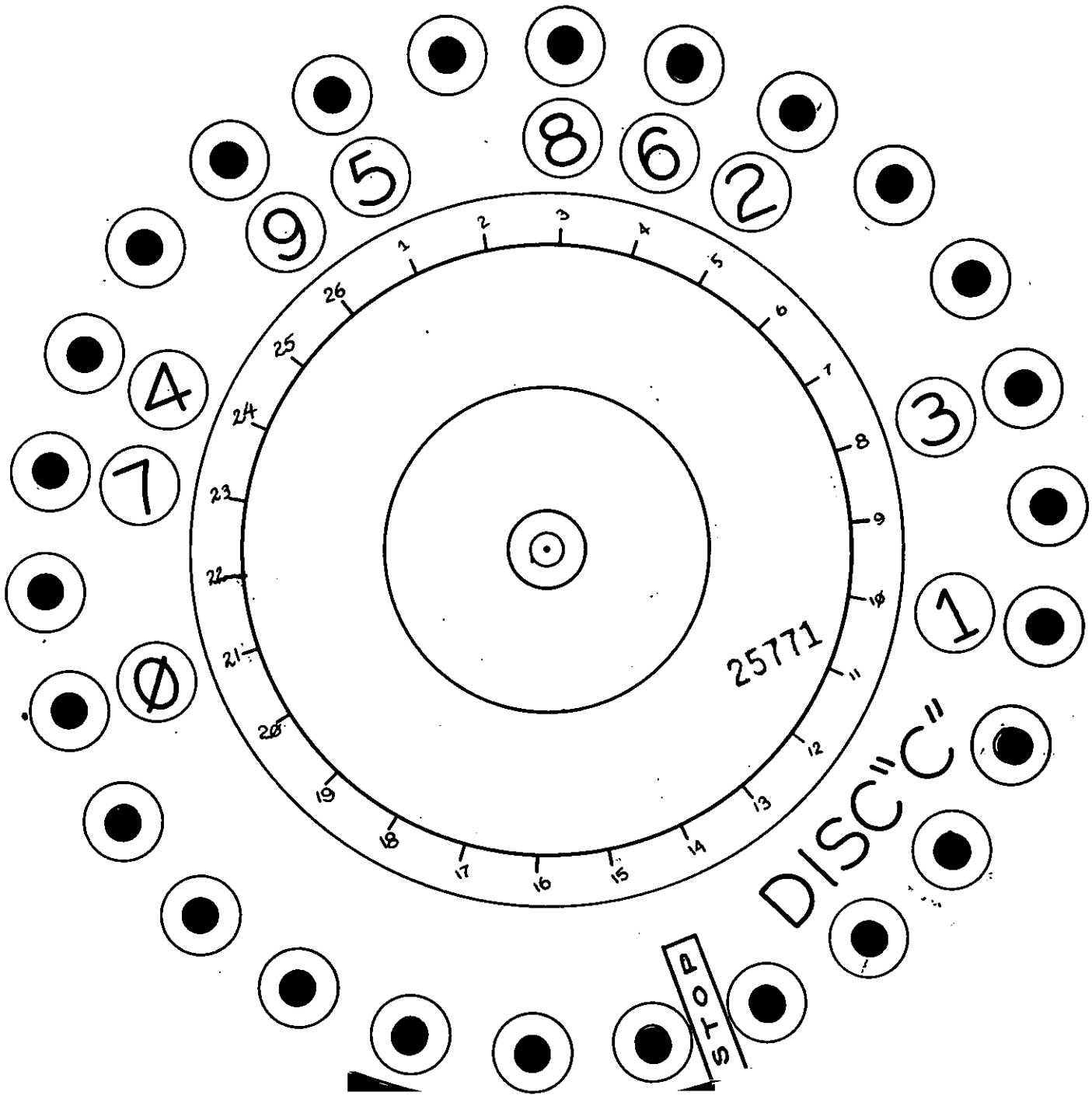
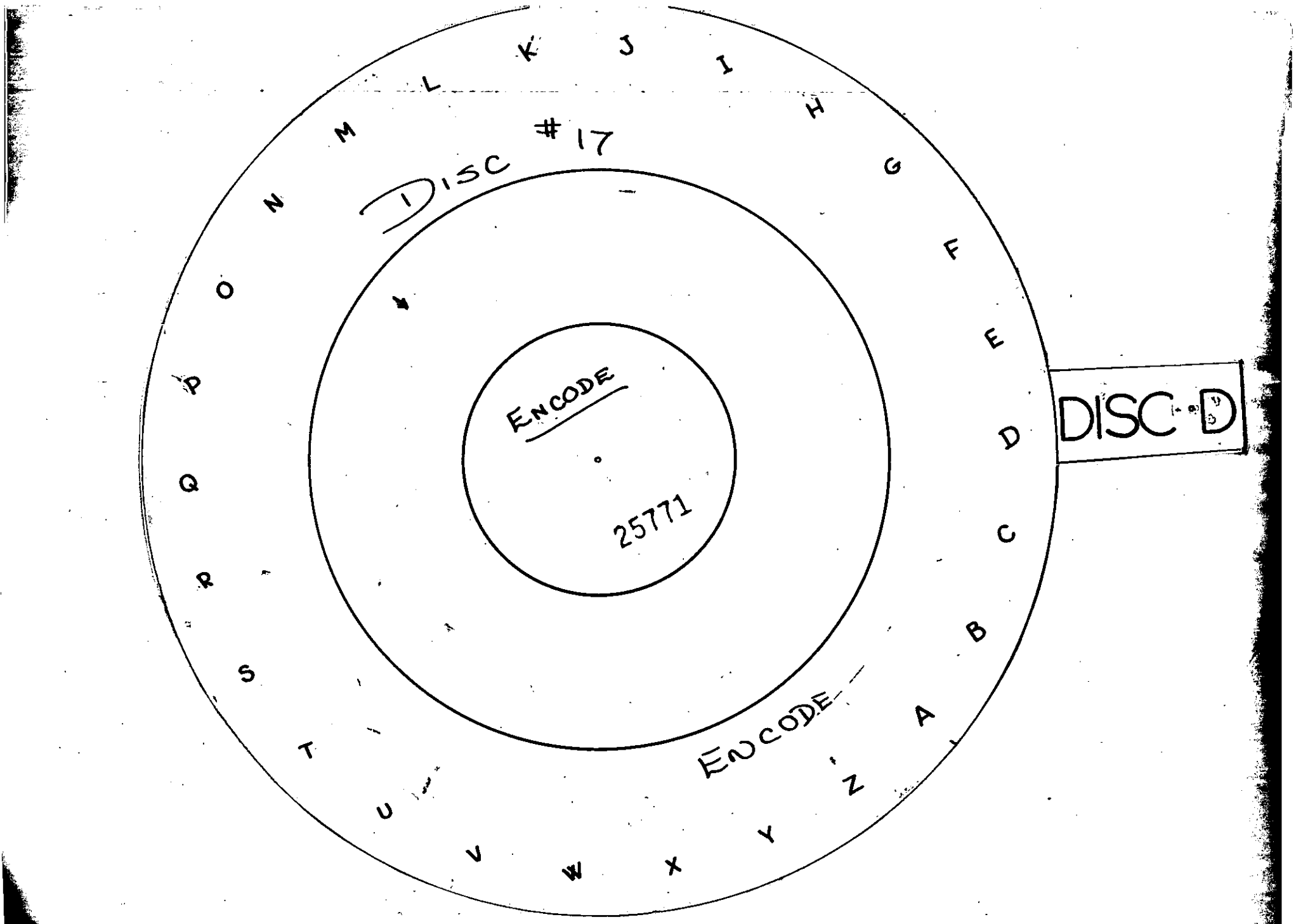
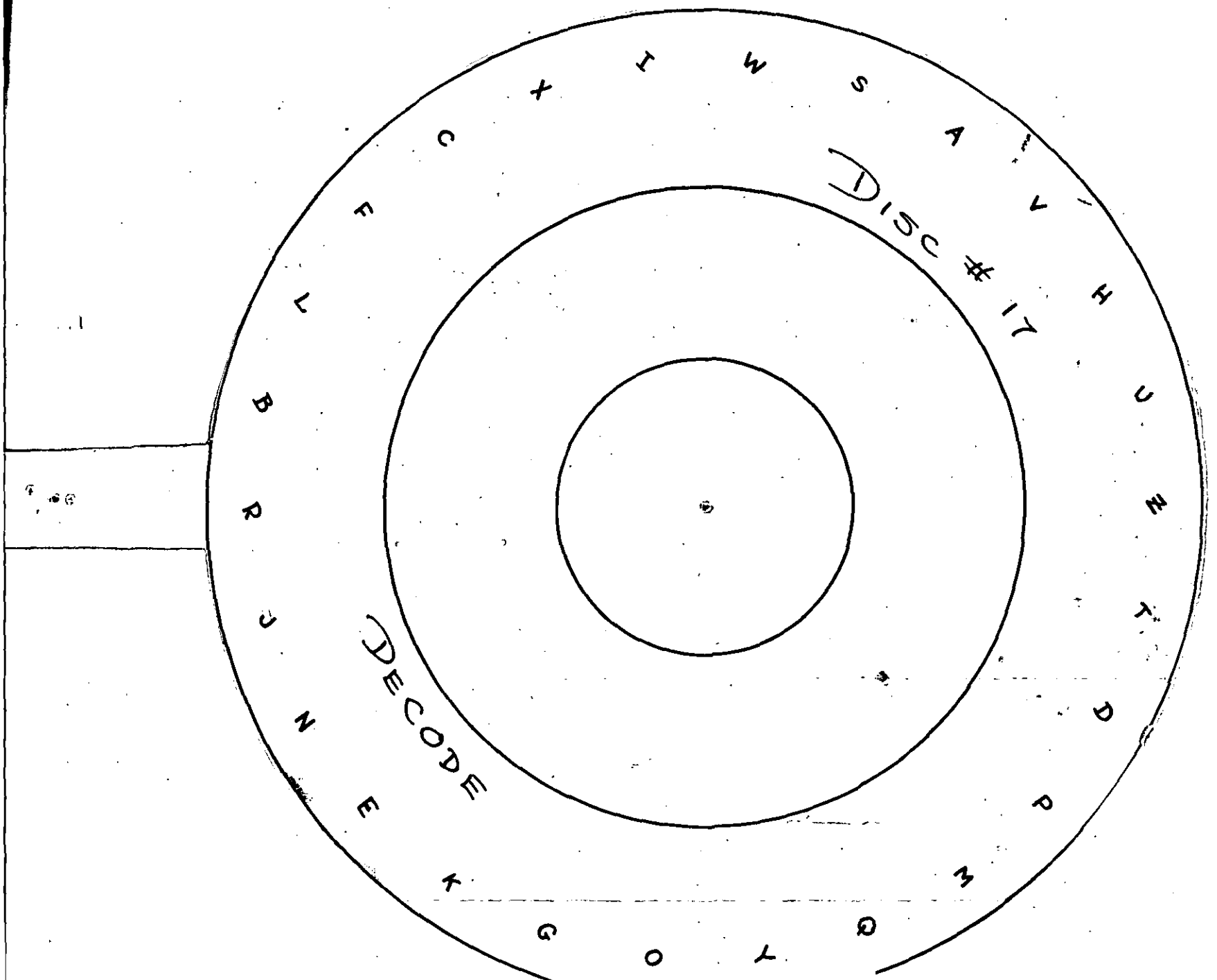


Declassified and approved for release by NSA on 07-16-2014 pursuant to E.O. 13526


DISC #17
ENCODE
25771
ENCODE
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
DISC D


Disc #17
DECODE
A V H U Z T D P M Q Y O G K E N J R B L F C X I W S

REF ID:A3079835

To Mr. Friedman with my compliments
and in due humility
Stu Tiltman
April 10. 1942

DOCID: A3079835

SECURITY

Copy No. 88

~~SECRET~~

S.I. COURSE

VOL. I

EXPLANATORY TEXT AND SHORT EXERCISES

Declassified and approved for release by NSA on 07-16-2014 pursuant to E.O. 13526

Col. Tiltman's
S. I.
Course

~~SECRET~~

REF ID:A3079835

S.I. COURSE

VOL. I

EXPLANATORY TEXT AND SHORT EXERCISES

SECTION I.—SUBSTITUTION.

SECTION II.—TRANSPOSITION.

(A) Simple Transposition.

(B) Double Transposition.

SUPPLEMENTARY EXERCISES.—A–M.

SECTION III.—PLAYFAIR.

SECTION IV.—COMPLEX SUBSTITUTION.

SUPPLEMENTARY EXERCISES.—INTRODUCTORY TEXTS N P.

SECTION V.—MACHINE.

ID:A3079835

SECTION I.—SUBSTITUTION

Figure 1 gives a passage of narrative English consisting of 340 letters. The division between words is not marked.

Recurring sequences of five or more consecutive letters are underlined.

Figure 2 shows graphically the number of occurrences of each letter of the alphabet. Figure 3 gives the number of occurrences again. Figure 4 the percentage frequency to the nearest whole number. In figure 5 the letters of the alphabet are rearranged in order of frequency. Figure 6 gives the percentage of the total confined to the vowels A, E, I, O and U.

Figure 7 gives graphically the bigram frequency, *i.e.* the number of occurrences of pairs of letters in sequence. For example, the figure shows that the "bigram" IN occurs seven times in the given passage.

Figure 8 gives the same information as figure 7 in a different form for the letters A, R and N. For example, it shows that A is preceded by C five times and followed by C once.

All the information contained in figures 2, 3, 4, 5, 6 and 8 can be derived from the bigram frequency table in figure 7. This form of frequency table is widely used in cryptography.

In figure 9 the passage given in figure 1 has been enciphered by the method of "simple alphabet substitution," *i.e.* a table giving a single letter equivalent for each letter of the alphabet has been used.

Thus the letter T at each occurrence is represented by W, H by K, etc. It will be seen from the underlined sequences that the recurrences of the original have been preserved. Figure 10 gives the number of occurrences of each letter of the alphabet in figure 9 and it will be seen that the frequency of the letters has also been preserved. In fact each letter of the clear text has been represented by the letter lying three places later in the alphabet. Thus H in the cipher version represents E in the clear text and has the same frequency. Note that Y is represented by B: this is because the alphabet is treated as cyclic. It might be said that the frequency table in figure 10 preserves the frequency pattern of the original text.

In figure 11 the passage in figure 1 has been enciphered again by the method of "simple alphabet substitution," but here there is a two-figure equivalent for each letter instead of a single-letter equivalent.

Here again the recurrences of the original text have been preserved. Figure 12 gives the number of occurrences of each pair of figures and its clear equivalent. It will be seen that the frequency of the original is still preserved but the pair equivalents for the letters in alphabetical order are not in numerical order. Such a shuffled table is frequently referred to as "hatted." In figure 13 the substitution table is rearranged to show the letters in alphabetical order. The table in figure 13 may be described as the "encipher" and that in figure 12 as the "decipher."

In the two examples of cipher so far given the "unit of substitution" is one letter and two figures respectively. The unit of substitution can, of course, be three or more figures or two or more letters or symbols of any kind, provided that no confusion between the various cipher equivalents is caused.

Exercise 1.—List all recurrences of three or more letters in figure 9 giving the "interval" between the various examples of the same recurrence. As an example of the form which the "interval" should take in your list, take the sequence F X U U H Q which occurs twice in the first line. The first letter of the sequence F

REF ID:A3079835

in the two occurrences is respectively the sixth and the twenty-fourth letter of the cipher text. The interval will be 24 – 6, *i.e.* 18.

Figure 14 gives still another cipher version of the text in figure 1.

Exercise 2.—Examine figure 14 for recurrences of 3 or more letters. Note that here some of the recurrences of the original text have been lost. List the intervals from all the recurrences observed. Figure 15 gives in graphic form the frequency table in figure 14. It will be observed that the frequency of the original text is here partially blurred. In the original text the letter E occurred 42 times and 5 letters did not occur at all. Here the commonest letter G occurs only 33 times and only one letter does not occur.

Exercise 3.—Compare the intervals obtained in Exercise 2 with those listed in Exercise 1. Observe that all recurrences have been preserved where the intervals are even and lost where the intervals are odd.

Figure 16 gives two separate frequency tables, I for letters occupying odd positions in figure 14, and II for those occupying even positions.

Exercise 4.—Now compare the clear text in figure 1 with the cipher text in figure 14 in conjunction with figure 16, and describe shortly the method of encipherment employed.

The unit of substitution in figure 14 is still one letter but the method is no longer " simple alphabetical substitution " ; it can be described as " periodic substitution," and the period is two letters.

Exercise 5.—Solve the following cipher text which has been enciphered by the method of " simple alphabet substitution." The clear text starts with the word " possession." (N.B.—The fact that the text is divided into 5 figure groups has nothing to do with the " unit of substitution." Messages sent by cable or W/T are most frequently transmitted in 5 letter or 5 figure groups.)

28827	73213	21167	32132	12112	77266	00021	13210	00343
32134	31232	44244	38700	02662	11266	16700	02882	77211
26633	23210	00277	17800	03322	00167	00024	41233	65000

Exercise 6.—The following cipher text represents the same clear text as in Exercise 5. Find the method of encipherment.

18172	12172	12111	17160	11210	23212	33141	42701	61116
70181	71116	22210	17802	21070	14325			

Figure 17 gives a cipher text of 280 figures. The clear text is not that of figure 1.

If the cipher text is cut up into pairs on the assumption that the unit of substitution is 2 figures, it will be seen that the pairs are limited to the numbers from 01 to 44, providing a fair check of the original assumption. Figure 18 gives in tabular form the analysis for 2- and 3-pair recurrences. Take for example the pair 23. The table shows that it occurs 4 times in the text, that when it occurs as the third pair it is followed by 38, 11, and that when it is the fifty-fourth pair it is followed by 18, 22, etc.

Figure 19 gives the 3-pair recurrences derived from figure 18. It will be seen that there are five such recurrences and that 7 is the highest common factor of the five intervals.

In figure 20 the pairs of the cipher text are written out in seven columns.

REF ID:A3079835

Figure 21 gives the frequency table for each of the columns separately. In any particular column the number of pairs is small and the count correspondingly unsatisfactory, but the patterns of the columns suggest that each column has its own "simple alphabet substitution" and that the order of the alphabet is preserved.

Figure 22 gives the result of the attempt to equate the cipher units of the seven columns to the same base by sliding according to the pattern. The right-hand column of the figure 22 gives the total number of occurrences in each line and should therefore give the frequency of the letters of the original text.

Exercise 7.—From figure 18 list the 2 pair recurrences and their intervals and observe how many of these recurrences have the period of seven pairs and how many are accidental. Go carefully again over the workings given in figures 17 to 22 and solve the text of figure 17.

Exercise 8.—Solve the cipher text in figure 23.

Exercise 9.—The clear original of the cipher text in figure 24 is the same as that given in figure 1 but in the simple table used for enciphering the whole range of pairs from 00 to 99 is used to represent not only the letters of the alphabet but also common syllables and words. Reconstruct the table as far as you can. Make a frequency table from the pairs of figure 24. You will see that the pattern of the frequency table is far less distinctive than that in the case of simple alphabet substitution.

Figure 25 gives a text enciphered by means of periodic substitution on the basis of the syllabic table you have derived from figure 24. The unit of substitution is the pair of figures. The period has already been found to be 4 pairs and the text has consequently been written in 4 columns. Two long recurrences on the period are underlined.

Figure 26 gives 4 bigram counts each giving the occurrences of pairs in the respective columns together with the pair appearing on the right in each case. For example the second and third pairs of the text are 06 38 ; 38 will be found in line 0, column 6 of Table 2. (N.B.—The expression "bigram count," normally used of 2 letters, is here used of 4 figures as the unit of analysis is 2 units of substitution.)

In contradistinction to the simply sliding pattern of figure 21 (*q.v.*), where the whole range of possible units is taken up in the basic substitution (*i.e.*, 26 letters or 100 pairs of figures) it is usual to treat the alphabet from A to Z or the numerical digits from 0 to 9 as cyclic.

The result of this is that, for example, X slid 4 places down the alphabet becomes B, the digit 7 slid 5 places down a series of digits 0–9 becomes 2, the digit 4 slid 9 places becomes 3, and the pair 74 slid 59 places down a series of pairs 00–99 becomes 23. This is obvious in the case of letters but may require further explanation in the case of figures where it is equivalent to "non-carrying addition." The arithmetical sum of 74 and 59 is 133, whereas it might be said that the "cryptographic sum" of 74 and 59 is 23.

REF ID:A3079835

Figure 27 gives what is known as the Vigenère table, an old type of cipher equivalent to the sliding alphabet type. Its use is exemplified below :—

To encipher the sentence " GONE WITH THE WIND " on the key word " NOBLE," write the letters of the key word as many times as required under the clear text :—

GONE WITH THE WIND
NOBL ENOB LEN OBLE

Look up in the Vigenère table the letter at the interesection of the line having G at the left and the column having N at the top. This gives the requisite cipher letter. The same result is obtained by looking up the letter at the intersection of the line having N at the left and the column having G at the top.

The cipher version will be :—

TCOPAVHIELRKJYH

The operation may be expressed algebraically :—

G + N = T
O + O = C
N + B = O, etc.

Exercise 10.—Encipher and decipher a sentence of about 20 letters according to the Vigenère system to satisfy yourself that you understand it thoroughly.

Figure 28 gives the digital equivalent of the Vigenère table. Inspection of the table will show that encipherment on this table is equivalent to " non-carrying addition."

Now examine again the cipher passage in figure 25 and its analysis in figure 26 ; as the frequency of the syllabic table is much less distinctive than a simple alphabet substitution, it may be difficult to equate the 4 columns on evidence of pattern alone. There is, however, a direct method of equating the columns where the period is very short. It will be found to be applicable in this case.

The pairs resulting from the subtraction (without carrying) of each pair from the pair 4 later than it (*i.e.*, at period distance from it) are written down in 4 columns. Figure 29 gives this result. You will notice that the recurrence 67 72 89 occurs four times, twice starting in column 4 and once each in columns 2 and 1. The two recurring sequences starting in column 4 correspond to a recurrence in the cipher text (*see* figure 25) ; the sequence in line 55 (of figure 29) and the shorter sequence 67 72 in line 3 also correspond to recurrences in the cipher text.

The purpose of this sort of analysis may perhaps be best understood when treated algebraically. Imagine a series representing consecutive clear units a, b, c, d, e, f, etc., enciphered on a recurring key w, x, y, z. The cipher versions can then be expressed as :— a + w, b + x, c + y, d + z, e + w, f + x, etc. The series obtained in figure 29 is equivalent to :—

e + w − (a + w), *i.e.*, e − a,
f + x − (b + x), *i.e.*, f − b, etc.

Thus it will be seen that any recurrence of n consecutive clear units will be revealed as a recurrence of $n - 4$ consecutive terms in a table such as figure 29.

REF ID:A3079835

Compare the recurring sequences in figure 29 with the cipher text in figure 25. They will be found to have resulted from the following passages :—

A.		91	93	01
	39	58	65	
B.		91	93	01
	39	58	65	80
C.				18
	74	84	58	75
	46	63		
D.				18
	74	84	58	75
	46	63		
E.	67	08	79	80
	24	70	58	

These 5 passages can be assumed to represent a 7-unit recurrence in the clear text starting in 3 different positions in the period (presumably the last letter is missing in A). Leave column 1 untouched, *i.e.*, assume that the first clear unit of the recurrence is 67. The other versions of the recurrence in columns 2 and 4 start with 91 and 18 respectively.

To reduce these to 67 it will be necessary to subtract (non-carrying) 34 and 51. These provisional " subtractors " when applied to the whole of their corresponding columns give the following result :—

	00	34	..	51
A.		67	..	50
	39	24	..	
B.		67	..	50
	39	24	..	39
C.				67
	74	50	..	24
	46	39		
D.				67
	74	50	..	24
	46	39		
E.	67	74	..	39
	24	46	..	

Exercise 11.—Find the provisional subtractor for column 3. You are now in a position to reduce the whole of figure 25 to one common base. Find the correction necessary to reduce the whole to the true figures of the syllabic table reconstructed in Exercise 9.

The above is only one of the methods which might have been employed to solve the cipher text in figure 25. In this case it is probably the most direct, but ciphers with such a short period are very vulnerable and when the period is longer than the normal length of recurrences this method would be useless.

REF ID:A3079835

Other methods which might have been employed are :—

(i) Reduction of the columns to a common base by fitting the frequency patterns.

(ii) Finding provisional subtractors for each of the columns which would equate the common pairs in them to common units of the syllabic table (which, in this case, has been partially reconstructed).

It cannot be emphasised too often that the proper method of solving a cipher is the shortest, and that it is the business of the cryptographer to proceed as rapidly as possible by experiment, devising at each stage new methods of approach based on the features observed.

Exercise 12.—Solve the cipher employed in the six cipher texts of figure 30. The clear texts are passages of narrative English taken from a book on meteorology. You will have to analyse the texts for recurrences and list the intervals between them, being careful to distinguish between internal recurrences (*i.e.*, those within one of the texts) and external recurrences (*i.e.*, those which connect two texts). But, before doing so, read through the cipher texts ; a preliminary cursory examination is always advisable and it may save you much trouble if you can recognise any non-textual groups inserted at prearranged places as key-indicators or check groups. (Such non-textual groups will always be fairly obvious at this stage of the course.)

REF ID:A3079835

SECTION II.—TRANSPOSITION

(A) Simple Transposition

Figure 1 gives a cipher text sent in 8 parts, the first 7 each containing 55 letters, and the eighth the remaining 12 letters. Figure 2 gives the frequency count which is clearly the count of unaltered English letters. Some method of transposition of the letters is therefore employed. It is a justifiable assumption that, as the first 7 parts are of the same length, the system of transposition is identical for all of them. The first 7 parts are therefore written under one another, and the columns numbered as in figure 1.

Consider the letter Q which is the 42nd letter of the 7th part. This ought to be followed in the clear text by U, and there happens to be only one U in the 7th part. Below will be found columns 42 and 41 of Figure 1.

42	41
E	R
O	N
W	T
T	S
H	E
E	D
Q	U

If Q and U are consecutive letters in the clear text of the 7th part, then the pairs of letters shown above should also be next to one another in the other parts. On the basis of these two columns, by trial and error, the following collection of columns is put together :—

18	2	49	13	28	42	41
A	N	U	M	B	E	R
N	S	A	T	I	O	N
A	Y	G	R	O	W	T
U	R	R	E	N	T	S
L	Y	T	O	T	H	E
E	L	O	P	P	E	D
S	O	F	R	E	Q	U

This is the process known as "anagramming". Once a start has been made it is not usually difficult to complete the text, given sufficient "depth", "depth" being defined as the number of texts of equal length to which the process is applied. For instance it will be seen at once that the next column to be added on the left should have M as the 3rd letter, C as the 4th, and V as the 6th. Column 33 will be found to fit.

Figure 3 shows a further stage of the process of anagramming. An attempt might now be made to find if there is any system revealed in the "anagram key", *i.e.* the series of column numbers in the anagram order.

Figure 4 shows the effect of arranging the "anagram key" on a series of different levels so that each level contains only consecutive numbers. The progression revealed can be used to carry the anagram further. For example, the next numbers to the left in the anagram key should be 51 4 20 34 21. Upon examination it is found that the first four of these are correct, but that column 21 is not correct. So a fresh start has to be made.

REF ID:A3079835

Exercise 1.—Complete the anagram.

Figure 5 shows the extension of figure 4 when the anagram key is completed. At the right-hand side, the levels have been numbered in numerical order, *i.e.* level 1 contains the numbers 1, 2, 3, 4, 5 and 6, level 2 contains 7, 8 and 9, level 3 contains 10, 11, 12, 13, 14, 15, 16 and 17, etc.

Take level 8—it contains the numbers 37 to 46; these are the 37th to the 46th cipher letters and they are the 55th, 54th, 50th, 49th, 41st, 40th, 28th, 27th, 11th and 10th letters of the clear text. Figure 6 is built up in this way and shows the original method of transposition—the "routing" is shown more clearly in figure 7.

Exercise 2.—What is the clear text of part 8?

The series 8 6 3 9 1 4 7 2 10 5 is known as the "transposition key". The diagonal "routing" is one of the innumerable geometrical transposition systems.

The original diagnosis of the system of transposition is often extremely difficult, and successful "anagramming" is the basis of all cryptography in this field.

The commonest of all systems of transposition is that known as "simple transposition". Here the text to be enciphered is written horizontally under a key and the cipher text consists of the columns so obtained written horizontally in the numerical order of the numbers, starting at the head of them. The example below gives a clear text written under a key :—

Transposition key :	5	2	6	4	1	3
Clear text :	T	H	E	C	A	P
	T	A	I	N	S	A
	N	D	T	H	E	K
	I	N	G	S	D	E
	P	A	R	T		

The cipher text will be :— ASEDH ADNAP AKECN HSTTT NIPEI TGR.

The decipherer reverses the process, but he has to construct the frame required to fit the key, and the number of cipher letters received.

Transposition keys are frequently derived from memorizable words or phrases or from sentences from a book. The normal method is to number the letters from left to right in alphabetical order. For example, the key phrase :—

	L	I	T	T	L	E	A	P	P	L	E	S
gives the key :	5	4	11	12	6	2	1	8	9	7	3	10

The feature of "recurrence" does not normally occur in transposition systems, but there are certain circumstances in which recurrences can be found and used. In simple transposition two of the most useful of these cases are :—

(*a*) where the same message is enciphered twice on two different keys of the same length, and

(*b*) where two messages enciphered on the same key contain the same clear passage (at least twice as long as the key) starting at the same column in the "cage". (This word is sometimes used to express the shape of a text when written under the transposition key.)

In figure 8 will be found three clear texts written under their transposition keys. Cages 1 and 2 have the same clear text, but the transposition keys are different, though of the same length. Cages 2 and 3 have the same transposition key and the

REF ID:A3079835

first 31 letters of the two clear texts are identical. (It will be realised that the commonest place for case (*b*) to occur is at the beginning of texts.)

In figure 9 the cipher versions are given in a form suitable for displaying the recurrences. It will be seen that the recurrences are portions of columns in the original cages, and that they do not represent consecutive passages of the clear text, but are series of clear letters, the key length apart.

Figure 10 shows the recurring portions between cipher texts 1 and 2; these are the columns of cage 1 rearranged in cage 2.

It will be seen that from figures 9 and 10 the key length 8 can be deduced, either by comparing cipher texts 1 and 2 or 2 and 3.

From any of the three cipher texts the clear text could be obtained by rearranging, as columns, the portions marked off in figure 9. It is very important to notice here the part played in reconstruction by the grouping of all long columns to the left of the cage and short columns to the right. In the system of simple transposition the last lines of cages are hardly ever completed so as to make the cages into " perfect rectangles." The latter only occur by chance and instructions are sometimes issued with a view to avoiding them.

Exercise 3.—In figure 11 will be found two cipher versions of the same clear text, one letter of the clear having been omitted in the first encipherment. Take a frequency count of the two messages in order to decide what the missing letter is. Examine the two texts for recurrences between them and find the clear text.

Figure 12 is intended to demonstrate the approach to solution of simple transposition ciphers by making use of stereotyped beginnings of the clear texts. The five cipher texts shown are five parts of the same clear text, all except the first starting with the word " continuation." The texts vary in length from 45 to 71 letters; the numbers from 45 to 71 have been written down in a column on the left hand side, and each of the cipher texts has been written out opposite to the number representing its length, *i.e.*, part 2 which has 52 letters is written in line 52, etc. The radial lines divide each text into 11 equal parts. It will be seen that near each dividing line the same letter occurs in parts 2, 3, 4 and 5. These letters are the letters of the word " continuation " and lie at the heads of columns in the original transposition cage. In fact, from the letters occurring at proportional positions in parts 2, 3, 4 and 5 of the cipher text, the key-length 11 could have been found.

This proportional method of writing out cipher texts on the same transposition key has wide applications in the solution of transposition systems.

Exercise 4.—Solve the texts in figure 12.

Figure 13 shows the classical method of treatment, known as the " hat," of simple transposition texts where the cage is not a perfect rectangle and the key-length is known or assumed. The five diagrams give this effect of the five parts of figure 12. Here the key-length is in each case 11, and as a result of the incidence of long and short columns those letters which might belong to either of two adjacent columns are shown twice. The thin lines enclose the columns on the assumption that all the long columns are at the right of the cage—the thick lines enclose the columns on the assumption that the long columns are all on the left.

Such " hat " figures are, of course, quite independent of the text—they are dependent only on the number of letters in the text and the key-length.

Figure 14 is a diagrammatic representation of the column limits for the key-length 10, and text lengths from 40 to 75. This arrangement is similar to that of figure 12, while the thin and thick lines have the same meaning as those in figure 13. Figure 15 shows the effect of superimposing a similar hat-diagram (but this time for the key-length 11) on the texts of figure 12.

REF ID:A3079835

Exercise 5. Make a careful comparison of figures 12 to 15 and make sure that you understand the various aspects displayed. You will notice that the radial lines of figure 12 have become lines expressing probability (of the positions of the column-heads) in figures 14 and 15. Consider how you would draw similar lines of probability in the hat-diagrams of figure 13.

To digress for the moment from the main line of argument, it has been stated *above* that transposition keys are frequently derived from memorizable key-words or phrases or from lines chosen at random from a prearranged book. The conventional method of forming a key from text has also been shown. It is sometimes necessary to attempt to find out the textual source of keys. The solution is much easier where the key is a long one, *i.e.* at least 25 terms. It is advisable to lay out the key in diagrammatic form as in figure 16.

It will be seen that the method of writing the key out has been to write down the numbers of the key in numerical order from left to right and to drop to a lower line every time it is necessary to go back to the left. As the occurrences of each letter are numbered from left to right, it follows that in figure 16 numbers on two different lines cannot represent the same letter. There must be at least 13 different letters represented in the key. A start is made by assuming that the occurrences of the letter E are represented by two or more consecutive numbers from the series 5, 6, 7, 8. If this is so, then 1 and 2 can only represent B, C or D, etc. The word THE might well be represented twice by 28 12 5 and 30 13 7. Then 9, 10 and 11 must be F or G and 29 must be T.

Exercise 6.—Find the sentence of English poetry represented by the key in figure 16.

Exercise 7.—Attempt to find the sentences of English poetry represented by the 10 keys given in figure 17.

The solution of simple transposition ciphers in the case where there is a different key for each text is chiefly a matter of experience and cannot be taught as a process within this course. But an example will demonstrate the general lines of work Figure 18 (A) gives a piece of narrative text enciphered by means of simple transposition. Figure 18 (B) shows 3 columns fitted together by trial and error without assuming any particular key-length. The trigrams enclosed between the two horizontal lines look correct.

Exercise 8.—Complete the solution of the text in figure 18 (A) by—

(*a*) finding the key-length, and

(*b*) constructing the " hat " diagram.

Exercise 9.—Figure 19 gives the " anagram keys " of five texts each enciphered by different processes of transposition. In each case find the method of encipherment. You may find it easier to work from the " encipher key " instead of from the " anagram key." The text following Exercise 12 describes how to form the one from the other.

Exercise 10.—Devise a transposition cipher to be used under the following conditions :—

(*a*) The cipher is to be used between an agent abroad and his headquarters at home.

(*b*) They will be out of touch with one another for at least a month.

REF ID:A3079835

(*c*) Each holder may be expected to send not more than one message a day of not more than 100 letters.

(*d*) The cipher should be as far as possible secure.

(*e*) The agent must be able to memorise the cipher completely and must not carry any compromising papers.

Give short but complete directions for enciphering and deciphering.

Exercise 11. Is there any method by which the headquarters can convey to the agent, in the cipher which you devised in the last exercise, instructions to change the cipher with a view to re-establishing security on the assumption that your cipher has been compromised?

Write out on paper your solutions of Exercises 10 and 11, and hand in to the instructor.

REF ID:A3079835

SECTION II

(B) Double Transposition

A far more secure system of transposition than any which has appeared so far in this section is that of "double transposition." Here there are two processes, each of simple transposition, either on the same key or on two different keys. In enciphering, what would have been the cipher version after simple transposition is written horizontally under the second key and taken out column by column according to that key.

Figure 20 gives two examples :—

(*a*) in which the same transposition key is used twice, and

(*b*) in which two different keys are used.

Exercise 12.—Make up an example for yourself so as to understand thoroughly the process of encipherment and decipherment.

Generally speaking the only method of solving double transposition is by anagramming either completely or partially, two or more texts of the same length.

Below will be found the complete anagram key of a text enciphered by double transposition. The following is a rapid method of reconstructing the transposition key or keys, given the complete anagram key. The method is applicable whether one key is used twice or two different keys are used.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
11	1	10	18	8	17	7	26	9	25	6	33	5	32	23
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
24	22	31	16	30	15	29	21	28	14	4	13	3	20	27
31	32	33												
19	2	12												

Numbers in the above series, the anagram key, represent the numbered positions of the text in the cipher order arranged according to their position in the clear text, *e.g.* the first number in the series, *i.e.* 11, means the eleventh letter in the cipher order and it is the first letter of the clear text.

Below is another series, the indexed version of the above :—

2	32	28	26	13	11	7	5	9	3	1	33
27	25	21	19	6	4	31	29	23	17	15	16
10	8	30	24	22	20	18	14	12			

The first term, *i.e.* 2, means the second clear letter which occupies the first position in the cipher order. To distinguish this series from the anagram key, it will be described here as the "encipher key."

From this series is derived a further series, here termed the "interval key." This gives the intervals, positive or negative, between consecutive terms of the encipher key.

+30	−4	−2	−13	−2	−4	−2	+4
−6	−2	+32	−6	−2	−4	−2	−13
−2	+27	−2	−6	−6	−2	+1	−6
−2	+22	−6	−2	−2	−2	−4	−2

REF ID:A3079835

The three occurrences of the sequence −2, −4, −2 are derived from the following sequences in the encipher key :—

	13	11	7	5
	27	25	21	19
and	20	18	14	12

These sequences are better arranged as follows :

13	11	7	5
20	18	14	12
27	25	21	19

The constant difference 7 between each number of the above figure and the one below it will be noted. That this must be the key-length of the first transposition key will be understood if the first cage is made up on this assumption.

1	2	3	4	**5**	6	**7**
8	9	10	**11**	**12**	**13**	**14**
15	16	17	**18**	**19**	**20**	**21**
22	23	24	**25**	26	**27**	28
29	30	31	32	33		

The four columns of the earlier figure :—

13	11	7	5
20	18	14	12
27	25	21	19

are now seen as portions of columns in the first cage.

In fact the 12 numbers concerned lie in the following positions :—

		5	7
11	12	13	14
18	19	20	21
25		27	

in the first cage, and in the positions :—

13	20	27
11	18	25
7	14	21
5	12	19

in the second cage, of which the transposition key-length is still unknown.

The block of the second cage just reconstructed can now be extended as follows :—

6	13	20	27		
4	11	18	25	32	
	7	14	21	28	
	5	12	19	26	33

REF ID:A3079835

The next extension of the second cage is obtained by completing the partial columns of the above figure from the encipher order :—

6	13	20	27	2	9
4	11	18	25	32	3
31	7	14	21	28	1
29	5	12	19	26	33

Now the earlier process can be repeated by extending the lines to include the complete columns of the first cage :—

				6	13	20	27	2	9	16	23	30
				4	11	18	25	32	3	10	17	24	31
3	10	17	24	31	7	14	21	28	1	8	15	22	29
1	8	15	22	29	5	12	19	26	33				

Exercise 13.—Complete the solution, *i.e.*, find the two transposition keys.

There is an alternative method of solution working only from the anagram key, but it is dependent on knowledge of the key-length of the first transposition key. In the problem solved above it is necessary to go back to the point at which it was established that the first key-length was 7.

The anagram key is written out in the appropriate cage as follows :—

11	1	10	18	8	17	7
26	9	25	6	33	5	32
23	24	22	31	16	30	15
29	21	28	14	4	13	3
20	27	19	2	12		

The key-length of the second transposition key is unknown but working from the anagram key the second cage will have an appearance similar to the following :—

6	17	28	23	1	12
7	18	29	24	2	13
8	19	30	25	3	14
9	20	31	26	4	15
10	21	32	27	5	16
11	22	33			

i.e., the columns will consist of consecutive numbers reading downwards. The lines will be composed of the columns of the first transposition cage. The columns of the first cage can be fitted together in lines to form part of the second cage as follows : –

	1	9	24	21	27	
		10	25	22	28	19
		11	26	23	29	20
and	17	5	30	13		
	18	6	31	14	2	
		7	32	15	3	
		8	33	16	4	12

Exercise 14.—Find the two transposition keys.

Exercise 15.—Find the two transposition keys from the following anagram key :—

3	1	2	27	25	26	28	21	19	20	6	4	5
7	14	12	13	10	8	9	11	24	22	23	17	15
16	18	31	29	30								

REF ID:A3079835

In figure 21 an anagram key is given and the diagram below it shows it as it appears in its two cages. Certain recurring features, known as "rhythms," are underlined. It will be seen that the terms thinly underlined conform to a recurring pattern :—

6	5	.	.	.	7
27	26	.	.	.	28
15	14	.	.	.	16
2	1				

The interval at which the pattern recurs is 9, *i.e.*, the first key-length. The first key-length is also revealed by the terms thickly underlined. It will further be observed that the terms entering into these "rhythms" are derived from columns of the second cage. Thus 6, 5 and 7 belong to one column of the 2nd cage, but 3 is not in the same column.

This feature of "rhythm" can always be used to find the first key-length, and is particularly valuable in cases where the anagram key is incomplete.

The following are the first 63 terms of the anagram key for a text 140 letters long :—

26	**29**	66	**32**	130	127	42	97	86
11	14	94	33	6	3	65	89	62
59	**67**	**70**	17	**73**	80	77	83	56
37	118	121	53	124	138	135	49	40
46	43	**18**	**21**	91	**24**	105	102	34
7	128	27	30	4	74	113	110	90
131	87	84	**92**	**95**	50	**98**	15	12

This partial anagram key is full of rhythms but those shown are sufficient to prove conclusively that the first key-length is 19. The partial anagram key is now written out again in a cage for a key-length 19 and text length 140 as follows :—

26	**29**	66	**32**	130	127	42	97	86	11	14	94	33	6	3	65	89	62	59
67	**70**	17	**73**	80	77	83	56	37	118	121	53	124	138	135	49	40	46	43
18	**21**	91	**24**	105	102	34	7	128	27	30	4	74	113	110	90	131	87	84
92	**95**	50	**98**	15	12	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.												

The incomplete columns of the above figure are fitted together in lines to form the second cage :—

33	124	74	.	.	.	.	66	17	91	50	.	.	.	.	42	83
34	.	.	.	.	.	26	67	18	92	.	.	.	.	59	43	84
.	.	.	.	11	118	27	.	.	.	.	3	135	110	.	.	.
.	127	77	102	12	.	.	.	.	94	53	4	.	.	.	.	86
37	128	.	.	.	.	29	70	21	95	.	.	.	.	62	46	87
.	.	.	.	14	121	30	.	.	.	.	6	138	113	.	.	.
.	130	80	105	15	.	.	.	.	97	56	7	.	.	.	.	89
40	131	.	.	.	.	32	73	24	98	.	.	.	.	65	49	90
.	.	.	.													

REF ID:A3079835

Exercise 16.—Go carefully over the working of the above example and complete the solution by finding the two transposition keys.

Exercise 17.—In certain special, and rather uncommon circumstances, there are two or more possible solutions of a particular anagram key. Try to make up an example to illustrate this.

The above method of solution of a partial anagram key is only applicable where the number of consecutive terms exceeds the first key length by a number sufficient to supply recognisable rhythms. Solution can be achieved however in cases where much shorter partial anagram keys have been obtained for several different text lengths. In practice it may be taken for granted that short partial anagram keys will only be obtained either at the beginnings or at the ends of texts owing to the occurrence of stereotyped formulae due to addresses, opening references or signatures.

In the example in figures 22 and 23 it is assumed that five texts of lengths 65, 66, 69, 72 and 75 letters enciphered in the same pair of keys have been anagrammed for the first 12 letters.

Figure 22 gives the positions of the first 12 letters for each text in the second cages, or, from another aspect, the positions in the second cages of the heads of the twelve columns of the first cage. A careful study should be made of the manner in which the column heads move across the cage with increasing text-length, those in the upper part of the cage slowly and the others more rapidly according to their level in the cage.

Figure 23A shows the positions of the column heads of the first cage in the enciphered texts—the column heads of the second cage are also marked with vertical lines. Figure 23B gives the appropriate " hat-figure."

Figure 24 shows the method of using the above features, *i.e.* " maintenance of level " and progressions to the right across the second cage with increase of text-length. Figure 24 shows the positions in the final enciphered form of the first 10 letters of the text for lengths 42, 45, 46, 48 and 50 on a pair of keys. The following deductions can be made :—

(i) 3 remains in the same (proportional) position from 45 to 50 and is immediately preceded by 6 in 46 ; therefore 3 is at the head of a column in the second cage for all the lengths, and 6 is at the bottom of a column for lengths 42-46.

(ii) 3 has moved between 42 and 45 while 8 remains in the same relative position throughout ; therefore 8 is at the head of a column in the second cage and to the left of 3.

(iii) 7 remains in the same relative position in 48 and 50, and is immediately preceded by 2 in 50 ; therefore 7 is at the head of a column in the second cage for all lengths, and 2 is at the bottom of a column for all lengths. (The position of 2 at the bottom is checked in 46 where it is the last term of the series.)

(iv) 3 remains in the same relative position from 45 to 50, while 7 moves between 46 and 48 ; therefore 8, 3 and 7 appear in the top line of the second cage in that order. 8 probably occupies the top left-hand corner of the cage, which means that it lies immediately under the number 1 of the transposition key in the first cage, *i.e.* 1 is the 8th term of the first transposition key.

In figure 25 the above deductions are incorporated. The divisions between columns of the second cage are marked where established. It will be realised that the approximate positions of many more of the heads of columns can be deduced.

REF ID:A3079835

Figure 26 shows that the second key length must be 13. The actual transposition key can be deduced from the changes of column of the various numbers with change of text length. In the first place those numbers which are in different columns in 45 and 46 can only have moved one place to the right in the second cage. Therefore 4 pairs of adjacent terms in the second transposition key are known :

2	5,	derived	from	change	of	position	of	number	9 of the encipher key.
3	7,	,,	,,	,,	,,	,,	4	,,	,,
10	13,	,,	,,	,,	,,	,,	2	,,	,,
12	6,	,,	,,	,,	,,	,,	6	,,	,,

Now 2 changes from column 8 to column 10 between 42 and 45, therefore 8 must be to the left of 10 in the second cage and there cannot be more than 2 terms in between them. But 9 changes from column 5 to column 10 between 46 and 48 and 5 must therefore be to the left of 10 with not more than one term in between. It has been proved above that 2 is immediately to the left of 5 ; therefore part of the second key has been reconstructed :—

8 2 5 10 13

Exercise 18.—Find the two transposition keys.

One further aspect of double transposition deserves consideration. Figure 28 gives the encipher keys for the five consecutive lengths from 56 to 60 derived as shown in figure 27.

Figure 29 gives the corresponding anagram keys. Comparison of any two consecutive encipher keys in figure 28 reveals that the terms divide themselves into three classes :—

(*a*) The same term occurs in the same position.

(*b*) The same term occurs one place further to the right in the longer encipher key.

(*c*) There is no obvious relation.

In figure 28 in each encipher key after the first, terms which belong to class (*c*), when comparison is made with the encipher key above it, are dropped one line. It will be seen that the shift to the right in class (*b*) happens in the case of terms occurring in columns of the second cage, numbered higher than the last long column in the second cage (*i.e.* the column which changes from short to long when the text-length is increased by 1). As an example, for the length 57, the last long column in the second cage is 6, and all terms belonging to columns 7, 8, 9, etc. are of the class (*b*) or class (*c*) varieties. Class (*c*) terms are all those lying in the second cage after the number identical with the text-length. For example, for the length 57, the class (*c*) terms are 11, 24, 37, 50, 3, 16, 29, 42, 55, which lie after 57 in the second cage. (The number 57 which does not, of course, occur in the encipher key for text-length 56 need not be classified.)

Turning to the anagram key form in figure 29, the same three classes may be observed, but here class (*b*) terms are in the same position but numerically increased by 1. In figure 29 class (*b*) terms are **underlined in red,** while class (*c*) terms are dropped a line. For text-length 57 class (*a*) terms are all numbered 28 or less, while class (*b*) terms are numbered 30 or more. This is because the last number in the second cage, *i.e.* 55, is the 29th letter to be taken out of the cage.

Exercise 19.—Study the class (*c*) terms in figure 29 and find a rule to account for their displacement between consecutive anagram keys. In what circumstances could the aspect described above be used to a[illegible]t solution ?

Figure 30 shows the anagram keys for lengths 56 and 57 put through the cages.

REF ID:A3079835

SUPPLEMENTARY EXERCISES A– M

A. Below will be found three cipher messages each sent in three or more parts. It is known that the correspondents are known to one another by the names of common colours, and it is thought probable that the 2nd, 3rd, etc. parts of messages begin with the word "continuation." The texts of the messages are narrative English and apart from addresses or signatures, no attempt has been made to render the text realistic.

Decipher one of the messages :—

A/1	EREAL	RFNHR	FPTPK	EIOWT	ASAIN
	RRFHM	ONAIH	SEOGA	ODMAO	BCZEO
	IGTOS	HDNLB	CEETO		
A/2	ENCNY	NBNYN	HTOEO	ATEAD	AAAEN
	UNRHA	AMOSW	OICVI	HHDTR	TAEKH
	TMETD	NMLUA	AGSIA	NT	
A/3	PETES	ECERU	DHISI	NUSLD	AESWU
	NICEO	LRPSO	HTOAN	TPMUR	SFOSH
	TREAC	OGRNA	ROSEL		
B/1	BOCPR	MRSEH	EEONE	INDEG	TMRDE
	NRDLT	BMOTF	RRFAH	ODUFI	NAAEO
	EMRTF	ETFII	RSOFG	AO	
B/2	NKTOT	AHILM	LTOOG	OEACN	BOBIN
	UNDFR	NNODM	OICOI	BWNRD	OUUBM
	OANMR	ULAME	TACIA	NT	
B/3	PLTIS	TRNHT	PLILR	NPIDO	NSNTU
	NICEO	LRPIO	OTOAN	TPMUR	LFOSS
	OEITR	AEEOO	SSIAO		
C/1	EHDTT	UTOOE	PEOMC	LGLBI	IFLIO
	PRMAS	WTETS	TUFOH	REELE	NHHLA
	EAAFS	FNOAM	SBISL	RPA	
C/2	GSHAS	UFGOL	TCIAN	TOUHH	OSOLU
	NICEE	IESSO	MTOTY	MOACM	VREEO
	YCRRO	TOSPN	TOATU	N	
C/3	FITLA	NNALV	TONMO	OTPNS	AONUO
	OTIWR	IELPO	UYEEN	ICOAN	DHIDT
	KPTAH	ROTOW	N		
C/4	PASRH	NNRIJ	SHYMA	IHVHT	AEPUO
	HTIEE	NVHPI	WIUPN	IGOAA	OHOID
	TETLO	ISTGE	D		
C/5	TUENE	EDTIS	ONIAN	TIDOH	GMPTU
	NICWF	OSNJO	ITONO	BORRM	PJIPH
	SRAPA	EATVH	HIEUN	N	

REF ID:A3079835

B. Encipher Key :—

2 3 6 34 5 12 22 18 23 30 20 9 14 21 31 16 26 28 33 29 27 32 1 7 8 10 15 11 25 35 4 13 17 19 24. (Double transposition but not normal.)

C. Encipher Key :—

79 93 105 115 127 19 30 44 58 69 83 95 9 117 17 24 35 49 63 74 80 94 5 116 13 20 31 45 59 70 86 98 108 120 130 26 38 52 66 76 90 102 112 124 134 27 41 55 144 1 3 7 11 15 22 33 47 61 72 75 89 101 111 123 133 139 40 141 143 88 100 110 122 132 138 140 54 142 82 4 8 12 16 23 34 48 62 73 85 97 107 119 129 136 37 51 65 81 2 6 10 14 21 32 46 60 71 78 92 104 114 126 135 29 43 57 145 87 99 109 121 131 137 39 53 67 84 96 106 118 128 25 36 50 64 77 91 103 113 125 18 28 42 56 68.

D. Seven messages in an unknown cipher :—

1. TDEVE HNGRI EOGAH ROQBT NETLA
ROUPT HIITA STCPY KEMFA IREHN
TEYRA RTMTK OTKAO HAJGH RTOSF
RHSSP SNEEE ENOO

2. UDINE TNODR GENYG BTEEA LNRAY
SIEMU CTIRY MNDNH TERAE IRWKA
NHNNO JSODH FRKRI FREPS EDO

3. NDTFR NTGSB DFISC IOICH REUYH
AIDUR OLRFR EFCPS EOE

4. IDTLE ENNNT NGSPT OBIRD ELADO
RIIUE NACEF WTMRT RHHRD DGANO
ENKSM DPSEJ RRIIS FGCYY IOEEU
AEO

5. ADPHV ENNLC GRLDO BGDEO LIMLR
OIPPS ECKTE YMNRN IHIPS AAAYP
KEIYI ATJRO EBFIU ATEFE LRSRO

6. TDEAE ENRIE OGSBM AQBTY FDLAK
UPECI MAGRT CPRTO MRTIR MHRDA
OARTI EKIDS AONRJ BRYOO SFTAC
NPSNE AYYHO A

7. TDVIW ONTFI EOGFH SBQRT ERRLD
ATUPF YITTA RTCPM TOMYC IREHE
WRIRA RTEAK EYRAO IAJDE NAOSF
CENAP SNENR SYOI

E. Double transposition. Six partial anagram keys on the same pair of transposition keys :—

Text-length 79. 45 68 35 69 34 31 41 72 75 3 27 43 36 46 21 65 39 60 78 40.
,, ,, 72. 65 56 57 1 61 17 36 19 52 59 54 63 22 5
,, ,, 75. 15 43 59 28 21 50 38 52 44 — — — - 69 9 72 26 30
,, ,, 76. 58 76 60 28 54 2 39 4 40 19 42 56 61 16 63 24 10 68 48 27 33 66 5 29 71
,, ,, 77. 59 28 61 29 55 2 40 4 41 19 43 57 62 60 64 25 10 69 49 11 34 67 5 30 72
,, ,, 82. 11 59 37 71 64 72 43 63 78 33 68 79.

REF ID:A3079835

F. The following are complete encipher keys :—

The combination of the form 41 1 standing at the left of each series is assumed to have been taken from the preamble of the message anagrammed.

41 1 7 19 30 4 26 37 12 23 34 8 20 41 5 16 27 38 1 13 24 35 3 15 36 9 31 6 17 28 39 10 21 32 18 29 40 11 22 33 2 14 25

70 1 7 19 30 52 63 4 26 37 48 12 23 34 45 56 67 8 20 41 64 5 16 27 38 49 60 1 13 24 35 46 57 68 3 15 36 59 70 9 31 42 53 6 17 28 39 50 61 10 21 32 43 54 65 18 29 40 51 62 11 22 33 44 55 66 2 14 25 47 58 69

73 3 8 29 40 51 62 73 4 27 37 59 70 12 23 34 44 55 66 19 30 52 63 5 16 38 48 71 1 13 24 35 45 56 67 3 15 26 47 58 69 9 20 31 41 64 6 17 28 49 60 10 21 32 42 53 7 18 39 50 61 72 11 22 33 43 54 65 2 14 25 36 46 57 68

41/6 8 17 25 33 4 22 30 39 9 18 26 34 5 14 31 40 1 11 20 28 36 3 13 29 38 10 19 27 35 6 15 23 41 7 16 24 32 2 12 21 37

G. Transposition keys to be resolved into the lines of poetry from which they are derived :—

(i) 28 23 19 5 16 8 25 29 1 26 9 4 17 32 18 35 10 21 30 24 13 6 11 2 33 15 31 14 27 12 34 20 3 22 7

(ii) 31 23 30 4 1 20 27 7 8 28 13 9 19 5 17 10 2 25 18 32 24 21 11 16 29 14 12 26 15 3 22 6

(iii) 5 28 25 14 11 26 7 15 16 18 21 6 1 8 9 29 2 24 10 22 3 20 12 17 19 23 27 13 4

(iv) 1 28 7 35 17 9 6 22 2 29 16 30 15 36 18 10 4 23 39 11 5 12 24 25 33 20 34 8 13 3 37 19 38 31 27 41 26 21 40 14 32

1 24 5 35 16 8 30 27 2 31 28 14 36 17 9 6 3 25 7 10 22 19 29 26 15 20 37 11 33 23 12 4 34 18 21 38 13 32

1 24 7 2 12 20 3 4 15 8 31 16 25 21 28 37 9 22 10 26 33 17 32 23 36 5 14 34 29 30 11 38 6 18 35 19 27 13

1 21 4 15 20 22 6 33 39 29 38 34 40 13 7 23 35 36 2 24 5 16 25 10 30 26 31 27 8 32 9 3 19 17 11 14 37 18 28 12

(v) 22 8 11 12 9 1 14 7 2 4 3 18 21 20 19 13 5 15 17 16 10 6 23

H. An encipher key :—

8 42 43 60 61 76 26 29 40 45 11 63 74 79 21 16 47 55 65 6 14 33 36 3 53 18 70 83 27 9 44 59 62 25 77 30 39 23 57 12 73 80 31 38 17 54 5 72 81 34 2 49 52 67 19 84 28 41 10 58 24 75 78 15 22 46 56 64 13 7 32 37 48 4 66 71 82 1 35 50 51 68 69 20

I. Two encipher keys on the same transposition keys :—

25 6 12 24 7 11 20 37 1 28 2 27 26 10 21 36 18 9 3 33 29 32 30 17 19 8 4 23 34 14 15 13 16 31 5 22 35

25 6 12 24 29 11 20 37 38 15 2 27 26 10 8 35 18 9 3 33 28 32 30 17 19 7 36 4 23 34 1 14 13 16 31 5 21 22

J. An encipher key :—

2 6 14 27 5 9 17 25 4 7 15 24 11 13 22 26 3 12 19 23 8 16 20 28 1 10 18 21

REF ID:A3079835

K. Partial anagram keys on the same two transposition keys for text lengths 76, 79, 127, 133, 134.

76	43 11 18 41 35 32 72 74 33 49 1 3 24 20 58 52 26 10 54 47 13 22 56 45 69
79	63 11 28 23 45 74 75 50 33 41 1 21 24 67 17 7 55 52 9 39 31 69 15 65 59
127	19 121 75 127 80 67 61 102 92 36 69 27 39 33 117 114 4 98 14 11 58 22 55 45 87
133	50 81 125 118 5 117 64 20 25 77 103 92 40 113 45 97 35 133 69 128 21 101 73 132 12
134	121 65 102 63 36 62 64 51 25 108 103 13 40 58 93 26 114 87 6 82 52 30 104 86 130

L. *See* Cipher Text L, in Vol. II. The twenty passages of cipher in this exercise represent the same passage of clear, ciphered in twenty different ways. Passage No. 19 contains an additional portion of text, designed to make its solution easier.

The passage is from an English opera.

It will probably be found advisable to begin the attack on Passage No. 3, or No. 4, these being as it were basic versions.

After solving the cipher text in every case, compare very carefully the different cipher versions in the light of the clear, and make a list of the various weak points and openings for attack on each cipher.

M. *See* Cipher Text M, in Vol. II. Eight passages of narrative English enciphered by means of a simple memorizable process.

REF ID:A3079835

SECTION III

Playfair

Description

The following is the method of enciphering and deciphering by means of the simplest form of Playfair cipher, the classical English method.

The basis is a memorizable keyword. The keyword is written down horizontally, any letter occurring more than once being cut out after its first occurrence. The remainder of the alphabet is written out after it in alphabetical order. The letter J is omitted to reduce the whole to 25 letters and the key alphabet is written into a square.

Example :—Keyword—NECESSITY. Key square :— N E C S I
T Y A B D
F G H K L
M O P Q R
U V W X Z

The message to be transmitted is written out in pairs of letters (wherever the letter J occurs I is substituted for it). Where a pair would consist of one letter doubled, the letter X is inserted after the first occurrence of the letter.

Example :— Text :— F R E E D F R O M H I S F E T T E R S
Pair form :— FR EX ED FR OM HI SF ET TE RS

In the process of encipherment a pair of letters from the key square is substituted for the pairs so formed according to the following rules :—

1. Where the two letters of the pair occur in the same line of the key square the two letters on the immediate right of them respectively are substituted for them. The lines are treated as cyclic.
2. Where the two letters of the pair occur in the same column of the key square the two letters immediately below them respectively are substituted for them. Again the columns are treated as cyclic.
3. Where the two letters of the pair are not in the same line or column they are regarded as the corners of a rectangle and the two letters at the other corners substituted for them, each by the letter on the same line.

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

Clear pairs :—UN DE RT HE SP RE AD IN GC HE ST NU TX TR EX EX

Cipher pairs :—NT YI MD GC CQ OI BT NE HE GC NB TN BU DM SV SV

The process of decipherment is merely the reversal of the above. The solution of Playfair in the above simple form presents little difficulty provided the cryptographer is in a position to guess at the beginning of a cipher text.

REF ID:A3079835

In the following example the clear text is known to begin "The voices blend and fuse....."

Cipher text

PN AX UG DA QD SD LF RH FG PT RA HF NH SG DL **UE SD HF DX RE AG HN HO UE SD HF** RS PC UR TU LA RO GR OR SR NG TQ CH **DX RE AG HN HO** RH LX ZM NY NX GH EW EM **UE SD** IY NX PN DX UZ OE QX RC SR GL XA EY **IR OG HO UL GB VF SD UL GB VF SD** UL GC RL RI RP GU LT PN RP PC XA OE XA LX UN VC **IR OG HO** VK RI ID IR RY ZM OE CO SR XA EF DX DA LF PD **KI EM** LR XA FN EH SX HO ZM LD PE DI FI DE RL VC TU TI RD AR SL PD **KI EM** PL DL GE OF LA EF PT HB **KI EM** PD RP SR IA OF CV RI RL OR EH LD ZK DT PR ET

Here the clear equivalents of 10 cipher pairs are known :--

Cipher	Clear	Cipher	Clear
PN	th	SD	le
AX	ev	LF	nd
UG	oi	RH	an
DA	ce	FG	df
QD	sb	PT	us

Some of the above can be provisionally classified at once.

(i) (FG = df) D, F and G in the keysquare must be consecutive in one line or one column. Alphabetical considerations suggest very strongly that D F G is part of the lines and follows closely after the key word which presumably contains the letter E.

(ii) (AX = ev) suggests the rectangle

A . . . . . E
. .
. .
V X

A and E being part of the keyword and V and X in the bottom line. If so, as there is only one possible letter, W, between V and X, A and E must be adjacent or separated by one letter.

(iii) (UG = oi) gives as one possibility with (i) above :—

I
D F G
O
U

(iv) (PT = us), in conjunction with (iii) above, gives :--

I
DFG
O
P STU

(v) (SD = le) with (iv) and (ii) above gives :—

A . E . I
. . D F G
. . L . O
P . S T U
V W X . .

REF ID:A3079835

Exercise 1.—Complete the key-square and find the key-word and the clear text.

Exercise 2.—Construct in graphic form a bigram table from the example given above showing the clear equivalents of all the cipher pairs of the example and their frequency.

Exercise 3.—Examine the problem theoretically (*i.e.* from the aspect of positional relationship, independently of what the key-word may be). Some of the questions to be answered are :—

(i) What is the number of cipher letters which can represent any one clear letter ?

(ii) Are all the possible cipher letters of one clear letter equally probable ?

(iii) For any one *first* letter of a *clear* pair, how many possible *second* letters of a *cipher* pair are possible ?

Exercise 4.—One known method of increasing the security of the Playfair cipher is the substitution of pairs from the key-square for pairs of letters not adjacent, but at a pre-arranged interval. For example, the 1st letter might be taken with the 11th, the 2nd with the 12th, etc., and the 21st with the 31st, etc. The resultant pairs may appear as pairs in the cipher version, or they may be split so as to occupy the positions of the clear letters in the clear text. How would you overcome the new cryptographic difficulties introduced by this complication ? (N.B.—You must not assume that the interval is known, but a guess at the textual beginning of a message may be assumed.)

REF ID:A3079835

SECTION IV—COMPLEX SUBSTITUTION

A. General Considerations

1. Students have already been introduced in Section I of the course to various aspects of simple substitution and of one of the simplest forms of complex substitution, *i.e.* encipherment in letters by use of the Vigenère table, or recipherment in figures by use of the figure equivalent of the Vigenère table, in each case by means of a short key. Vigenère substitution is frequently known as " sliding alphabet " substitution. The loose term " subtractor " for an addition series (non-carrying) of any length will already have been understood.

2. In dealing with the later exercises of Section I, students will have become accustomed to present their material in the form of a table in which those units of substitution of a cipher text are arranged in a column to which the same process of substitution or resubstitution has been applied. Such a table displays the following general features :—

(*a*) Recurrences in the cipher text lie under one another ; and

(*b*) the frequency of the original textual units is a feature of individual columns and not common to all columns.

3. Solution depends on the adjustment of the columns to a common base and the correctness of work carried out on these lines is normally checked by the appearances of offset (*i.e.* overlapping) recurrences additional to those lying under one another in the original table. Units of a column of the original table may be said to be " homogeneous." It is very important that all the implications of this method of presentation " in depth " should be grasped. The word " depth " here has a somewhat different significance from that of the same word applied to the solution of transposition systems by anagramming. Here it may be defined as the number of lines at any point in a table of the kind under discussion.

Exercise 1.—Refer back to exercise 12 of Section I. Arrange the beginnings (excluding non-textual groups) of the six texts " in depth." Observe that, when the true significance of the starting point indicators has been revealed, units of substitution appear on two " cuts " owing to the fact that pairs belonging to two texts of odd and even starting point respectively do not coincide in columns arranged in depth. (Conversely, it should be noted that this feature of " non-coincidence of cut " of the units of substitution may in certain circumstances be used to arrive at the true figures of a complex substitution.) This aspect is worthy of careful study.

B. Long Subtractors

1. " Long subtractor " ciphers may be defined as systems in which the subtractor is longer than the individual texts to which it is applied. In modern practice such ciphers take the following form :—

(i) First process. Direct substitution for the letters, syllables, words and phrases of the clear text of cipher units taken from a code book in 4 or 5-figure groups. Such a code book may be—

(*a*) alphabetic, *i.e.* the cipher groups in numerical order correspond to the clear units in alphabetical order ; or

(*b*) " hatted," *i.e.* the cipher groups are shuffled, and two books have to be prepared, one for enciphering and the other for deciphering, the latter being the index in alphabetical order of the former.

REF ID:A3079835

(ii) Second process. Non-carrying addition to the figures obtained in the first process by means of part of a long subtractor. Subtractors may be of a great length.

2. The following are some of the more important characteristics of ciphers of this type :—

(i) "Mixed unit" code books are sometimes employed, *i.e.* mixed 3 and 4-figure, or mixed 4 and 5-figure. In the preparation of such books there must, of course, be no ambiguity for the decipherer as to the division into units of the cipher text of the first process. (In this connection reference should be made to the substitution employed in exercise 6 of Section I.) In one historical instance a mixed 2, 3 and 4-figure book is known to have been used under a long subtractor.

(ii) Systematic code books are sometimes employed where the arrangement is not strictly alphabetic but is sufficiently systematic to permit encipherment and decipherment from the same book.

(iii) Dictionaries are sometimes employed as code books; in these the cipher groups are normally made up of the page and position on the page of the word requiring encipherment.

(iv) Sometimes a number of separate subtractors are employed. If so, the particular subtractor chosen has to be indicated for the benefit of the decipherer in some prearranged manner.

(v) When one long subtractor is employed and there are a number of different possible starting points, the particular starting point used has to be indicated.

(vi) In the case where there is only one starting point for all telegrams, indication is obviously unnecessary.

(vii) Indicators may be in the preamble of the telegram, or at the beginning or end of the text, or hidden in the body of it.

(viii) There may be many alternative indicators for each starting point, or they may vary according to the date, the serial number, or even the length of the telegram, or according to certain figures of the enciphered text.

(ix) Sometimes the starting point depends directly on the date, the serial number, or the length of the message. In such cases there are frequently non-textual groups in the text which check the starting point.

3. The basis of any method of solution of long subtractor ciphers must always be the accumulation of "depth." The following are the vulnerable points in the construction of this type of cipher which most frequently assist the cryptographer :—

(i) Obvious or insufficiently concealed starting point indicators.

(ii) Limitations in the basic book.

(iii) Limitations in the subtractor.

(iv) Groups which are an integral part of the subtractor inserted unchanged in the text for check purposes.

(v) Overloading of the substractor.

These vulnerable characteristics will now be treated in more detail.

4. Types of indicators are too numerous for classification, but it may be stated generally that attempts, however ingenious, to conceal indicators systematically are rarely successful against experienced cryptographers. For this reason, where concealed indicators have not been found but are suspected, a systematic scrutiny of the tabulated beginnings and ends of telegrams, however laborious, has frequently to be undertaken.

REF ID:A3079835

5. Book limitation will be best understood from a few historical examples :

(i) A 25,000 group 5-figure book in which the cipher groups all lie between 00000 and 24999.

(ii) A 4-figure book in which the cipher groups consist of 1 even or 4 odd figures only 1250 of the 10,000 possible 4-figure groups are used.

(iii) A 5-figure book in which the non-carrying sum of the digits of each group is 0 ; groups such as 23799, 34625 and 15680 occur, but 23467 does not ; only 10,000 possible groups are used. This type is known as " value " limitation. Its only advantage is that any group in which one figure has been wrongly transmitted is immediately recognisable.

(iv) A 4-figure book in which the carrying sum of the four digits of each group is a multiple of 3.

(v) A 33,000 group 5-figure hatted book in which the first pair of each group is limited to one of the following :- 00, 13, 15, 17, 21, 23, 25, 27, 31, 35, 37, 41, 43, 45, 47, 51, 53, 57, 61, 63, 65, 67, 71, 73, 75, 81, 83, 85, 87, 91, 93, 95, 97.

(vi) A 4,000 group 4-figure book in which all groups start with 0, 3, 6 or 9.

Exercise 2.- Examine the effect of applying subtractors to each of the above limited books :—

(i) In which of the examples given could the limitation be used to set overlapping messages in their true relationship to one another, *i.e.*, to get depth ?

(ii) How would you proceed to get sufficient depth to recognise the form of the limitation in the first instance (assuming that you get no help from the indicating system) ?

(iii) How would you use the limitation to get as much depth as possible at all points of the subtractor ?

6. Limitations of the subtractor are not commonly found, but the following, which have been seen in actual use, may serve as a general guide :—

(i) The figure 0 is omitted, presumably on the quite mistaken assumption that the security of a subtractor cipher depends to some extent on the fact that no figure obtained in the first process remains unaltered in the second.

(ii) The subtractor is formed by each holder of the cipher independently by expansion from a short series of figures or a key according to a prearranged system. As an example of this a subtractor might be formed from an arbitrary 5 figure group as follows :—

Take any arbitrary 5-figure group ; this will be the first group of the subtractor ; the 5 figures of the second group will consist of the sum of the 1st and 2nd figures, the sum of the 2nd and 3rd, the sum of the 3rd and 4th, the sum of the 4th and 5th, and the sum of the 5th and 1st figures of the first group. Thus the subtractor derived from the arbitrary group 23791 would be 23791 50603 56638 12913 31044 41487 55251 07766, etc. The particular arbitrary group on which the subtractor is based would, of course, have to be indicated by the encipherer.

(iii) The subtractor is taken from a limited or regular source, *e.g.* trigonometrical or logarithmic tables.

REF ID:A3079835

(iv) The subtractor is an actual mathematical series, such as the successive powers of the figure 2, which would give 24816 32641 28256 51210 24204, etc.

(v) The subtractor is formed from successive groups of the *encipher* of the basic code book employed in the first process, where that book is hatted.

Exercise 3.—What limitation, partial or complete, would you expect to find in the groups of the final enciphered form of messages where the basic book has the limitation of para. 5 (v) above and the subtractor consists of groups from the encipher ?

(vi) The subtractor is formed by substitution of either 1 or 2 figures for each letter of a prearranged narrative text. In this type the base would be a code or dictionary and the subtractor derived from a book, such as a novel, of which all the holders of the cipher possess a copy. Each holder must also be in possession of the substitution table to be used for converting the text into figures and he must know how to indicate his starting point in the novel.

Exercise 4.—Suppose that you are required to solve cipher messages in considerable quantities knowing that a 300-page (approx.) English Dictionary is used as the basic code and that the solution is derived from an unknown novel by use of the following substitution table :—

A25 B23 C97 D01 E41 F05 G64 H95 I19 J63 K45 L00 M65 N78 O23 P80 Q83 R37 S86 T78 U89 V50 W78 X79 Y47 Z54

In the first process each word or letter may be assumed to be represented by a 5-figure group of which the first 3 figures are the page of the dictionary on which the word occurs and the last 2 figures are the position on the page, *e.g.*, the group 03219 means the 19th word on page 32, and 25701 means the first word on page 257. It may further be assumed that the starting point indicating system is known and expresses directly the page, and the line on the page, of the starting point of the subtractor for each message, also that there are several cases of 4 or 5 messages reciphered from the same starting point. On what lines would you suggest approaching the solution of messages in such a cipher ?

Exercise 5.—What would be the effect of substituting single figures for letters in the construction of the subtractor instead of pairs in the above cipher according to the following table ?

A, K, U	represented	by	0
B, L, V	,,	,,	1
C, M, W	,,	,,	2
D, N, X	,,	,,	3
E, O, Y	,,	,,	4
F, P, Z	,,	,,	5
G, Q	,,	,,	6
H, R	,,	,,	7
I, S	,,	,,	8
J, T	,,	,,	9

7. One peculiar type of long subtractor has been seen on rare occasions ; in this type there is an extra arbitrary 5-figure group after the last group of each line of the subtractor as printed, or of each alternate line. Such groups are inserted unchanged in the message when recipherment has reached the end of the line where they lie. They are presumably intended as a position check for the benefit of the decipherer, but they are of course completely destructive of security, as they can be used to set

REF ID:A3079835

all overlapping messages in their proper interrelationship. When they are used, they are quite easily recognisable as recurring groups, which appear at regular intervals in two or more long messages.

8. A subtractor may be said to be overloaded when it is so short or used for so many messages that it is practicable to set messages at some places in sufficient depth for solution, merely by message-to-message recurrences. It is difficult to make any definite statement as to the amount of depth required for the solution of long subtractors, but it has frequently been found possible to solve on a depth of as little as 5 where a sufficient number of identifications have been established to read some messages.

9. So far little has been said about the actual process of breaking into an unknown long subtractor cipher. Investigation on the following lines in order to get depth is a necessary preliminary :—

(i) All messages must be " registered," *e.g.*, the beginnings and ends tabulated together with all relevant external information, such as date and time of origin, identity of originator and addressee, call signs of transmitting and receiving wireless stations, external indicators, if any, etc.

(ii) The register formed above must be scrutinised for initial or final recurrences between messages and for evidence of concealed starting point indicators.

(iii) It may now be possible to lay out the whole material in depth. If not, that portion of the material which can be arranged in depth should be tabulated and the columns so obtained examined for limitations of the basic book. Such limitations, if found, should make it possible to complete the tabulation in depth.

(iv) If the above procedure is unsuccessful or only partially successful, it may be necessary to analyse the whole material or a large portion of the material for message-to-message recurrences. Here students should remember that recurrences are not to be expected within the same message, and that, as large numbers of groups will have to undergo analysis, recurrences of single groups will very frequently be accidental, while recurrences of two or more consecutive groups are very unlikely to be accidental.

10. Below will be found a portion of the tabulated depth in a 5-figure long subtractor cipher. The best depth is here 15, and a section 7 groups wide is given. The demonstration following shows some of the information which can be obtained from this small amount of material. It will, no doubt, be realised that the example is a very favourable one.

		A	B	C	D	E	F	G
1		(31892	64437	12991	82384	45306	**87882**	**91445**..
2			(54906	22775	85570	16687	**87419**	08502..
3				(12244	95354	19873	58790	**06328**..
4	..	67072	80559	**33541**	73774	31360	46739	78358..
5	..	45492	57229	26844	85622	53700	89693	06791..
6	..	34810	**80186**	40608	87917	12449	72536	14722..
7	..	69256	54358	34948	13287	32231	89664	01580..
8	..	23791	41612	49942	07239	37344	**87419**	04858..
9	..	47200	46805	11247	07527	24255	**41314**	**91445**..
10	..	46921	44081	**33541**	**11003**	47580	**87882**	**91445**..
11	..	24367	76140	02646	14862	02331	**41314**	**91445**..
12	..	53665	**80186**	42669	**11003**	47700	**87419**	70333..
13	..	44882	60353	21048	70323	12780	54257	64484..
14	..	75050	98409	07744	20002	18551	45738	**06328**..
15	..	65502	58906	**33541**	07682	47580	43823	92842..

All positional recurrences of one or more complete groups are shown in heavy type. The passages numbered 1, 2 and 3 are beginnings of messages, the remainder are sections from the middle of messages.

REF ID:A3079835

11. Examination for limitations reveals that the first figures of groups are limited as follows :—

Column	A	..	2, 3, 4, 5, 6, 7.
,,	B	..	4, 5, 6, 7, 8, 9.
,,	C	..	0, 1, 2, 3, 4.
,,	D	..	7, 8, 9, 0, 1, 2.
,,	E	..	0, 1, 2, 3, 4, 5.
,,	F	..	4, 5, 7, 8.
,,	G	..	6, 7, 9, 0, 1.

This can only mean that there is a limitation of the first figure of all groups in the basic book which may be assumed to begin with 0, 1, 2, 3, 4, or 5. This provides a provisional skeleton subtractor as follows :—

9 3

2.... 4.... 0.... 7.... 0.... 4.... 6....

12. The majority of the groups which occur more than once in a column may be presumed to represent very commonly used groups in the basic book. Certain groups may in fact occur more than once in two or more columns. To test this, each group which occurs more than once in a column is subtracted from all the other groups in the same column. Analysis of the result reveals certain recurrent groups which are underlined in the table below :—

Group subtracted.	B 80186	C 33541	D 11003	F 87882	F 87419	F 41314	G 91445	G 06328
1	84351	89450	**71381**	00000	**00473**	46578		**95127**
2	74820	99234	74577	00637	00000	46105	**17167**	**02284**
3		89703	84351	71918	**71381**	17486	15983	00000
4	**00473**	00000	63771	89957	**69320**	05425	87913	72030
5	77143	93303	74629	02811	**02284**	48389	15356	**00473**
6	00000	**17167**	76914	95754	**95127**	31222	23387	18404
7	73272	**01407**	**02284**	02882	02255	48350	10145	05267
8	61536	16401	96236	00637	00000	46105	13413	08630
9	66729	88706	**96524**	64532	**64905**	00000	00000	**95127**
10	**64905**	00000	00000	00000	**00473**	46578	00000	**95127**
11	96064	79105	03869	64532	**64905**	00000	00000	**95127**
12	00000	19128	00000	00637	00000	46105	89998	74015
13	80277	98507	**69320**	77475	77848	13943	73049	68166
14	18323	74203	19009	68956	68329	04424	15983	00000
15	78820	00000	96689	66041	66414	02519	**01407**	**96524**

REF ID:A3079835

It will be seen at once that column B with the subtractor 80186, column D with the subtractor 11003, column F with the subtractor 87419 and column G with the subtractor 06328 are interlinked. These subtractors are used as provisional subtractors in the following table, but the first figure has in each case been corrected to agree with the skeleton subtractor at the end of para. 11 above.

Provisional Subtractor :—	A 2....	B 40186	C 9 0....	D 71003	E 0....	F 47419	G 66328
1	(31892	64437	12991	82384	45306	87882	91445....
			2				
	1	*24351*	*1*	*11381*	*4*	*40473*	*35127*
2		(54906	22775	85570	16687	87419	08502....
			3				
		14820	*2*	*14577*	*1*	*40000*	*42284*
3			(12244	95354	19873	57790	06328....
			2				
			1	*24351*	*1*	*11381*	*40000*
4....	67072	80559	33541	73774	31360	46739	78358....
			4				
	4	*40473*	*3*	*02771*	*3*	*09320*	*12030*
5....	45492	57229	26844	85622	53700	89693	06791....
			3				
	2	*17143*	*2*	*14629*	*5*	*42284*	*40473*
6....	34810	80186	40608	87917	12449	72536	14722....
			5				
	1	*40000*	*4*	*16914*	*1*	*35127*	*58404*
7....	69256	54358	34948	13287	32231	89664	01580....
			4				
	4	*14272*	*3*	*42284*	*3*	*42255*	*45262*
8....	23791	41612	49942	07239	37344	87419	04858....
			5				
	0	*01536*	*4*	*36236*	*3*	*40000*	*48530*
9....	47200	46805	11247	07527	24255	41314	91445....
			2				
	2	*06729*	*1*	*36524*	*2*	*04905*	*35127*
10....	46921	44081	33541	11003	47580	87882	91445....
			4				
	2	*04905*	*3*	*40000*	*4*	*40473*	*35127*
11....	24367	76140	02646	14862	02331	41314	91445....
			1				
	0	*36064*	*0*	*43869*	*0*	*04905*	*35137*
12....	53665	80186	42669	11003	47700	87419	70333....
			5				
	3	*40000*	*4*	*40000*	*4*	*40000*	*14015*
13....	44882	60353	21048	70323	12780	54257	64484....
			3				
	2	*20277*	*2*	*09320*	*1*	*17848*	*08166*
14....	75050	98409	07744	20002	18551	45738	06328....
			1				
	5	*58323*	*0*	*59009*	*1*	*08329*	*40000*
15....	65502	58906	33541	07682	47580	43823	92842....
			4				
	4	*18820*	*3*	*36689*	*4*	*06414*	*36524*

REF ID:A3079835

Exercise 6. -Examine the three message beginnings as provisionally deciphered in the above table and complete the provisional subtractor. Examine the result for "offset" recurrences (*see* para. 3 on the first page of this section) to satisfy yourself that the result you have achieved is correct.

13. An alternative method, more general in application, could have been used to obtain a provisional subtractor. An index could have been prepared of the difference between every pair of groups occurring in the same column. In practice the smaller of the two possible complementary differences between any two groups is given in such an index.

The following table exhibits graphically the differences between each pair of groups in column A :—

TABLE OF DIFFERENCES FOR COLUMN A

	67072	45492	34810	69256	23791	47200	46921	24367	53665	44882	75070	65502
31892	36280	14600	03028	38464	18101	16418	15139	17535	22873	13090	44268	34710
67072		22680	33262	02284	44381	20872	21151	43715	14417	23290	18088	02530
45492			11682	24864	22701	02818	01539	21135	18273	01610	30668	20110
34810				35446	11129	13490	12111	10553	29855	10072	41240	31792
69265					46565	22056	23335	45999	16691	25474	16804	04754
23791						24519	23230	01676	30974	21191	52369	42811
47200							01389	23943	16465	03428	38850	28302
46921								22664	17744	02149	39139	29681
24367									39308	20525	51793	41245
53665										19883	22495	12947
44882											31278	21720
75050												10558

Exercise 7.—Study the above table. Assuming that you have prepared such a table for each column, how would you analyse your differences with a view to discovering if any pair of columns have three different groups in common ?

14. Yet another approach could have been to assume that messages 1, 2 and 3 all start with the same recurrence. The result of subtracting 2 from 1 and 3 from 2 is shown below.

	B	C	D	E	F	G
1–2	10531	90226	07814	39729	00473	93943
2–3		10531	90226	07814	39729	02284

Exercise 8.—Use the above information to obtain provisional subtractors for the seven columns.

Exercise 9.—You have now reduced the material provided to homogeneity. List the groups so obtained and count the number of occurrences of each. Prepare a difference table for the commonest groups (not more than 6 or 7 of them). *N.B.*—It is wise to omit those groups which occur only in the stereotyped beginning of messages 1, 2 and 3.

REF ID:A3079835

Exercise 10.– Below will be found portions of 8 further messages in the same cipher as above. Each set in depth" at another part of the subtractor. Find provisional subtractors to reduce them to the same base as above. Add the new groups obtained to those prepared in Exercise 9.

	78848	23766	53088	87395	28000	46811.
1	64074	15331	68961	71256	32419	72618.
18 .	70022	99207	76284	46115	40440	89775
19 ..	70022	24028	44197	61010	27163	87591..
20 ..	70242	23393	32976	79072	05259	87591..
21 ..	64431	23393	62106	36367	34440	87591..
22 ..	63965	09814	25013	38460	12975	54339..
23 ..	71607	25577	68334	64199	32046	44517..

Exercise 11.—Message No. 24 of which the first 5 cipher groups are given below is set against the subtractor, one figure (not one group—one figure) to the right of message No. 1 above. Find the true figures of the basic book and reduce the list of groups prepared in Exercises 9 and 10 to the correct base. Reduce the two portions of the subtractor solved to the original figures.

45015 86682 59285 82882 54335

REF ID:A3079835

SUPPLEMENTARY EXERCISES—N-P

N.—The following series of messages was intercepted by the German Wireless Interception Service in Occupied France during September and October, 1940. Owing to the very high frequency used by the transmitters it was impossible to locate the sets with any certainty by direction-finding ; one set however was fairly certainly across the Channel, and the other in the coastal sector near the important aerodrome of Bois-le-Duc. The character of the transmission made it fairly evident that the messages P1, 2, 3, etc., were those of a hostile secret agent reporting from this area, and the A1, 2, 3, etc., series the replies from his H.Q.

The Gestapo gradually narrowed the search and finally raided a hotel room in the local town ; their bird had flown, but among the burnt papers in the grate they were able to identify part of the last message (A.8.) intercepted ; a miniature wireless transmitter was also found, together with two sheets of paper ; one of these was a torn sheet of official French notepaper from the local Mairie, with notes on it as follows :—

RÉPUBLIQUE FRANÇAISE

Liberté *Egalité* *Fraternité*

Mairie,
Blanqueville,
PAS-DE-CALAIS.

le.....19...

Origine	Alphonse	Poirot	Cas d'urgence
Endemique	Elaine	St.-Etienne	Nouvelle Elève
Pas-de-Calais	1	1	2
Democrat	Octave	Neu-Offenbach	Sous-Officier

	No. Tel.
Paul	Blanqueville 16
Edouard	Bapaume 43
Xerxès	Bois-le-Duc 9
Nigel	Givry-sur-Somme 2
Quichotte	Blanqueville 44
Zadig	Courtois 23

This suspicious document was accompanied by another, a sheet of squared school paper, on which was scribbled in English an unfinished message :—

" FROM P16 STOP YOUR A8 URGENT ACKNOWLEDGED STOP ACTION BEING...."

The agent was probably in the middle of writing this message when the raid took place ; no other indication of his method of enciphering was found, except some more blank sheets of squared paper, on one of which was scribbled in English :—

" Play up, play up, and play the game ".

" Ach," commented the Chief of the German cipher bureau on seeing this, " Der Engländer, auch wenn er Spion wird, muss immer ' gentleman ' bleiben, er muss ' play fair ' ! "

REF ID:A3079835

O.—The background to this exercise is the early part of the British offensive in Libya in January, 1941, culminating in the fall of Bardia. The messages are supposed to be Italian, taken by our Interception Service. The contents are imaginary, but more or less realistic, and the text is English.

You may expect the Italian commanders concerned to use signatures and addresses as a regular practice. The following extracts from the Italian Order of Battle published by the Intelligence Branch of the General Staff may be of assistance :—

ANTONELLI	General	Intendant-General (Supplies)	Located at BENGHAZI.
ARGENTINO	General	Commanding Defences	,, ,, DERNA.
BERGINZOLI	General	,, ,,	,, ,, BARDIA.
GALLINA	General	C.-in-C., Eastern Libya, at advanced G.H.Q.	,, ,, TOBRUK.
LEO	Lt.-Col.	O.C., Saharan Battalion	,, ,, HON.
RUFFO	Col.	Second in Command	,, ,, DERNA.

The Wireless Intelligence Service has provided the following identifications of the Italian W/T stations concerned :—

W/T Station.	*Identification.*
X	Advance H.Q., E. Libya, near TOBRUK.
Y	BENGHAZI area (Probable).
Q	DERNA (Probable).
S	H.Q., BARDIA.
N	TOBRUK (Probable).
O	Believed to be a form of C.Q. (all stations) call, since traffic is always to O, and never originates there.
P	HON.

This exercise is best tackled by a syndicate. Write a description of the different processes used and of the indicating systems, and build up the original book or books as far as possible. Describe also the reasoning you used in arriving at a solution.

P.—The recipher and concealed indicator systems used in this problem are typical of a fairly high-grade cipher. The original cipher is not as elaborate as the dictionary code-book used in the last problem, and the texts are quotations from a modern novel. Write a full description of the cipher and of your attack on the problem.

(C 41687—1) 250 8/41