MEMO
FROM: R&D DEPT., SUB-SUB-BASEMENT
TO: CRYPTANALYSIS TEAM
RE: CIPHER CLOCK

HARRY:

WE RECEIVED THE INTERESTING SPYCLIST CIPHER CLOCK FROM YOUR FIELD AGENTS. WHILE WE HAVE NOT MADE MUCH PROGRESS IN UNDERSTANDING THE DEVICE, IT DID BRING TO MIND SOMETHING WE OURSELVES HAVE WORKED ON. I CONTACTED THE ARCHIVIST AT THE ROYAL ACADEMY, AND SHE SENT THESE MIMEOGRAPHED PAGES. PERHAPS THEY CAN BE OF HELP TO YOUR CRYPTANALYSIS TEAM. THE DEVICE IT DESCRIBES IS NOT THE SAME AS THE SPYCLISTS' DEVICE, BUT THE OPERATION SHOULD BE SIMILAR. THE MOST NOTABLE DIFFERENCES ARE:

1. LENGTH OF PLAIN AND CIPHER ALPHABETS ARE DIFFERENT (SEEN BY SIMPLE INSPECTION)
2. METHOD OF MIXING THE KEY COULD BE DIFFERENT (NO WAY OF KNOWING AT THIS POINT)

p.s. Please send food and water. We are suffering here in the dark and dank sub-sub-basement. Have some human pity on us.

Instructions for the Employment of Wheatstone's Cryptograph.

[From a Pamphlet published to accompany an instrument called "The Cryptograph."]

A CIPHER which at the same time should be perfectly secure and easy in its application is a desideratum; and these combined advantages can only be obtained by means of an instrument in which all the complexity necessary to ensure security shall be effected by mechanical arrangements, whilst its manipulation shall be subjected to the simplest rules. Such an instrument is now offered to the public, after its utility has been proved by extensive employment in various departments of the public service and by telegraph companies.

One thing is yet wanting to render the benefits of the Electric Telegraph complete. Letters by post are sent sealed, and their contents are conveyed, with a secrecy seldom violated in free countries, to their destination; but telegraphic messages are in general transmitted so that their contents are understood by all the officials concerned in their conveyance. This arises from several causes: some persons are totally ignorant of the principles on which any ciphers are constructed; others acquainted with particular methods are afraid to employ them in their uncertainty regarding their security, and with good reason, seeing the facility with which those in ordinary use have been detected; and others who possess what they consider to be secure methods are deterred from using them on account of the great difficulties attending their translation and re-translation.

With the aid of this instrument an extensive secret correspondence can be carried on with several persons, and a sepa-

rate cipher can be employed for each correspondent. The despatches prepared by it are indecipherable by any person unacquainted with the word that may have been selected for the base of the cipher alphabet; moreover, so long as the key-word remains undivulged, even the possession of the instrument employed, or of one similar to it, would not in the least assist any endeavour to discover the translations.

The number of telegraphic messages relating to domestic occurrences are very much limited by the disinclination of parties to let their family affairs be known to officials in their neighbourhood; and there can be no doubt were this difficulty removed, this class of messages would be considerably augmented, to the benefit of the telegraphic department as well as to that of the public.

The advantages of communication by cipher for military purposes are too obvious to be insisted upon.

Instructions.

Formation of the Permutated Alphabet.

Choose any name or word, in which the same letter does not recur, as "France," "Carlton," "Palmerston."

Write down beneath it the omitted letters of the alphabet in their regular order, placing them in columns thus:—

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

Then write the letters as they appear in the successive vertical columns, in a single row, thus:—

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

The letters of the alphabet of the Cryptograph are then to be placed in the above order round the inner ring, the initial letter C in this case being placed exactly below the blank of the permanent alphabet.

It is not ***necessary*** to adopt a word in which the same

letters do not recur. Any word whatever will answer the purpose by erasing the redundant letters. For example :—

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

This gives

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

If a different key-word be adopted for each correspondent, it will be impossible for any one of them to decipher a despatch addressed to another.

If the divided letters be employed, their subsequent distribution, after the despatch is prepared, will render the discovery of the key-word impossible even on possession of the instrument. This is of importance when the cryptograph is employed for military purposes; but when no fear is entertained of its falling into other hands, it will be more convenient to make use of the entire card circles having the cipher alphabets written upon them. A distinct cipher may thus be always ready for each correspondent, one circle being instantly changeable for another.

The Cryptograph can be secured to a desk or table by means of the pins on the lower surface. As by these means it can be made perfectly steady, the hands can be worked by one hand. It will be found preferable to use the left hand for this purpose, as thereby the right hand is left free for writing.

Rendering a Despatch into Cipher.

At the commencement, the long hand must correspond with the blank of the outer circle and the short hand be directly under it.

The long hand must be brought successively to the letters of the despatch (outer circle), and the letters indicated on the inner circle by the short hand must be written down.

At the termination of each word the long hand must be brought to the blank, and the letter indicated by the short hand also written down. By this arrangement the cipher is

continuous, no intimation being given of the separation of the words.

Whenever a double letter occurs, some unused letter (as, for instance, *q*) must always be substituted for the repeated letter; or the latter may be omitted.

It will be best to divide a despatch into short sentences, and to commence each sentence with the instrument adjusted as at the beginning of the despatch. By this arrangement an error in one sentence cannot affect the other sentences.

The full-stop at the end of each sentence should be represented by a dash following the letter that is used to conceal the blank or termination of the last word.

To translate a Cipher Despatch back to the original.

Make the long and the short hands coincide at the blank as before, and then by the movement of the long hand place the short hand opposite each of the letters of the cipher despatch in succession, writing down the letters indicated by the long hand.

The rule respecting the double letters is not to be observed in turning a cipher despatch back to the original. A slight error in copying the cipher can be retrieved in the translation by trying the letters beyond, omitting previously a turn, or adding an extra one according to circumstances.

After using the instrument, if there be any occasion to make it impossible for persons about one to discover the key-word of the cipher, the letters of the cipher or inner circle should be removed. This can be effected by applying the ivory punch to the apertures at the back. The order of the cipher can be reproduced by remembering the key-word.

In cases where no fear of loss or abstraction of the instrument is apprehended, the card circles may be employed. The letters of the cipher must be written in their proper order in the divided spaces. Ciphers with different keys appropriated to each correspondent may be thus always kept in readiness, and one may be promptly substituted for another.

The chief circumstances which render this cipher so secure are these:—

1. The same letter of the despatch is represented indifferently by any letter of the cipher.

2. No indication of the number of letters that there may be in any word is afforded.

3. There is no clue to the separation of the words, as the blank is itself represented indifferently by all the letters of the alphabet.

4. The changes in the signification of a letter depend on a *regular law*, the accessory hand making in some cases a complete revolution after one letter, and in others after two, three, or more letters.

5. The permutations of the cipher alphabets are practically infinite.

Before despatching a letter in cipher, the sender should translate the different sentences in order to ascertain that no mistakes exist.

In practice only, the most important parts of a despatch need be rendered into cipher.

The same instrument can be employed in corresponding with several persons, as the order of the letters in the cipher on the inner circle is capable of being changed in an almost infinite number of ways.

As the secret of the cipher is the particular order or succession of the letters, it is not necessary to keep the instrument under lock and key, provided that the cipher alphabet has been removed after use.

The following despatch of the Duke of Wellington, translated into a cipher constructed by means of this instrument, will afford an exercise both for translating into cipher and re-translating into ordinary language. The key-word is *France*. The dash indicates that the long and short hands of the cryptograph are both to be brought back to the blank, so that the following sentence may be translated without running on from the preceding.

Lieut.-Gen. Viscount Wellington, K.B., to Lieut.-Gen. Hill.

Sir, Arruda, 8th October, 1810.

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

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

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

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

(Signed) WELLINGTON.

---

*The * Quarter * Master * General * sends * orders * to * Major * General * Fane * to * withdraw * the * Cavalry * under * his * command * to * Tojal * and * Loures * ——*

*I * request * you * also * to * send * a * Brigade * of * six * pounders * to * Sobral * de * Monte * Agraca * to * join * the * Sixth * Division * I * also * request * you * to * send * from * Villa * Franca * the * nine * pounder * Brigade * to * Copua * de * Montecheque * where * it * is * to * remain * in * reserve * and * in * readiness * to * move * at * a * short * notice * ——*

*There * must * be * a * Brigade * of * Infantry * for * the * occupation * of * the * lines * extending * from * the * high * road * to * the * Tagus. ——*

N.B. The above despatch is given nearly at length in order to illustrate the system of cipher; but in practice only the most important parts requiring concealment need be rendered in cipher.