CRYPTO AG.
ZUG
(Switzerland - Suisse)

No.

Vertraulich
Confidential

Usage of Hagelin cryptographer CX-52.

A. Introduction.

Mr. Boris Hagelin, head of Crypto A. G., has been a recognized expert in the field of cryptography since shortly after the First World War. Crypto A. G. with its predecessor organizations is today the oldest established firm in this field in the world. While it is impossible to disclose the identities of our customers, it is no secret that over forty governments are using our equipments and that the number is steadily increasing. Even more impressive is the loyalty to our products that has been demonstrated through the years by our customers. The confidence thus displayed in our products is, we believe, justified by the cryptographic and mechanical excellence of our machines.

The past forty years have seen advances in ciphering machines comparable to those in the same period of time in aircraft. The great volume of messages requiring protection in the Second World War, followed by the development of modern computers, necessitated major advances in the art of cryptography and consequently in the design of ciphering machines. The Crypto A. G. engages in continuing research in these fields, and our line of ciphering machines has been carefully developed to meet those as well as many other exacting demands.

In the machine type CX-52 Crypto A. G. provides a basic ciphering equipment which is so designed as to permit each individual customer to select and arrange a tremendous number of variable elements, each selection and arrangement being cryptographically entirely different from every other selection and arrangement. It is through the selection and arrangement of these variable elements that you yourself create your own personal and unique ciphering machine. The number of selections and arrangements of these variable elements is so great as to be far beyond the capacity of even the most powerful modern computers.

The best way in which to use the machine to cipher messages depends upon the nature of the correspondence, and the special needs of those who correspond. Consequently, just as there is no one best correspondence plan to cover all situations, there is no one best way in which to use the machine. The remarkable flexibility of our machines permits a usage precisely tailored to your particular circumstances. This, combined with the selection and arrangement of the variable elements, constitutes a ciphering system which is truly individual.

The machine type CX-52 has been designed to permit encipherment of any kind of clear language texts, and no special precautions are needed for messages of specialized or unusual content. In particular the use of the machine type CX-52 is not restricted to certain languages or kinds of languages, but can be adapted to any language whatsoever. We will be glad to advise customers in this matter. Our standard machines are provided with the Latin alphabet, consisting of the letters A to Z. However, we can also supply equipments with other alphabets or symbols, selected and arranged in exact accordance with the requirements of individual customers. Moreover, it is possible to have one alphabet or set of symbols used for the cipher text and a different one for the clear text. This is particularly useful when it is necessary to send messages internationally through commercial channels which are normally limited to the Latin alphabet. For instance, the twenty-six letter Latin alphabet may be used for the cipher even though the clear text be written in a special alphabet.
It is even possible to have cipher text that can be read left to right and clear text that is read from right to left. Upon decipherment the clear text will appear in the symbols in which it was originally written.

As with any system of encipherment, the details of your unique machine must be afforded the greatest possible protection. This kind of information is like the combination to a safe. Our ciphering machines are in many ways comparable to safes. The manufacturer delivers a product of great inherent security. The purchaser, to take advantage of this, must have a personal keying element. In the case of the safe, it is the combination; in the case of the ciphering machine, it is the selection of variables combined with the usage. In either case, if this information falls into the wrong hands, the security provided by the equipment is lost until the keying element is changed. It is one of the outstanding features of Crypto A. G. equipments that when compromise is suspected such changes can conveniently be made without the expense of new equipment or even parts. In this connection, it should be pointed out that our equipments for machine encipherment require a far smaller amount of secret material to be protected than do most other ciphering systems, and that consequently this material is relatively easier to protect.

It is not good business practice for us to be knowledgeable of the details of the customer's machine and usage, which should be truly national secrets, any more than it would be for the safe manufacturer to know the combination to his customer's safe. The safe manufacturer therefore gives his customer advice on the basic principles of good combinations and on how to set them in the safe. Similarly, the purpose of this leaflet is to provide you with a sufficient understanding of our machine type CX-52 to enable you to create a unique machine and a usage tailored to your needs. Naturally we will always be delighted to give further explanation of the principles outlined here, and advice on how to cope with particular requirements not adequately covered.

B. Cryptographic principles of the Hagelin cryptographer type CX-52.

Our machine type CX-52 has been produced in many versions to meet the most exacting preferences of our customers. The most important advance over the machine type C-52 is the incorporation in the type CX of irregular advancement of the keywheels. The machine type C-52 produces, by a constant stepping of the keywheels, a very long keying chain which is the major factor in the ciphering. In the machine type CX-52, the advancement of the keywheels which interact to produce the key cycle is as irregular and unpredictable as the key chain itself. However, when irregularity is introduced into the stepping of the keywheels, it is necessary to take special precautions in the selection and arrangement of the variable elements which affect the stepping in order to insure that the length of the keying chain is not affected. The problem is how to achieve an ideal balance between the desire for maximum irregularity in stepping of the keywheels, for maximum guaranteed length of the keying chain, and for maximum simplicity in usage.

We consider that our M model of the machine type CX-52 achieves this balance more effectively than earlier models. Only a few simple rules must be observed in placement of the lugs on the drum bars and a keying chain of maximum length is achieved despite irregular advancement of the keywheels throughout the cycle. The M model is used as the basis for this discussion. However, many of the remarks are equally applicable to older models of the machine type CX-52.

In technical terms, the cipher produced by the machine type CX-52 is described as polyalphabetic encipherment of the Vigenere or St. Cyr strip type. That is to say, to encipher a single letter the machine selects one of twenty-six juxtapositions of a pair of alphabets, a new selection being made for each letter as it is enciphered. The secrecy that this machine provides is not due to the availability of twenty-six positionings of the alphabets (a small number for the modern crypto-analyst), but derives from the method of selection among the offsets, which is for all practical purposes absolutely unpredictable. This selection is determined by a key which is over 10,000,000,000 letters long. The principal parts of the machine are in fact used solely for the generation of this key, and the machine is capable of producing over 10^{84} different keys of this length, depending on the selection and arrangement of the variable elements. In addition, the simple external setting of the machine enables the user to begin his encipherment at any point in this key. The method of encipherment employed by the machine may be thought of as one of subtraction, following this rule: let the letters of the alphabet be represented by the numbers from 1 to 26, i.e., A=1, B=2, C=3, . . . , Z=26. Then when a letter is to be enciphered, the machine computes the cipher letter from the plain letter by means of the following formula: K - P = C, modulo 26 — where K is a letter of the key, P is the plain letter to be enciphered, and C is the resulting cipher letter. The cipher letter is further modified by the relative position between the primary and secondary alphabets on the typewheels. This relative setting is also easily altered on the machine, and may be used to provide an additional element of secrecy if desired. Considering this, the complete enciphering equation for the machine is: K - P + S = C, modulo 26 — where S is the numerical representation of the relative position of the typewheels. The value of K changes each time a letter is enciphered. Once more it can be seen that the secrecy provided by the machine depends fundamentally upon the fact that the key is unpredictable; therefore, the solution of the equation is prevented unless the adversary is in possession of your complete selection and arrangement of the variable elements which generate the key and, in addition, the starting point in the key for the particular message, and the relative positions of the primary and secondary alphabets on the two typewheels.

C. Principles of constructing a unique machine; inner settings.

Having shown the significance of the key in encipherment on our machine type CX-52, we are now in a position to discuss the selection and arrangement of the variable elements in the creation of your unique version of our machine. A judicious procedure for this will assure key, and consequently cipher, of the highest quality. The machine type CX-52 comes equipped with a set of six keywheels, each carrying a pin disc. Each pin disc has forty-seven pins around the circumference. The pins on each disc may be set in either of two positions, called "active" and "inactive". The discs are so constructed that each pin may be set without regard to the setting of any other pin. The settings of the pins on each disc are some of the variable elements referred to in the discussion preceding. It may be of interest to show the number of different ways in which the pins may be set. Since each pin may be set in one of two ways and without regard to any other pin, a 47 pin disc, that is, a pin disc carrying forty-seven pins, may be set in any one of 2^{47} different ways, or over 120,000,000,000,000 combinations may be set on one wheel alone. Since the selection of the combination on one of these pin discs in the set of six in no way restricts the selection on any other disc, the total number of ways in which the pins may be set is actually the product of the number possible for each of the six or over 7.7×10^{84}. It can be seen that the possible variations offered by this variable element alone are so vast that they cannot be exhausted: even a lifetime of work with the aid of the best modern computers would not make the slightest impression on a number of this size.

The experts employed by our firm, as well as others we have consulted, recommend that in choosing a pattern for setting the pins, a method be used which is statistically random. One of the simplest methods, and one which is as good as any other we know, consists of flipping a coin once for each pin to be set. If the obverse of the coin turns up, the pin is set in the active position; if the reverse turns up, the pin is set in the inactive position. Another simple method for determining the pin settings is to derive them from a long stream of random numbers by letting the odd numbers represent active pins and the even numbers represent inactive pins. (Do not use such things as tables of logarithms for the number stream, as they are not statistically random.) Of course it is necessary to record the pin settings as they are selected, even though they may be immediately set in a machine, for all machines that are to correspond with one another must have identical pin settings. A convenient format for doing this is shown in Figure 1. An active pin setting may be indicated by the insertion of a plus in the appropriate box and an inactive pin setting by the insertion of a zero. It is evident that one wants to avoid a very uneven distribution of active and inactive pins on any disc: to take an absurdly extreme case, if one happened to make all the pins active on a given disc then its effect would be just the same at all its positions. If you want to be absolutely safe against any danger of an uneven distribution we suggest that you might use some such rules as the following:

1. Do not allow more than three successive pins on any disc to have the same state of activity.

2. See that no more than 26 nor less than 21 of the pins on any disc are active. The closer to 50% the better the pattern will be.

You will find it quite easy to meet these rules by a few changes in your randomly derived pattern. These limitations will reduce the number of possible pin patterns from 7.7×10^{84} to 4.2×10^{83}, an insignificant change in a number of this magnitude. The advantage to be gained by the even distribution of the pins far offsets the reduction in the number of possible pin patterns. Figure 2 shows examples of pin settings.

When a considerable number of machines are to be set up at one time with the same inner settings so as to be able to correspond together, the setting and checking of so many pins may be somewhat time consuming, even with the device provided for the purpose with the machine. In recognition of this problem, we have developed a special device, the type SRP-58 pin setter, for use in these circumstances. It is based on the equipment used in our factory, and will set all of the pins on a single disc at one time in any desired combination with such reliability that no checking of the individual wheels is required. We will be glad to provide particulars on this equipment if desired.

Having selected the pin settings, we turn now to the insertion of the keywheel groups containing the pin discs into the machine. The machine type CX-52 is so constructed that the keywheel groups may be inserted into the

5. Keywheel five steps one step whenever there is an active pin on either keywheels one, two, three or four.

6. Keywheel six steps one step whenever there is an active pin on either keywheels one, two, three, four or five.

The result of the foregoing law of stepping is that, although their progression is irregular, from any initial alignment the six keywheels will step through every possible offset before coming back to the initial setting. This is a cycle of 47^6 or over 10,000,000,000 steps. This can be demonstrated relatively simply.

Let: W_1 = keywheel one, W_2 = keywheel two, etc.
P = number of active pins which must be from 1 to 46.
P_1 = number of active pins on W_1, etc.
Q_1 = number of inactive pins on W_1, etc.

W_1 steps one step with each letter ciphered and therefore cycles every 47 steps. W_2 steps one step every time there is an active pin on W_1, therefore every time W_1 cycles, W_2 steps P steps. P_1 being from 1 to 46 must be prime to 47. Consequently W_1 and W_2 cannot return to their initial alignment until they have stepped through all possible alignments or 47^2 settings. W_3 in a single cycle of W_1 W_2 steps every time there is an active pin on W_1 or W_2. Or inversely it doesn't step only when there are simultaneously an inactive pin on both W_1 and W_2. In 47^2 steps, therefore, W_3 steps $47^2 - Q_1 Q_2$ steps. This number must be prime to 47, therefore W_1, W_2 and W_3 cannot return to their initial alignment until they have stepped 47^3 steps. In the cycle of the first three keywheels W_4 steps $47^3 - Q_1 Q_2 Q_3$. This number must be prime to 47, therefore W_1, W_2, W_3 and W_4 cannot return to their initial alignment until they have stepped 47^4 steps. Similarly the first five keywheels return after 47^5 steps and the entire six keywheels return after 47^6 steps. Therefore from any initial alignment of the six keywheels they will step through every possible alignment or over 10,000,000,000 steps before returning.

In the generation of key if a pin in the active position on the keywheel in the leftmost position is presented for interaction with the bar drum, each bar lug on the bar drum which is in the leftmost position on any bar will add a numerical value of one to the key for the encipherment of the plain letter set on the typewheel. If the pin so presented is in the inactive position, the corresponding bar lugs will add nothing to the value of the key. Likewise, if a pin in the active position on the keywheel in the next to leftmost position is presented, each bar lug in the next to leftmost position on any bar will add a numberical value of one to the key, and so on for all keywheels. It should be noted in this connection, however, that the mechanical process of the machine is such that no matter how many bar lugs are placed on a single bar, the value added to the key by that bar will never be greater than one. Also, a bar lug interacting with a pin in the active position will have exactly the same effect, regardless of which bar it is placed on, so long as it is in the position on the bar corresponding to the position of the keywheel concerned. In an early version of the CX-52 M ciphering machine the first five bars contributed to both the key and the stepping of the keywheels. This complicated greatly the preparation of acceptable lugging patterns. There are also theoretical advantages to a complete independence of the key from the stepping. Consequently on later models of this machine the effect of these five bars has been limited to the stepping of the keywheels.

The combination of these features means that when placing the bar lugs on the drum bars, a simple and systematic procedure can be used, which is both convenient for the person performing the task and subject to very few errors, without in any way reducing the quality of the key or reducing the secrecy provided by the machine. All of the bar lugs which are to be placed in the leftmost position may be put in place at once, beginning with the first bar and proceeding upwards on succeeding bars until the required number have been placed. The bar lugs to be placed opposite the next keywheel may now be put in place, beginning with the next unused bar, and proceeding with the rest in order, and so on. Bar lugs which have been so placed are easily checked to insure that the work has been done correctly, and in addition this sort of arrangement increases the smoothness of operation of the machine, thereby reducing operator fatigue when long messages are to be enciphered. A diagram showing the placement of bar lugs in this fashion may be seen in Figure 4.

Since the individual values of the key are composed of sums of numbers represented by the placement of the bar lugs, and since it is highly desirable to ensure that all key values from zero to twenty-five will be included in the key, it is vital to exercise care in the determination of the numbers of bar lugs to be placed opposite each keywheel. If this is done it is clear that every letter of the clear alphabet will be enciphered by every possible letter of the cipher alphabet with roughly equal frequency. An easy way to meet this condition, and one which takes full advantage of the capabilities of the machine, is as follows: Select six numbers (corresponding to the number of positions on the bars) from one to fourteen whose sum is twenty-seven corresponding to the total number of bars used for generating key. These numbers need not be all different. Observing that there are sixty-four different combinations of pin activity which the keywheels may present to the drum bars at any given time, calculate for each of these combinations of activity what key value would be produced by them in the following way (please refer to Figure 5):

1. Write out all of the possible sixty-four combinations of pin activity. This is readily done in systematic fashion by following the order of binary numbers for those who are mathematically inclined. The ordering in Figure 5 is of this kind; however, the order is immaterial since the combinations will not occur in this or any predictable order in the key. An active pin may be represented by a plus sign and the inactive pins by a zero.

2. Write the set of six numbers selected across the top of the listing. Again the order in which this is done is of no importance. They have been listed in descending order in Figure 5 purely for convenience.

3. Beginning with the first combination, find the sum of all the numbers which are written over a plus in the first combination. Write this sum to the right of the first combination. (If the sum is greater than twenty-five, subtract twenty-six from it, and record the resulting difference rather than the original sum obtained. For convenience on Figure 5 values over 25 are shown beside the number with which they pair. The machine will produce this effect mechanically in the process of encipherment.) Find the sum of all the numbers which are written above a plus in the second combination. Record this sum to the right, as before, reducing it by twenty-six if necessary. Continue in this manner until sums corresponding to each of the sixty-four combinations have been computed. If the pin settings have been chosen in accordance with the principles we have described, all of these combinations will occur in with approximately equal frequency and in a truly unpredictable way in the operation of the machine, so that the result of your calculation with only these sixty-four combinations will be representative of the statistical composition of the key. Examine the results of your calculations. Check to see whether your sixty-four sums include all possible numbers from zero to twenty-five. If they do not, discard this set and begin anew. If all possible numbers from zero to twenty-five are included, the set of numbers which you have chosen may be used as the numbers of lugs to be placed opposite

the keywheels with full confidence that your machine is producing key of the highest quality. While this procedure may seem somewhat labourious at first, a little experience will enable you to correct faults of the original set by altering two or three of the original numbers without changing their sum, and to recalculate only those combinations which are affected by the alteration. A simple rearrangement of the numbers, however, will have the same faults as the original set. Also it will soon be observed that a set of numbers containing one number in the range of ten to thirteen and another in the range of six to eight will obey this rule much more often than a set which does not contain such a combination. Following are a few typical sets which we have tested and found to conform to the rule stated above.

13	6	3	3	1	1
10	6	4	4	2	1
11	7	4	2	2	1
14	6	3	2	1	1
14	7	3	1	1	1
12	6	4	2	2	1

It will be observed that no set in our example can be rearranged to form any other set. While it is true that the machine can be made to produce an entirely different key by merely rearranging the numbers in a set without changing their values, the effect of such a rearrangement may be obtained by merely rearranging the keywheels in a corresponding manner. This is a much simpler and quicker procedure than removing and replacing the bar lugs. The computation of the number of cryptographically different arrangements of bar lugs on the drum bars is somewhat complex. Suffice it to say here that there are approximately 65,000. Any one of these, of course, may be used in combination with any one of the enormous number of combinations of pin settings which are possible, each combination being in effect a different machine, producing a different key from any other machine.

This completes the discussion of what are called the "inner" variable elements of the machine type CX-52. When all the pins, the keywheels, and bar lugs have been positioned according to your selection, the inner cover of the machine may be locked, using the key with two notches. These are the variable elements of the machine which, taken together, constitute your personal machine and which must be most carefully protected. If it ever

No.

is suspected that these elements have been compromised, they should be changed at once. The machine may be used without opening the inner cover for any purpose, and a separate key is provided which will lock and unlock only the outer cover. This feature is of great assistance in preventing unauthorized persons from viewing the elements of your personal machine, even though they may see the machine in operation. The clerk who carries out the actual encipherment of correspondence has no need for access to these inner settings, as we shall see, and it is a good practice to provide him only with the key with the single notch which will open the outer case only, the double-notched key being retained in the custody of special personnel.

D. Principles of machine usage: outer settings.

The usage of your machine type CX-52 is an integral part of your over-all plan for secret correspondence, and no usage plan can be drafted without a careful analysis of your secret correspondence needs. Since every user has different secret correspondence requirements, there is no one best plan for secret correspondence and in turn no one best usage of the machine type CX-52. Nevertheless, just as in the case of the selection of inner settings, there are principles valid for all cipher machines which apply to usage and the selection of the outer settings. The first of these, which should be kept in mind at all times, is: the simpler the plan for secret correspondence, the better it will be. Every complication will increase the difficulty of achieving effective correspondence, and its value must be carefully weighed against its cost in operating difficulties. The design of our machine type CX-52 is such that complete secrecy can be achieved with procedures of the utmost simplicity, making tedious and complicated cryptographic procedures altogether unnecessary.

To prepare a secret correspondence plan, you should first determine:

1. The number of correspondents involved.

2. With whom it is necessary for each of them to correspond.

3. Approximately how many messages will be exchanged in each case.

4. Whether there is any special need for "privacy" among certain correspondents.

5. Whether any of the above listed circumstances are subject to unexpected change.

After carefully analyzing the data collected, the planner should determine the simplest correspondence plan which will meet all the requirements. The requirement which most seriously complicates all secret correspondence plans is the "privacy" requirement, that is, the desire to limit to an extent the ability of some of the correspondents to decipher certain messages not intended for them. Fortunately, the design of the machine type CX-52 is such that this can be done merely by the preparation of a separate set of instructions for the outer settings without resorting to a change in the inner settings. The simplest possible situation for the planner of the secret correspondence exists when there is no objection to any individual correspondent who is an authorized holder of the machine being able to read any message enciphered on the machine, which may not be intended for him but accidently comes into his possession. In such a situation, a single set of usage instructions may be prepared for all correspondents, following one of the systems for selecting outer settings which we shall describe below. In such a case, each correspondent may address every other correspondent without having to resort to special instructions with the attendant danger of selecting the wrong ones, and thus sending a message which cannot be read by the intended recipient. On the other hand, if a compromise both of the inner settings and of the instructions should occur in the office of one of the correspondents, then the correspondence of all may be endangered; therefore, when a plan of this kind is in use, all correspondents must provide the greatest possible protection to the usage instructions and to the machine itself.

When a need for limiting the ability of the correspondents to decipher messages to those actually intended for them exists, it is likely to arise from one of the following situations:

1. The location of one or more of the correspondents is such that the materials he holds are especially vulnerable to compromise.

2. Correspondence on a particular subject is regarded as being more secret than others, and must have special protection to prevent those having no need for the information from receiving it. When one of these requirements exists, it is necessary to prepare a separate set of instructions for each group of correspondents having the need to correspond among themselves. This may be regarded as the preparation of several separate correspondence plans of the simpler type, with some correspondents being each a member of a multiplicity of plans. The advantage of conducting the secret

correspondence in this manner, in addition to meeting the special "privacy" requirements, is that if one set of instructions is compromised, only that part of the correspondence which was enciphered using those instructions can be in danger. The rest of the correspondence is unaffected. On the other hand, no matter how extreme the requirement for privacy is, there will almost certainly be messages which must be sent to nearly all correspondents at once, and then either an additional set of special procedures is required or the same message must be enciphered according to several different sets of instructions, either of which imposes a burden on the central office. The problem can become still more complicated if there is a requirement for flexibility and a need to handle sudden changes and emergencies.

It may happen that in determining the requirements for the secret correspondence plan, it will be found that the number of messages to be exchanged among some correspondents is very much larger than the number to be exchanged among others. While the machine type CX-52 offers a very high speed of encipherment for a hand-operated machine, where really large volumes of correspondence must be enciphered there is a definite advantage to an electrical machine. At the same time, it is most undesirable to complicate the secret correspondence plan by providing different ciphering machines to correspondents merely because of a different volume of work. In recognition of this very troublesome problem, we have designed an electrical base for your machine type CX-52 which will convert any model type CX-52 into an electrical ciphering machine in a matter of minutes. The converted machine is absolutely compatible with the hand-operated model, and all of the same usage instructions may be employed. It is operated by a keyboard, offering nearly the same speed as a typewriter. The production and sale of this as an accessory, rather than offering a separately designed and built electrical machine, results in great flexibility and economy for the customer. Where the budget is small, it is possible to begin operation with the full secrecy of the machine type CX-52, but without the expense of purchasing all electrical equipment. Then as the funds are available, or as the amount of enciphering increases, the original machines may be converted a few at a time to electrical operation, without incurring any conversion problems whatsoever or any greater expense than would have been involved in purchasing all electrical equipment originally. In the initial purchase of machines, it is often found to be desirable to purchase electrical bases for those correspondents having a great deal of enciphering to do, such as the central office and a few large posts, and allow all others to use the manually operated machines. Further, so that the smallest outpost may correspond with the largest and most modern automated communication center, without complicating the secret correspondence plan in the least, we have available an attachment, PE 61, for the machine type CX-52 which will produce the enciphered message on perforated paper tape in a form ready for input to automatic communication facilities, and will accept an enciphered message on perforated tape and decipher it automatically.

Having considered all of the factors listed, the planner must determine the absolute minimum number of separate instructions necessary to satisfy the conditions and proceed to prepare them. Let it be noted once more that no information about the inner settings is necessary for the operator of the machine. Every precaution should be taken to insure that no such information is contained in the usage instructions. It will be remembered that the complete inner and outer settings are required for an adversary to decipher your correspondence, and by keeping information concerning the inner settings out of your usage instructions, you will protect the correspondence even when the usage instructions are compromised.

The two problems of usage are first the method of selection of the variable elements for the outer settings, and second the method of informing the intended recipient of the message of the selection that has been made. The variables to be chosen for the outer settings are the relative position between the primary and secondary alphabets on the typewheels, referred to in section B, and the keywheel alignment. The keywheel alignment is the sequence of letters and numbers, one on each keywheel, which is visible through the slots on the front of the machine and in a line with the white index line. The keywheels are easily moved by hand, one at a time, to bring any desired keywheel alignment into place, and it is this window setting that determines the starting point in the key to be used to encipher the message. The relative position between the primary and secondary alphabets on the typewheels may be adjusted merely by separating the two typewheels and rotating one of them until the desired letter is brought into juxtaposition with the A on the other. (Please see our leaflet No. A 035.) The keywheel alignment should be changed with the encipherment of every message, for as in all known methods of encipherment, if sufficient messages are enciphered with all of the variable elements exactly the same, the encipherment of the messages is vulnerable to attack by a skilled adversary. Sometimes the relative position between the two typewheels is also changed as each new message is enciphered. More commonly it is kept the same at all times between chosen correspondents or for fixed time periods for all correspondents. Once outer settings are selected for the message, they must be transmitted to the recipient. The secrecy provided by the CX-52 is so great that even if the outer settings for a message are known to the adversary, he will be unable to read the message unless he is also in possession of the inner settings of the machine. However, the sending of the outer settings openly or en clair to the recipient should never be engaged in as a regular practice. If the inner settings have been compromised without your knowledge, the message can be read in such a circumstance; or if the inner settings should be compromised some time in the future, all messages which have been handled in this way may be read. Furthermore, it is characteristic of all known ciphering systems, that if a large enough number of messages of which the precise keying elements are known are collected together, some further information about the method of encipherment may possibly be deduced by a skilled adversary. Therefore it is desirable to conceal this kind of information.

As in the selection of the pin settings for the inner settings of the machine, nothing better than selection at random can be recommended for the selection of the variable elements in the outer settings of the machine. The number of choices possible for the keywheel alignments (over 10,000,000,000) is so vast that the chance of repeating an alignment purely by accident is so small as to be negligible. This random selection may be performed in advance by a central bureau and lists provided to the correspondents, or the selection may be performed by the clerk who enciphers the messages. Advance preparation of lists has the advantage that they can be prepared under ideal conditions at a central office by experienced personnel. Every requirement for limited ability to decipher will require a separate list. They are quite satisfactory for correspondence between a limited number of correspondents under stable conditions; however, a secret correspondence plan which makes use of these lists tends to be inflexible and unable to cope with emergencies or unexpected communications needs. For instance, correspondents under the secret correspondence plan, who do not normally correspond with one another, may not have been provided with a common list; then an unexpected need for them to correspond will necessitate their doing so through the central office where all lists are held, a very slow and frequently expensive procedure. If there is a large number of correspondents, and if it is desired to limit the reading of correspondence by certain of them, the number of lists involved and the complications ensuing tend to discourage their use. If, however, the communications plan is such that the use of lists is practical, it is desirable that there be no means by which the listed outer settings can be associated correctly with specific messages if the list should be compromised. This may be achieved by having the code clerk select in a random manner from the list rather than use it in order, and providing him with a secret means of indicating his choice to the recipient. This may be done in a number of ways, some simple and some complex. One way is to prepare the lists in a format with coordinates similar to those used on maps. The choice from the list may then be indicated by placing the coordinates of the chosen window setting at the beginning of the enciphered text. If many lists are in use, it will also be necessary to indicate which list was used by adding a letter or number to identify the list. Outer settings which are selected from a prepared list may also be enciphered in the same manner as that described for settings which are chosen directly by the code clerk.

Leaving the random selection of the outer settings to the code clerk has several advantages. It requires the smallest possible amount of secret material to be contained in usage documents, leaving less to be lost in the event of a compromise. It is practical even under very complicated secret correspondence plans and is flexible enough to be readily adapted to almost any kind of change, even the addition of new correspondents to the plan. On the other hand, leaving the determination of the outer variables to the discretion of the code clerk has the disadvantage that it is difficult to force him to select the variables in a truly random manner. This, however, can be overcome by a variety of simple devices in the usage instructions, telling the code clerk how to proceed to select the outer settings in a random fashion.

Whichever method of selecting outer settings is chosen, it will be necessary to encipher the choice and transmit it to the correspondent who is to decipher the message. One of the simplest and safest ways of doing this is to encipher the outer settings (or the coordinates giving their location in the prepared list) on your machine type CX-52. Not only is this the safest way, but also the flexible design of the machine type CX-52 allows you to create limitations for privacy requirements through a simple and elegant variation of this method (see Figure 7). To begin with, all those who must correspond with one another are supplied with a single "basic" outer setting. This consists of six letters or numbers for the keywheels and one letter for the relative setting of the two typewheels (if used). To encipher the outer settings which have been selected for the message, either from a prepared list or chosen by the code clerk, (or even the coordinates giving the location of a window setting and slide in the prepared list) the basic outer settings are set on the machine in the normal fashion and the chosen settings for the message enciphered in the same manner as you would encipher a message. It is desirable, for the sake of reliability, to repeat the message outer setting and encipher the resulting twelve letters. Then in the case of transmission by radio, or other corrupting influence, a check is provided on the receipt of the correct version. This will result in twelve letters, or three groups, which must be sent with the enciphered message, and which are on the surface completely indistinguishable from the message itself. Having enciphered the outer settings for the message on the basic setting provided for the purpose, the chosen setting for the message is now placed on the machine and the encipherment of the message can proceed. The recipient of the message has only to repeat this simple procedure to obtain the outer settings necessary to decipher the message. First he sets the prearranged basic outer settings on his machine and deciphers the first twelve letters of the message, thereby obtaining the outer settings for the message. He then sets this outer setting on his machine and proceeds to decipher the message. It can be seen at once that the proper outer settings to decipher the message cannot be ascertained by anyone who does not have possession of the prearranged basic settings and in addition the inner settings of your personal machine. Furthermore, an absolute minimum of secret material is required, so small it is in fact that it may even be memorized in case of real necessity. Now, if it is desired to create a special usage for correspondents requiring privacy, it is only necessary to provide them with a special basic outer setting for the encipherment of their message outer settings. No one not in possession of the basic settings can determine the proper setting for deciphering the messages, thus the requirement for limitation of those who can decipher the correspondence is met with both certainty and ease.

Returning now to the matter of the selection of the outer settings used each one by itself, then advance any keywheel showing a number to the next letter. This may then be taken as the keywheel alignment to be used for the encipherment of the message. Another simple method is to place a pencil point at random on a newspaper and set the keywheels in accordance with letters selected in this way. Any procedure that will serve to discourage the code clerk from repeatedly selecting the same outer settings will serve.

E. Summary.

In the machine type CX-52, you have purchased a machine of the most advanced cryptographic design, and the utmost in mechanical reliability and operational flexibility. To obtain the full benefit of the secrecy which this fine equipment provides, only the following simple rules need be followed.

1. Prepare your personal, inner settings in accordance with our suggestions given above, i.e., select the pin settings at random and test the numbers of bar lugs to be attached to the drum bars in accordance with the procedure given.

2. If it is ever suspected that the inner settings have fallen into the hands of an adversary, change them at once.

3. When messages are to be enciphered on the machine, select the outer settings at random and transmit them to the recipient in a secret form.

4. Exercise caution in the selection of the outer settings so that the same outer settings are not used repeatedly on different messages.

For correspondents who need to encipher a large volume of material, various attachments to speed the work and to make the machine type CX-52 compatible with automatic facilities are available. For those having only a few messages each week, the hand-operated models are most economical and reliable.

In planning the correspondence, introduce no needless complications, but provide through simple variations for the privacy of special correspondents when required. In preparing instructions for your code clerks, remember that they will do the best and fastest work if the procedures are simple, fixed, short, and as interesting as may be.

HAGELIN-CRYPTOS

KEYWHEEL

DIVISION	A	B	C	D	E	F
01						
02						
03						
04						
05						
06						
07						
08						
09						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						

Format for Recording Pin Patterns.

No.

KEYWHEEL

DIVISION

	A	B	C	D	E	F
1	+	O	+	+	O	O
2	+	O	O	O	+	+
3	O	+	+	O	O	O
4	O	O	O	+	O	O
5	+	O	O	+	+	+
6	+	O	+	O	O	O
7	O	+	+	+	+	O
8	O	+	O	+	+	+
9	O	+	+	+	O	O
10	+	O	+	O	O	+
11	O	O	O	+	O	O
12	+	+	+	O	+	+
13	+	+	O	O	O	+
14	O	O	+	+	+	O
15	+	+	O	O	O	O
16	O	+	+	+	+	+
17	O	+	O	O	+	O
18	O	O	O	+	+	+
19	+	+	+	O	O	O
20	+	+	O	O	+	O
21	O	+	O	+	O	+
22	+	O	+	+	O	O
23	+	O	O	+	+	+
24	O	O	+	O	O	O
25	+	+	O	+	O	+
26	O	O	+	+	+	+
27	+	O	+	O	O	O
28	+	+	O	O	+	+
29	O	O	+	+	+	O
30	+	O	O	O	O	+
31	+	+	+	+	O	+
32	O	O	O	O	+	+
33	O	+	+	O	O	O
34	O	+	+	O	+	O
35	+	O	O	+	O	+
36	O	O	+	+	+	O
37	O	O	+	+	+	+
38	+	+	O	O	O	O
39	+	+	+	O	+	O
40	O	+	O	+	O	O
41	O	O	O	O	O	+
42	+	+	O	O	+	+
43	+	O	+	O	O	O
44	O	O	O	+	+	O
45	O	+	O	O	O	+
46	+	O	O	O	+	+
47	O	+	+	+	+	+

Example of Typical Set of Pin Patterns

No.

CRYPTO AG. ZUG (Schweiz)

Figure 2

25.11.64

13	7	3	2	1	1	
O	O	O	O	O	O	0
+	O	O	O	O	O	13
O	+	O	O	O	O	7
+	+	O	O	O	O	20
O	O	+	O	O	O	3
+	O	+	O	O	O	16
O	+	+	O	O	O	10
+	+	+	O	O	O	23
O	O	O	+	O	O	2
+	O	O	+	O	O	15
O	+	O	+	O	O	9
+	+	O	+	O	O	22
O	O	+	+	O	O	5
+	O	+	+	O	O	18
O	+	+	+	O	O	12
+	+	+	+	O	O	25
O	O	O	O	+	O	1
+	O	O	O	+	O	14
O	+	O	O	+	O	8
+	+	O	O	+	O	21
O	O	+	O	+	O	4
+	O	+	O	+	O	17
O	+	+	O	+	O	11
+	+	+	O	+	O	24
O	O	O	+	+	O	3
+	O	O	+	+	O	16
O	+	O	+	+	O	10
+	+	O	+	+	O	23
O	O	+	+	+	O	6
+	O	+	+	+	O	19
O	+	+	+	+	O	13
+	+	+	+	+	O	0

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

NO. OF OCCURRENCES OF EACH SUM

SUM		NO
0	26	2
1	27	3
2		2
3		3
4		3
5		2
6		2
7		2
8		2
9		2
10		3
11		3
12		2
13		3
14		3
15		2
16		3
17		3
18		2
19		2
20		2
21		2
22		2
23		3
24		3
25		3

Note: This is an extremely good bar lug pattern. It is possible for any clear text letter to be enciphered by every cipher text letter with as equal a probability as feasible.

Procedure for Testing Bar Lug Patterns.

No.

Figure 5

4	4	4	4	4	4	
O	O	O	O	O	O	0
+	O	O	O	O	O	4
O	+	O	O	O	O	4
+	+	O	O	O	O	8
O	O	+	O	O	O	4
+	O	+	O	O	O	8
O	+	+	O	O	O	8
+	+	+	O	O	O	12
O	O	O	+	O	O	4
+	O	O	+	O	O	8
O	+	O	+	O	O	8
+	+	O	+	O	O	12
O	O	+	+	O	O	8
+	O	+	+	O	O	12
O	+	+	+	O	O	12
+	+	+	+	O	O	16
O	O	O	O	+	O	4
+	O	O	O	+	O	8
O	+	O	O	+	O	8
+	+	O	O	+	O	12
O	O	+	O	+	O	8
+	O	+	O	+	O	12
O	+	+	O	+	O	12
+	+	+	O	+	O	16
O	O	O	+	+	O	8
+	O	O	+	+	O	12
O	+	O	+	+	O	12
+	+	O	+	+	O	16
O	O	+	+	+	O	12
+	O	+	+	+	O	16
O	+	+	+	+	O	16
+	+	+	+	+	O	20

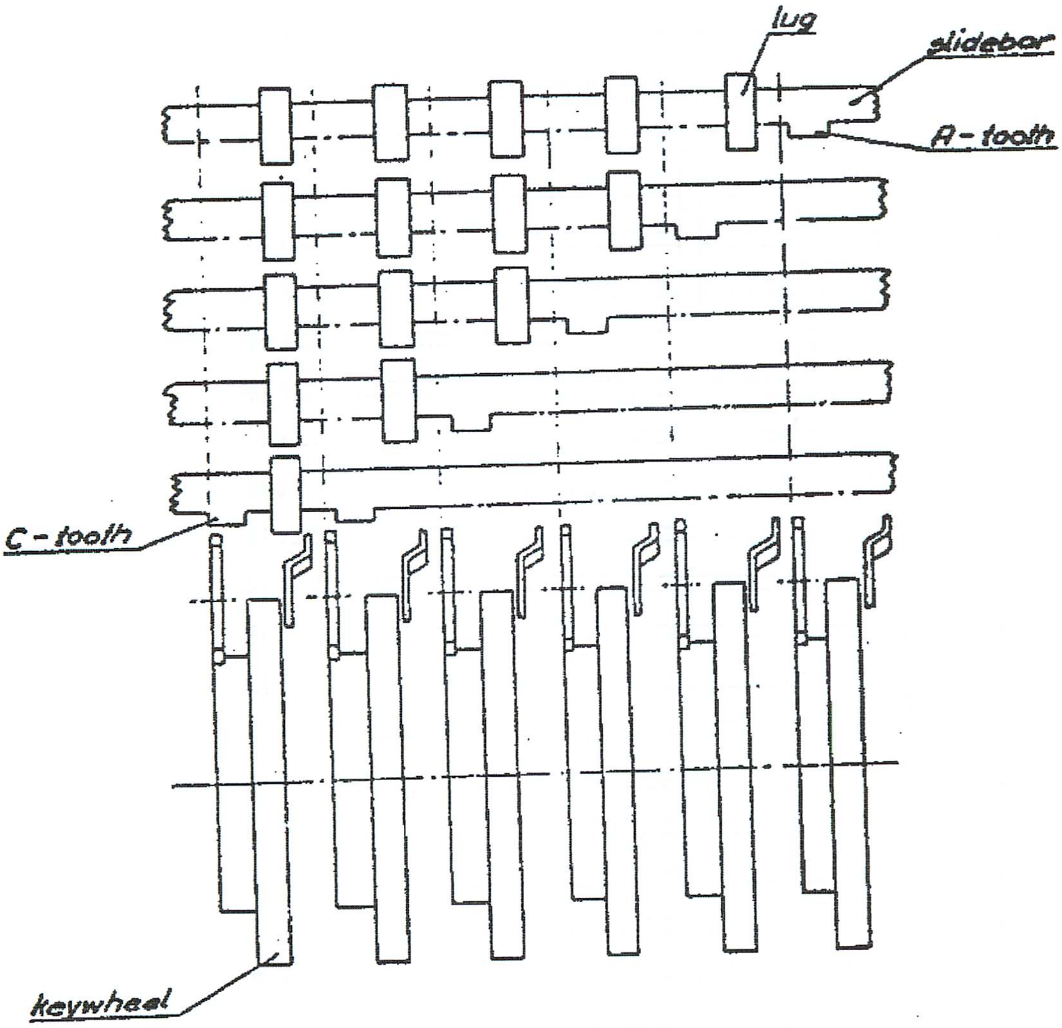
4	4	4	4	4	4	
O	O	O	O	O	+	4
+	O	O	O	O	+	8
O	+	O	O	O	+	8
+	+	O	O	O	+	12
O	O	+	O	O	+	8
+	O	+	O	O	+	12
O	+	+	O	O	+	12
+	+	+	O	O	+	16
O	O	O	+	O	+	8
+	O	O	+	O	+	12
O	+	O	+	O	+	12
+	+	O	+	O	+	16
O	O	+	+	O	+	12
+	O	+	+	O	+	16
O	+	+	+	O	+	16
+	+	+	+	O	+	20
O	O	O	O	+	+	8
+	O	O	O	+	+	12
O	+	O	O	+	+	12
+	+	O	O	+	+	16
O	O	+	O	+	+	12
+	O	+	O	+	+	16
O	+	+	O	+	+	16
+	+	+	O	+	+	20
O	O	O	+	+	+	12
+	O	O	+	+	+	16
O	+	O	+	+	+	16
+	+	O	+	+	+	20
O	O	+	+	+	+	16
+	O	+	+	+	+	20
O	+	+	+	+	+	20
+	+	+	+	+	+	24

NO. OF OCCURRENCES OF EACH SUM

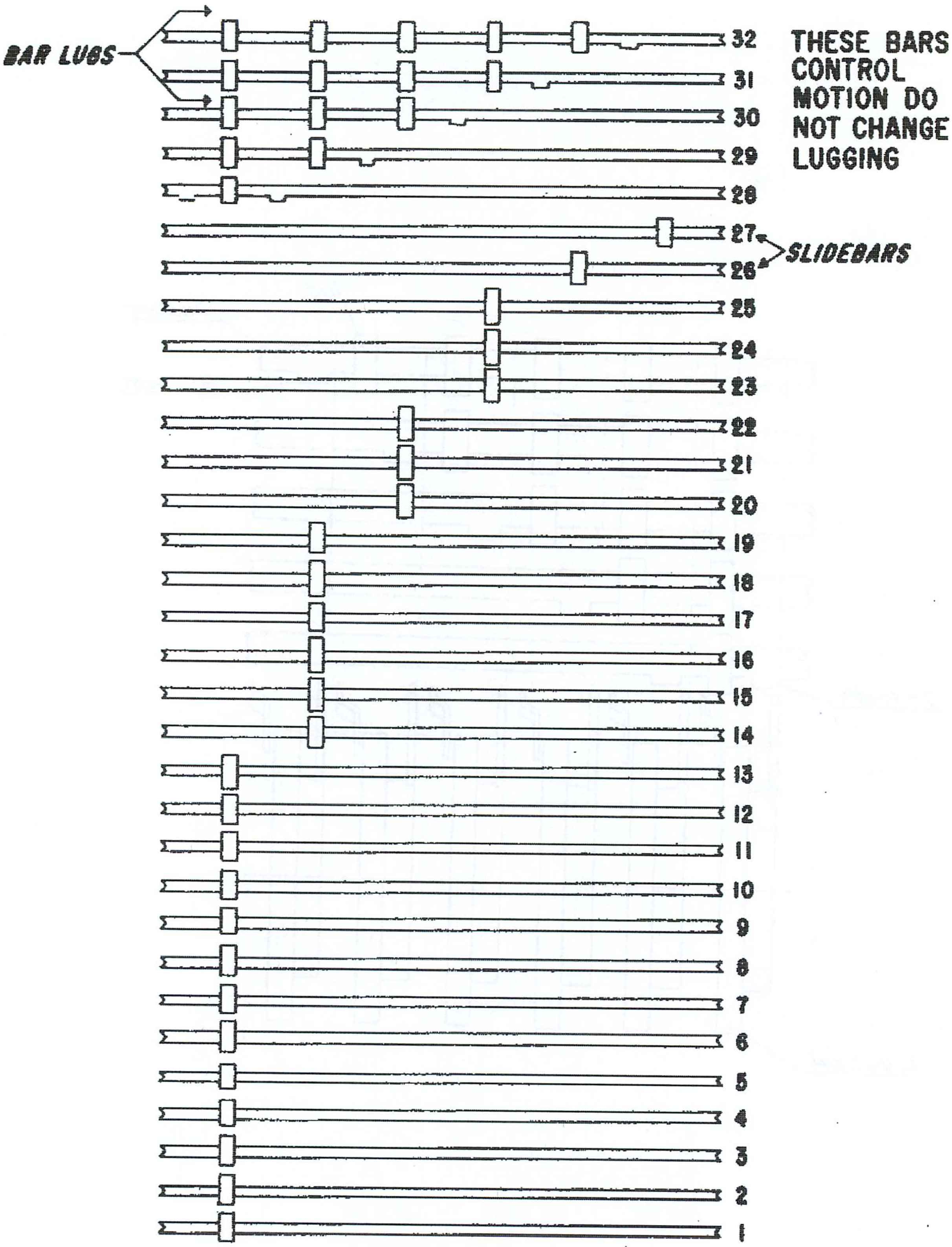
SUM	NO.
0 26	1
1 27	–
2	–
3	–
4	6
5	–
6	–
7	–
8	15
9	–
10	–
11	–
12	20
13	–
14	–
15	–
16	15
17	–
18	–
19	–
20	6
21	–
22	–
23	–
24	1
25	–

Note: This bar lug pattern is most unacceptable because only seven key values are used and these vary widely in frequency. It is not possible for a given clear text letter to be enciphered by every cipher text letter.

Example of Unacceptable Bar Lug Pattern	No.



	No. [illegible]
Placement of Lugs on Bars Controlling Motion, CX-52M	[illegible]
	Figure 3
CRYPTO AG. ZUG (Schweiz)	[illegible]



No.

Figure 4

CRYPTO AG. ZUG (Schweiz)

It is desired to encipher a message using a basic setting technique, prearranged basic being K L Q H N Z.

The operator sets the six keywheel groups in his machine so that the six prearranged letters K L Q H N Z appear against the index line.

The operator next selects at random by any convenient means six letters. Let us suppose he selects W M Z C F L. He writes this out repeated, i.e., W M Z C F L W M Z C F L.

He enciphers this twelve-letter group on his machine set at the prearranged basic. The resulting twelve letters, let us suppose Q L C N F - R Z Z N P - S Y, are his indicator group and are placed as the first twelve letters of the cipher text.

Next the operator resets the six keywheel groups to W M Z C F L and enciphers the message. It is urged that external information such as message numbers, classification, address information, etc. be reduced to a minimum as such data is of considerable value to enemy analysts. All possible data of this type should be enciphered with the clear text as part of the message.

The recipient of such a message sets up the prearranged basic K L Q H N Z on his machine and proceeds to decipher Q L C N F - R Z Z N P - S Y. If the message is not corrupt he will get W M Z C F L W M Z C F L. The repetition confirms he is proceeding properly.

Next he sets up the indicated outer setting W M Z C F L on his machine and deciphers the message proper.

Should a letter in the indicator be corrupted in transmission so that the recipient when he deciphers gets a conflict, as W M Z C F L X M Z C F L, the difficulty is readily apparent and in two trials the message will be deciphered. It is rare that more than a single letter will be corrupt. Such a procedure insures that the message will not be delayed by corruption.

Obviously there are many variations of this method. The message outer setting W M Z C F L could have been enciphered after the message and the result placed on the end of the cipher.

This basic setting technique has the additional advantage of concealing the message indicators.

Example of Basic Setting Technique of Message Encipherment.	No.
	Figure 7
CRYPTO AG. ZUG (Schweiz)	25.11.64