonant line chart. The vowel line including just the letter Y's contacts is shown below.

Y

| | |
|---:|:---|
| WWWWW | W |
| R | R |
| A | AAA |
| O | |
| | FF |
| UU | UU |
| VVV | VVV |
| C | |
| | D |
| XX | X |
| | K |
| | Q |

(8) The vowel line shows us we were correct in not initially accepting the letter V as a vowel. It contacts the low frequency consonants quite readily, but it also contacts a vowel readily. It may be a consonant such as R, L, or N which easily

combines with other consonants. We will not try to place V in either line at this point.

(9) The letter W contacts Y six times and is a likely consonant. We will continue by going back to the consonant line and adding W.

W
C H J L O P D N K R X G

| | |
|---|---|
| E | |
| YYYYYY | YYYYYYYYYY |
| TTTT | TTTT |
| BB | BBB |
| VV | VVVV |
| I | |
| S | S |
| UU | U |
| | R |
| K | |
| GGG | |
| | N |
| D | |
| A | |
| FF | FF |

Y

| | |
|---|---|
| WWWWW | W |
| R | R |
| A | AAA |
| O | |
| | FF |
| UU | UU |
| VVV | VVV |
| C | |
| | D |
| XX | X |
| | K |
| | Q |

(10) The letter T now appears as a strong candidate for a vowel. It is second only to Y in consonant contacts so far, and just as importantly, it does not contact the already selected vowel at all. We add T and its contacts to the vowel line.

W
C H J L O P D N K R X G

| | |
|---|---|
| E | |
| YYYYYY | YYYYYYYYYY |
| TTTT | TTTT |
| BB | BBB |
| VV | VVVV |
| I | |
| S | S |
| UU | U |
| | R |
| K | |
| GGG | |
| | N |
| D | |
| A | |
| FF | FF |

YT

| | |
|---|---|
| WWWWW | WWWW |
| RRR | R |
| AAAA | AAA |
| O | |
| | FF |
| UUU | UUUUU |
| VVVV | VVVV |
| C | |
| D | D |
| XX | X |
| K | K |
| | Q |
| G | G |
| | B |
| | EEE |
| | H |
| SSS | |

(11) The vowel line shows A and U as likely consonants. Adding these letters to the consonant line produces the next diagram.

```
                A U W
C H J L O P D N K R X G
-----------------------------
          EEE |
  YYYYYYYYYYY | YYYYYYYYYYYYY
      TTTTTTT | TTTTTTTT
       BBBBBB | BBBB
           VV | VVVV
            I | I
            S | S
          UUU | UU
              | RR
            K |
          GGG | GG
            N | N
            D | D
           AA | A
           FF | FFF
              | Q
```

```
           YT
----------------
WWWWW | WWWW
  RRR | R
 AAAA | AAA
    O |
      | FF
  UUU | UUUUU
 VVVV | VVVV
    C |
    D | D
   XX | X
    K | K
      | Q
    G | G
      | B
      | EEE
      | H
  SSS |
```

(12) B appears to be a vowel. This is reinforced by the letters BUUB in the first line of the text. If U was correctly selected as a consonant, B is probably a vowel on the basis of this letter pattern. It is a good idea at this point to return to the text and underline all the recovered vowels.

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

```
p: a b c d e f g h i j k l m n o p q r s t u v w x y
c:
```

A U W

| C H J L O P | D N K R X G |
|---:|:---|
| EEE | |
| YYYYYYYYYYY | YYYYYYYYYYYYY |
| TTTTTTT | TTTTTTTT |
| BBBBBB | BBBB |
| VV | VVVV |
| I | I |
| S | S |
| UUU | UU |
| | RR |
| K | |
| GGG | GG |
| N | N |
| D | D |
| AA | A |
| FF | FFF |
| | Q |

BYT

| | |
|---:|:---|
| WWWWW | WWWWW |
| RRR | R |
| AAAA | AAAAA |
| O | |
| F | FF |
| UUUU | UUUUUUU |
| VVVVVVV | VVVVVV |
| C | |
| D | D |
| XX | X |
| KK | K |
| | Q |
| GGGG | GG |
| | B |
| | EEE |
| H | H |
| SSSS | SSS |
| L | |
| | N |
| T | |

(13) Examination of the vowel-consonant patterns in the text confirms additional consonants. Double letters preceding or following the vowel are very unlikely to be vowels. We can then assign ciphertext E and Gas consonants. The GGBG segment on the first line could not all be vowels. EE occurs three times in the text following a vowel.

(14) V appears to be a consonant from the number of contacts in the vowel line, and its appearance between vowels in the segments YVB and TVY confirm it as a consonant. Placing G, E, and V in the consonant line produces this diagram.

A U W G E V

| C H J L O P | D N K R X Q |
|---:|:---|
| EEEEEE | EEE |
| YYYYYYYYYYYYYY | YYYYYYYYYYYYYYYY |
| TTTTTTTTTTTT | TTTTTTTTTT |
| BBBBBBBBB | BBBBBBBBBB |
| VVV | VVVV |
| IIIII | III |
| S | SS |
| UUU | UU |
| | RR |
| K | K |
| GGGG | GGGG |
| NN | N |
| D | D |
| AAAA | AAA |
| FFF | FFF |
| QQ | Q |
| J | J |
| | P |
| | C |
| | XX |

BYT

| | |
|---:|:---|
| WWWWW | WWWWW |
| RRR | R |
| AAAA | AAAAA |
| O | |
| F | FF |
| UUUU | UUUUUUU |
| VVVVVVV | VVVVVV |
| C | |
| D | D |
| XX | X |
| KK | K |
| | Q |
| GGGG | GG |
| | B |
| | EEE |
| H | H |
| SSSS | SSS |
| L | |
| | N |
| T | |

(15) The letters F, I, and S remain unidentified. At least one of these is likely to be a vowel, since four of the letters are expected to be vowels and we have only identified three so far. Comparing the appearance of F, I, and S in the vowel and consonant lines, we see that the letter I is the best candidate for a vowel. The letter I does not appear on the vowel line at all, whereas, F and S directly contact a number of the recovered vowels. We now underline I in the text and add it to the vowel line.

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

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:
```

| A U W<br>C H J L O P | G E V<br>D N K R X Q |
|---:|:---|
| EEEEEE | EEE |
| YYYYYYYYYYYYYY | YYYYYYYYYYYYYYYY |
| TTTTTTTTTTTT | TTTTTTTTTT |
| BBBBBBBBB | BBBBBBBBBB |
| VVV | VVVV |
| IIIII | III |
| S | SS |
| UUU | UU |
| | RR |
| K | K |
| GGGG | GGGG |
| NN | N |
| D | D |
| AAAA | AAA |
| FFF | FFF |
| QQ | Q |
| J | J |
| | P |
| | C |
| | XX |

| BYT I | |
|---:|:---|
| WWWWW | WWWWW |
| RRR | R |
| AAAA | AAAAA |
| O | O |
| FFF | FFF |
| UUUUU | UUUUUUU |
| VVVVVVVV | VVVVVVV |
| C | |
| D | D |
| XX | X |
| KK | K |
| | Q |
| GGGGG | GGGGG |
| | B |
| | EEE |
| H | H |
| SSSS | SSS |
| L | |
| | N |
| T | |

(16) There are a number of directions you can take at this point. No single example can demonstrate them all. Some of the approaches that can be tried are—

- To analyze vowel combinations to determine individual vowels.

- To search for the plaintext consonants N and H. These two letters have typical patterns of contact with consonants and vowels. N tends to follow vowels and precede consonants. H tends to follow consonants and precede vowels. In some cryptograms these features will be very evident in the vowel and consonant line diagrams. In others, they will not stand out at all.
- To recover double letters by frequency analysis. Plaintext LL is the most frequent double consonant. EE and OO are the most frequent double vowels.
- To recover common word endings such as -ING and -TION, which often appear as repeats even when complete words do not repeat.

(17) We will use several of these approaches to complete the solution of the sample problem. First, one vowel combination appears in the cryptogram, the ciphertext TB as part of the segment TGTBU. Referring to the two-letter frequency data in Appendix A, page A-2, the most frequent vowel combinations are EE, IO, OU, and EA. TB is not EE, because it is not a double letter. It is likely to be one of the other three. IO is particularly significant, because it is usually part of a -TION combination when it appears. The letters G and U, which precede and follow BT in the text, are high frequency consonants and support the -TION possibility. The letter T occurs again before G, which would produce -ITION, a very good letter combination.

(18) If TGTBU is -ITION, the letter U may appear with the typical pattern of plaintext N. Examining the occurrence of U in the vowel and consonant lines, we see that U follows vowels more often than it precedes them. It also precedes consonants more often than it follows. The differences are slight, but they help to confirm the initial assumption.

(19) Ciphertext EE occurs three times. This is likely to be plaintext LL. Each time it is preceded by ciphertext T, which we have tentatively identified as the plaintext I. ILL is another good combination that appears as part of many common words such as HILL and WILL.

(20) Y is the most common letter, and it is a vowel. While we would not usually begin analysis by assuming the most common vowel is E, our tentative identification of I and O make this much more likely. If Yc is Ep, then the remaining high frequency vowel, Ic, is probably Ap.

(21) Placing all the tentative recoveries in the cryptogram produces the next example.

```
  o   e     e   t t o   t a   e     o   i t i   o n n o
L B W Y R   Y A G G B   G I O Y F   B A T G T   B U U B V

t   o       i l l   i     o n e     e   e n         i   e
G K B S K   T E E A T   H B U Y A   Y W Y U F   Q V T W Y

      o       i n       i l l   e     i n a t     e   o
V J V B A   A T U D R   T E E C Y   D T U I G   X Y V B S

i   e       n     e             e     a   a t   o       i
T W Y K N   U Q V Y Q   F Q F V Y   F I V I G   B V P S T

  e     i   l l   t o     a t   e     o   o         i   e
V Y A R T   E E A G B   F I G X Y   V B S B N   V S T W Y

n i n e
U T U Y X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: I       Y       T     E   U B         G
```

(22) With the assumed letters filled in, two numbers stand out. *ONE* appears in the second line, and *NINE* appears in the last line. Since numbers tend to occur with each other, our next objective is to try to place additional numbers adjacent to these two. If we try *SEVEN* after *ONE* because of the -E-EN pattern, it leads to the recovery of *SIX* before *ONE* and *FIVE* before *NINE.*

(23) All of the high frequency plaintext letters except R are now recovered. Vc is the obvious candidate for Rp due to its high frequency and appearance in the text.

(24) Placing plaintext S, V, X, F, and R reveals this text.

```
  o v e     e s t t o   t a   e     o s i t i   o n n o r
L B W Y R   Y A G G B   G I O Y F   B A T G T   B U U B V

t   o f     i l l s i   x o n e s   e v e n       r i v e
G K B S K   T E E A T   H B U Y A   Y W Y U F   Q V T W Y

r   r o s   s i n       i l l   e     i n a t     e r o f
V J V B A   A T U D R   T E E C Y   D T U I G   X Y V B S

i v e       n   r e           r e     a r a t   o r   f i
T W Y K N   U Q V Y Q   F Q F V Y   F I V I G   B V P S T

r e s   i   l l s t o     a t   e   r o f o     r f i v e
V Y A R T   E E A G B   F I G X Y   V B S B N   V S T W Y

n i n e
U T U Y X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: I       Y S     T     E   U B     V A G   W   H
```

(25) Many possibilities for plaintext appear now. *ZERO, POSITION, RIVER CROSSING, PREPARATORY,* and *FOUR* can all be seen upon close examination.

```
m o v e w   e s t t o   t a k e p   o s i t i   o n n o r
L B W Y R   Y A G G B   G I O Y F   B A T G T   B U U B V

t h o f h   i l l s i   x o n e s   e v e n p   d r i v e
G K B S K   T E E A T   H B U Y A   Y W Y U F   Q V T W Y

r c r o s   s i n g w   i l l b e   g i n a t   z e r o f
V J V B A   A T U D R   T E E C Y   D T U I G   X Y V B S

i v e h u   n d r e d   p d p r e   p a r a t   o r y f i
T W Y K N   U Q V Y Q   F Q F V Y   F I V I G   B V P S T

r e s w i   l l s t o   p a t z e   r o f o u   r f i v e
V Y A R T   E E A G B   F I G X Y   V B S B N   V S T W Y

n i n e
U T U Y X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: I C J Q Y S D K T ? O E L U B F ? V A G N W R H P X
```

(26) Analysis of the cipher sequence shows it to be a simply transposed keyword mixed sequence, which identifies Jp as Zc and Qp as Mc.

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