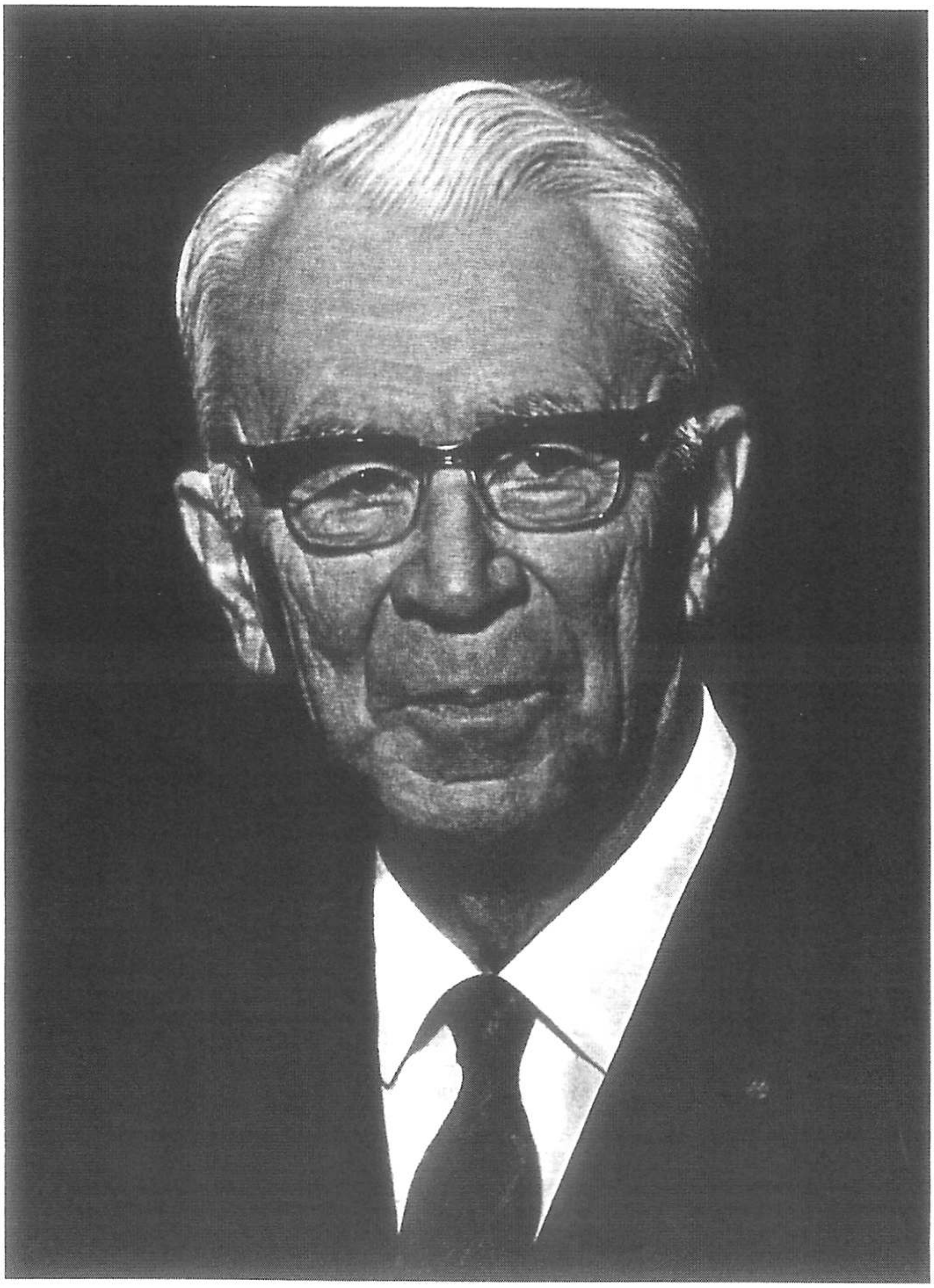
CRYPTO AG

The Story of the HAGELIN-CRYPTOS

THE STORY OF THE "HAGELIN CRYPTOS"



Boris Hagelin

3E720

THE STORY OF THE "HAGELIN CRYPTOS"

INTRODUCTION

The "Story of the Hagelin Cryptos" could never have been written if Russia after the revolution had become a democratic republic. The expected defeat of the Bolshevik minority and the return of a moderate government would have caused me to remain an employee of the Nobel Brothers Oil Production Company, and there would have been no CRYPTO AG - the present manufacturer of ciphering machines.

I was born on July 2nd, 1892 in Adschikent, a small summer resort in the Russian Aserbeidjan. My father, a Swede who had been born in St. Petersburg in 1860, was at that time manager of the Nobel company's oilfields and refineries in Baku. He had joined the company in 1879 when it was founded by an older brother of the famous Alfred Nobel. My father was made a director of the company in 1899, and moved with his family to St. Petersburg. I went to a Russian school until 1904, when my father sent me to a Swedish school. After finishing this school I entered the Royal Technical University in Stockholm where I graduated in 1914 with a degree in mechanical engineering. It was taken for granted that my future would lie in Russia with the company, where my father held a leading position and had become the closest friend of Emanuel Nobel, head of this famous family.

My first job would have been the supervision of the construction of an electric power station on one of the Nobel oil fields in Baku. As I was a mechanical engineer, I had first to broaden my knowledge of electrical engineering. Nobels had ordered the equipment from the large firm ASEA in Vasteraos, and therefore it seemed to be a good idea for me to work in different departments of that firm for a year.

However, the Russian Revolution broke out, and it became obvious that the project would have to be delayed until normal conditions returned. I thus stayed on at ASEA in their foreign department since I spoke five languages.

In 1920 the Nobel family made an agreement with Standard Oil Company, N.J. for a future collaboration in Russia, and I was sent to the USA where I worked in their general engineering department during 1921. At the end of that year it became clear that stable moderate conditions in Russia could not be expected under the rule of the Bolsheviks, who had in the meantime confiscated all private enterprises, including the Nobel works.

I could have stayed with Standard Oil, but I did not feel at home in America and wanted to get back to Sweden. There was no future for me in the oil business but my ties with Emanuel Nobel remained unbroken. The Nobels managed to retain their non-Russian businesses, but had to live in exile, like my father.

Emanuel Nobel was very generous towards me and financed the establishing of a small engineering office in Stockholm. During my stay in the USA I had acquired some inventions, which I developed which made me financially independent. The decisive turning point in my life came, however, when Emanuel Nobel entrusted me with the supervision of a small company which he had begun to finance in 1921 -- the A.B. Cryptograph. This company was founded in 1915 with the objective to develop and manufacture ciphering machines invented by the Swedish engineer A.G. Damm. In 1925 I assumed the management of the company as well as the development of saleable products. This was a fascinating task although I did not have any knowledge of cryptography. Mr. A.G. Damm died in 1927. In 1932 the A.B. Cryptograph was liquidated and replaced by the A.B. Cryptoteknik.

A.B. Cryptoteknik manufactured only mechanical and electro-mechanical ciphering machines. After World War II the need for ciphered telegraph transmission became obvious. In order to be able to work without the interference of the Swedish Government -- ciphering machines were at that time considered war material -- I decided to move to Zug, Switzerland. I first collaborated with the Swiss inventor Dr. E. Gretener, but later established a small independent laboratory. CRYPTO AG was incorporated on May 13, 1952, and had at first just one employee. My Swedish activities were transferred to CRYPTO AG, and since the name "Hagelin Cryptos" had already become well known before World War II the enterprise grew so fast that in 1966 a new manufacturing and administration building was built in Zug/ Steinhausen.

The basis for the growth of the CRYPTO AG were the mechanical machines, which were conceived and developed in Sweden -- the original "Hagelin Cryptos". The first products of CRYPTO AG were the "Telecryptos". They were succeeded by the electronic ciphering equipment which have during the last six years become predominant. The old mechanical machines are, in decreasing quantities, still being produced. Without their basis, however, the new developments which have culminated in a large number of different versions would never have evolved. The trade name "Hagelin Cryptos" has therefore been applied to all the different products of CRYPTO AG. It would be presumptious for me to claim the credit for the success of CRYPTO AG, however, it was internationally acknowledged as the most important manufacturer of ciphering equipment before I retired from the company in 1970.

The art of invention -- and I have mainly become known as an inventor -- has for me been sudden ideas or the combination of existing designs for totally different purposes. But the hard detail work to obtain the finished products has been performed by many collaborators, for all of whom I retain a sincere thankfulness. In this context I feel that I must mention several names. First, C.A. Lindmark, who became indispensable to me when I developed my best known machine, the C-type, in 1934.

My son Boris Jr., who met a tragic death in 1970, had an inventive mind, and his contributions when the postwar CX-type was designed were very important. Mr. Oskar Stürzinger, my first employee when I began my activities in Switzerland, developed my original ideas for the "Telecrypto" machines. He also began to experiment with electronic ciphering devices, at first against my wishes, as this new technology was alien to me. To achieve success, however, it is not enough to have an excellent product but also superior management. Here, Mr. Sture Nyberg, who was first the manager and then the director of CRYPTO AG until his retirement in 1976, proved to be the ideal choice. He also contributed by analyzing the security of the machines which were produced.

In closing this introduction I must pay my humble respect to Emanuel Nobel and to my father, without whose financial and moral support during the long and not always easy years of my work with ciphering machines I would remained an insignificant engineer.

Zug, Spring 1981

I. The Beginning

The use of cryptographic methods of various kinds stretches back some thousands of years. A few hundred years ago inventive minds began to make devices to facilitate the process of enciphering and deciphering messages. In 1891 the Frenchman Etienne Bazéries invented a device (Fig. 1), which to the best of my knowledge was still used until World War II. The same principle used by Bazéries had been propounded earlier by the third president of the United States Thomas Jefferson (1743 - 1826) for the construction of a cipher device, but his writings were not discovered until after World War I.

Fig. 1 Cipher Cylinder of General Bazéries

In Sweden too, interest existed very early in the use of mechanical devices for secure communication. My old friend Sven Wäsström, a Swedish cryptologist, has discovered in the national archives in Stockholm some very interesting documents on this subject. In 1786 a Baron Fridric Gripenstierna received permission from King Gustav III to make a cipher device in accordance with Gripenstierna's drawings. In his "submissive" letter to the King, Gripenstierna indicated that he had gotten the idea for the device from his father-in-law, the celebrated inventor Christopher Polheim. The machine itself, unfortunately, has been lost, but the invoice (Fig. 2) by the builder, which is dated August 26, 1786, shows that the device was actually built. A remarkably detailed description allowed CRYPTO AG to produce a replica of this machine (Fig. 3a).

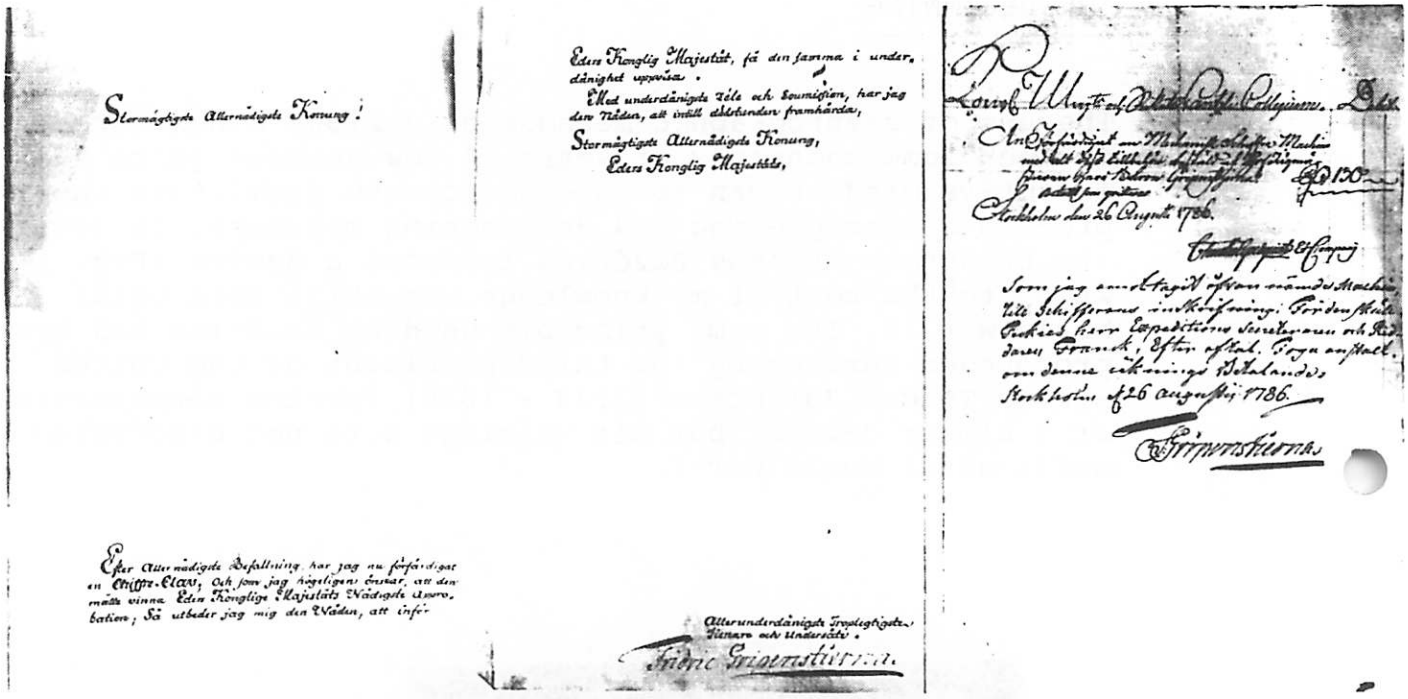
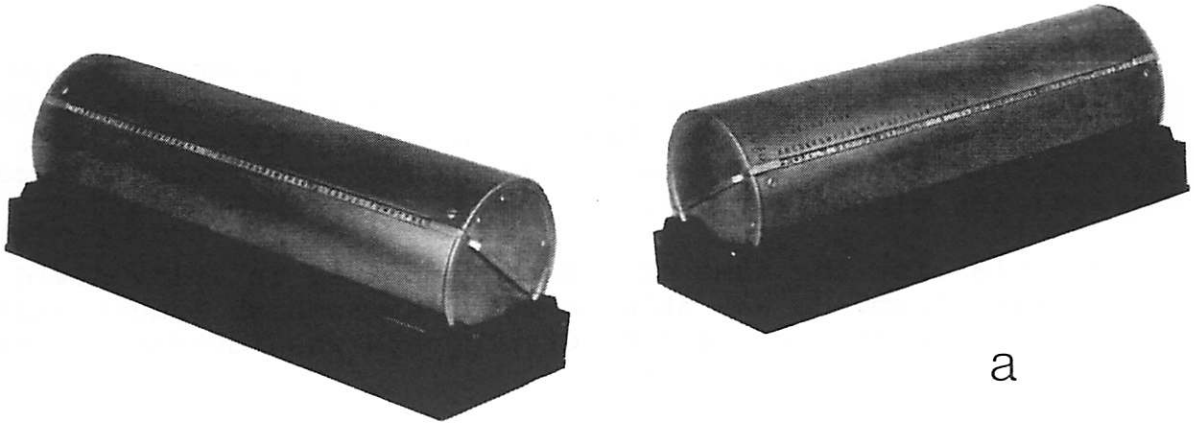


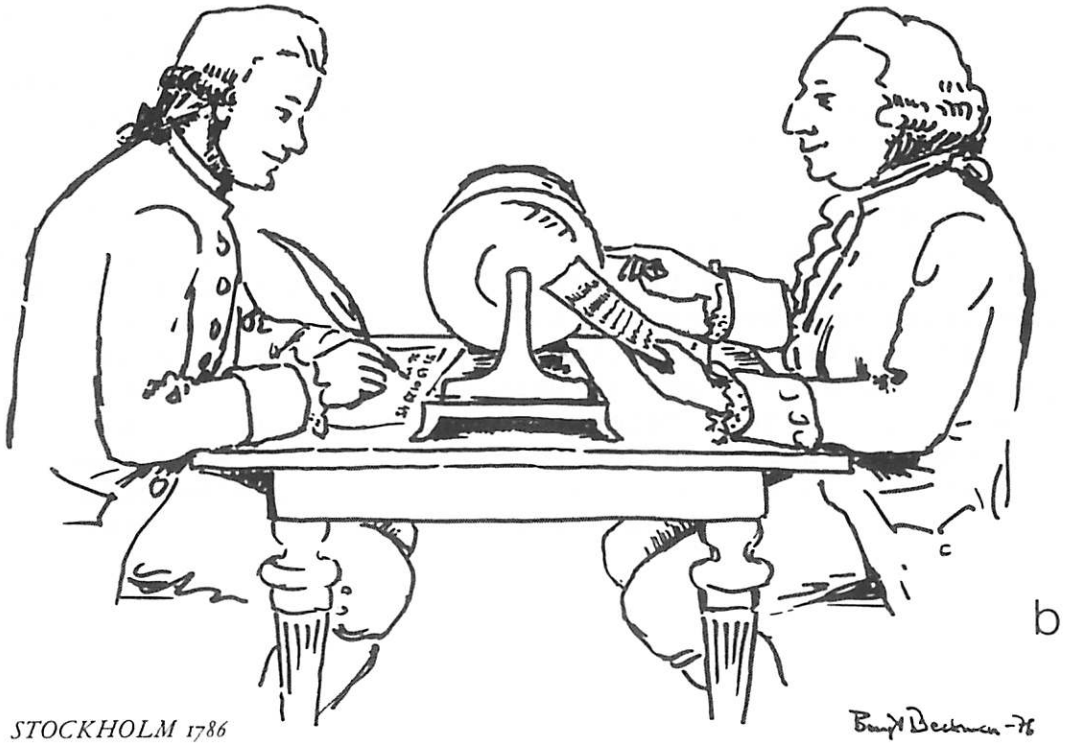
FIG. 2 GRIPENSTIERNA'S INVOICE

This device displays certain resemblances to the one developed much later by Bazéries but far surpassed the French device as far as security and method of operation are concerned. Wässtr intends to publish a study of this earlier device in the next few years.

Gripenstierna's device consisted of 57 disks, each of which carried two alphabets. These disks, mounted on an axle, could all be rotated independently of each other. A longitudinal slit with an index guide on each side of the device exposed two sequences of letters. The authorized person who was to perform the enciphering (at the right in Fig. 3b) adjusted the disks during enciphering so that the plaintext appeared row by row in "his" slit. The assistant (at the left in Fig. 3b) then copied down from the other slit the ciphertext, again row by row. During the decipherment the assistant adjusted the disks to show the ciphertext row by row in the slit on his side. The authorized person then copied down plaintext row by row from his slit. Here we have a modern security concept which separates the ciphering process from the transmission of the cipher.



a



b

FIG. 3 CIPHER MACHINE OF GRIPENSTIERNA

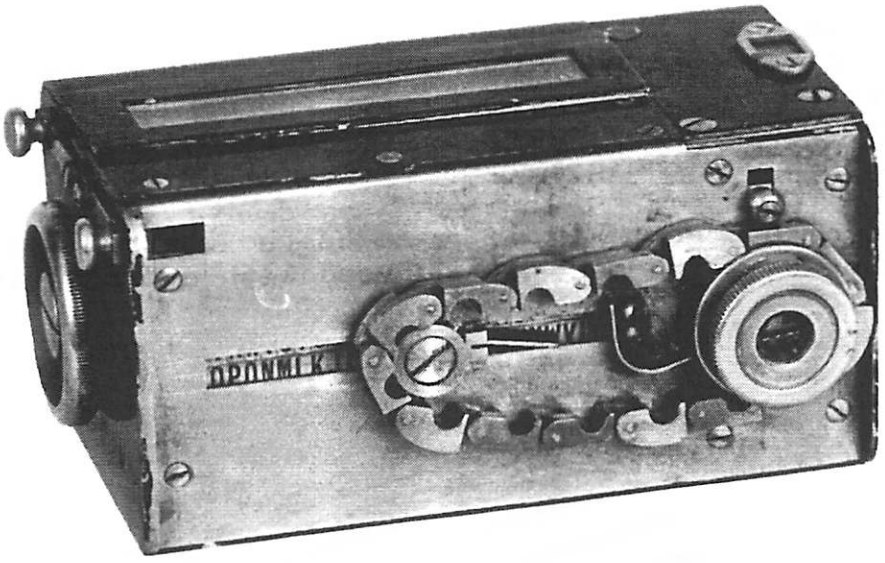
In the 19th century inventors increasingly concerned themselves with the development of ciphering devices and machines. An investigation shows that in the German patent office, which was founded in 1877, about 150 patents were issued before 1927 for cipher devices.

In this list the name of a Swede appeared in 1915: Arvid Gerhard Damm. He was able to interest Swedish industrialists in his inventions and A.B. Cryptograph was founded in 1915 to exploit his inventions.

His first fundamentally sound machine is shown in Figures 4a and b. He used a revolvable drum, on which 26 alphabet strips could be fixed in any desired order. The alphabets were formed so that they could be considered to be a scrambled Vigenere square, with the alphabets in reversed order. Close to the alphabet drum a reference alphabet in the normal order (A...Z) was mounted (the dark strip).

When ciphering, the drum would be advanced one step for each operation, while the reference alphabet could take one of two positions (see Fig. 4b). Through a slit at the top of the machine (Fig. 4a) one could read off the letters to be ciphered from the reference alphabet to one of two drum alphabets. The positions of the reference alphabet were controlled by the chain (Fig. 4b) which advanced one step for each operation. The low links set the referenced alphabet one operation, while the high links set it to the other.

The length of the chain and also the position of low and high links could be varied within certain limits. These options as well as the possibility of changing the relative positions of the drum alphabets made it possible to obtain a large number of different cipher series. The use of reciprocal alphabets made it easy to use the machine, as the reading from the reference alphabet could be done both when enciphering and when deciphering. In emergency cases the machine could be opened and the chain disassembled into the individual links, thus destroying an important key element.



a

b

FIG. 4 A-21 BY ARVID G. DAMM

Using the same principle, Damm also built a number of office machines equipped with keyboards. When a key was pressed, a letter would be exposed below the alphabet strips. During encipherment it would be a ciphertext letter, during decipherment the plaintext letter (Fig. 5).

Here too the chain was used as the controlling element. In operation the machine was used with a protective cover.

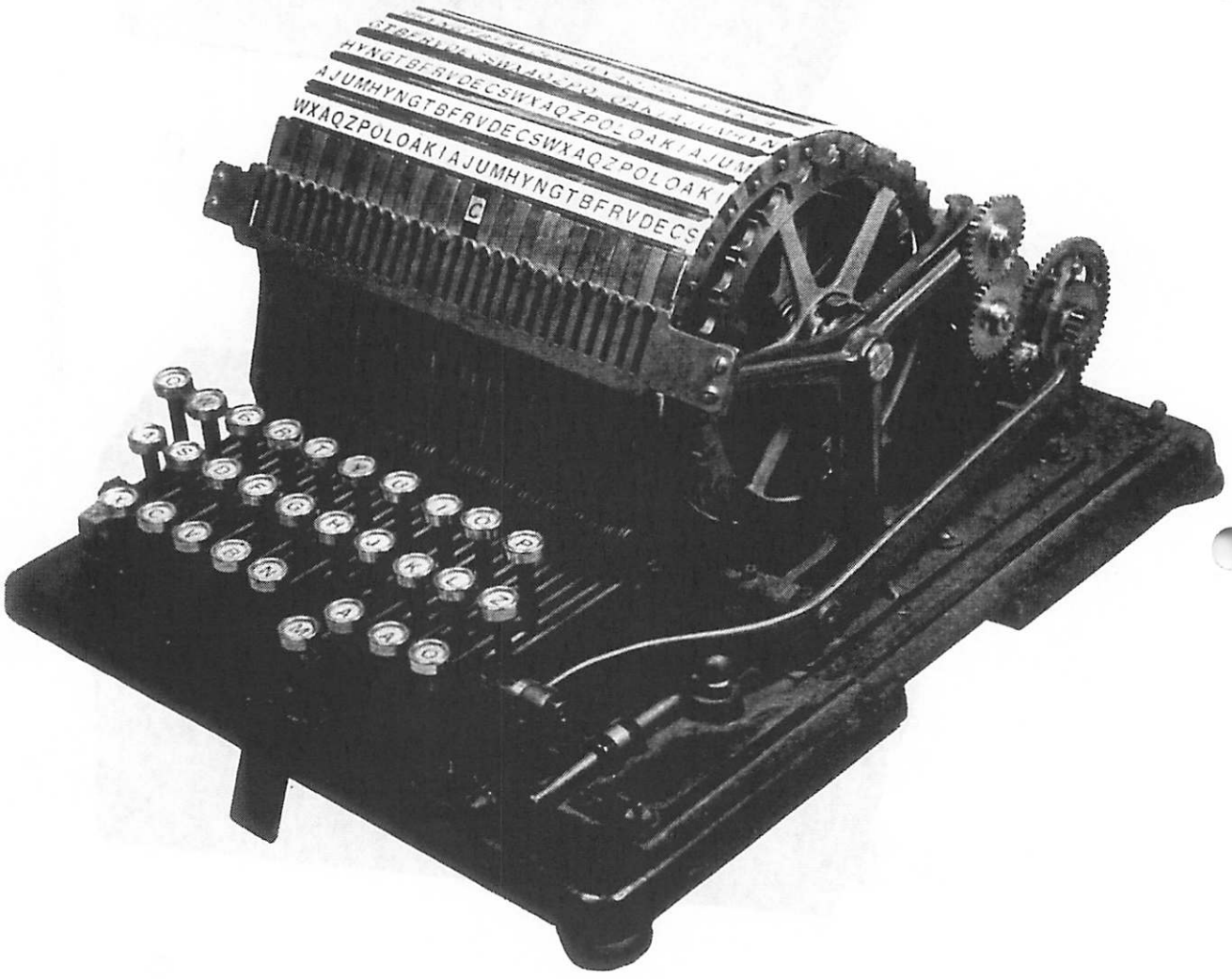


FIG. 5 OFFICE MACHINE BY A.G. DAMM (COVER REMOVED)

He also constructed another purely mechanical machine which printed both the plaintext and the ciphertext. Four of these machines were sold to Japan. Finally Damm invented a system with so-called rotors, i.e., alphabet permutating wheels, an invention which was made at almost the same time by the American Hebern, the Dutchman Koch, and the German Scherbius.

FIG. 6 "MECANOCRYPTO" BY A.G. DAMM

A normal rotor at that time consisted of a disk which had on each of its two faces 26 metal contacts embedded around the circumference. These contacts were connected in pairs through the inside of the disk in a random fashion, one contact on one face connected to one contact on the other face. The best-known machine using rotors was the German "ENIGMA", equipped with 3 or 4 rotors which were set to a new starting position for each message in accordance with the keying instructions. The machine (Fig. 7) was provided with a keyboard and a lamp field. Each lamp was arranged to light up one letter. To operate the machine only a flashlight battery was needed.

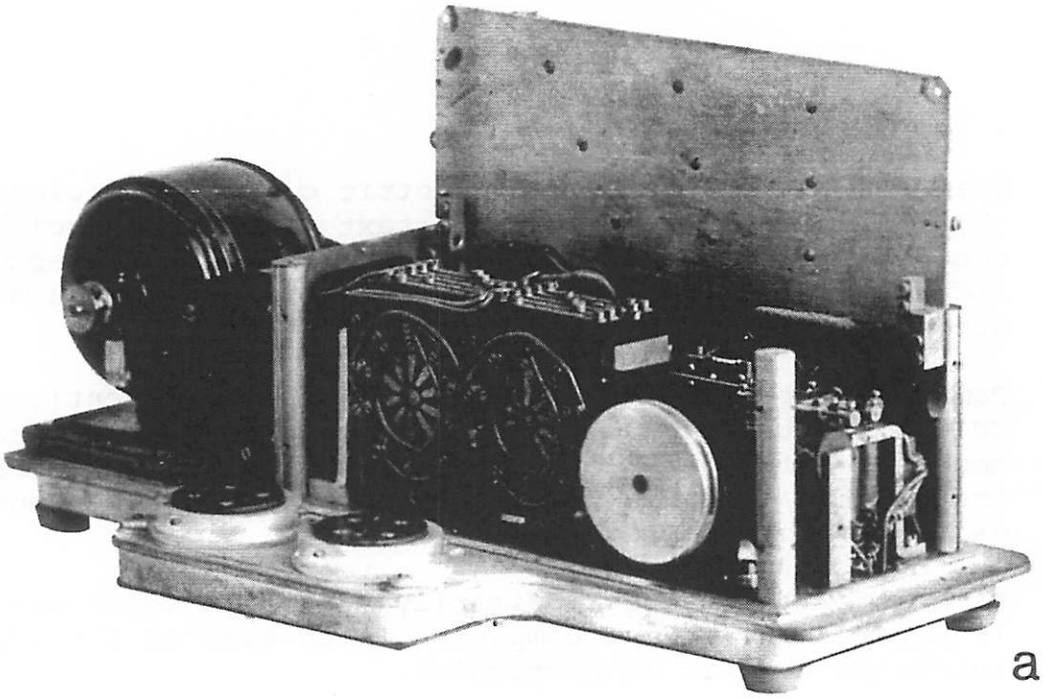
FIG. 7 "ENIGMA" PRODUCED BY CHIFFRIERMASCHINEN AG BERLIN

When a key was pressed, an electric circuit was closed so that in encipherment the ciphertext letter, in decipherment the plaintext letter, corresponding to the key pressed was lighted up. At the same time the rotors were moved step-by-step according to a fixed program.

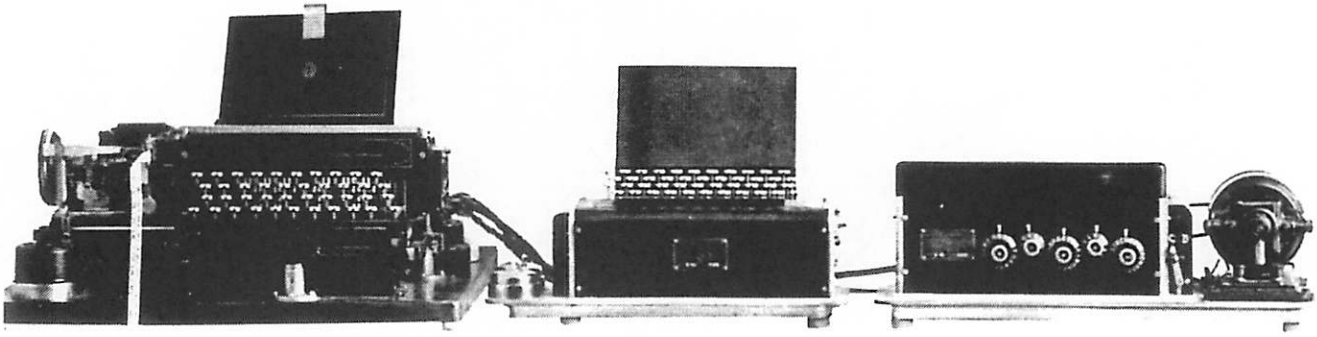
Damm's rotors were constructed somewhat differently from the ENIGMA's but produced a similar effect. They were made for machines which were intended for the ciphering of messages transmitted by radio telegraphy, because such messages could easily be intercepted.

Damm aimed to interest primarily the large telegraph companies in his machine, those companies which handled the transatlantic telegraph traffic in particular.

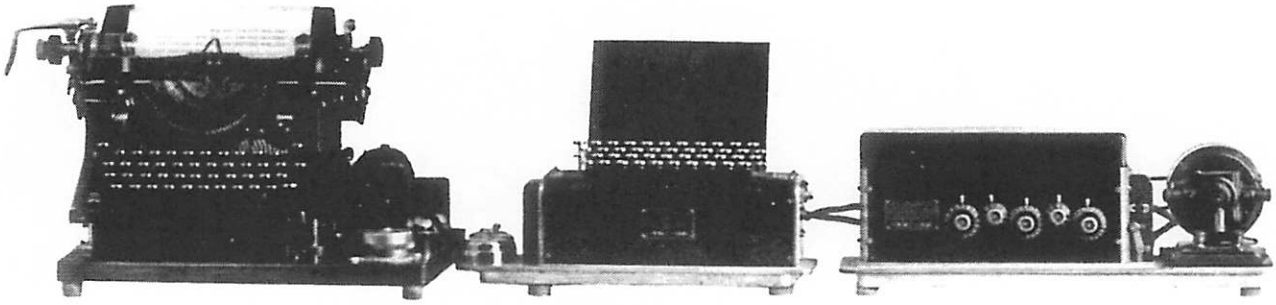
In fact with such machines the radio traffic could have been just as secure as the cable traffic.



a



b



c

FIG. 8 "ELECTROCRYPTO B-18" BY A.G. DAMM

II. The First Machines

When in 1921 the capital of A.B. Cryptograph was exhausted, none of the stockholders would or could make further funds available. However, at this point the director of the company succeeded in interesting Dr. Emanuel Nobel in the A.B. Cryptograph and its possibilities. Because of the Revolution the Nobels had lost their holdings in Russia: a large mechanical factory and the largest Russian Oil firm, the "Nobel Brothers Oil Production Company".

With regard to the A.B. Cryptograph Dr. Nobel consulted his colleague and close friend Karl Wilhelm Hagelin, my father, and they came to the conclusion that the possession of good cipher machines for written communications could play a decisive role in often difficult business affairs. Based on that conclusion Nobel himself decided to invest new funds in the A.B. Cryptograph, and my father also took a small part in the company. He was technically interested as he was an engineer himself.

Since the director of the A.B. Cryptograph, Arvid Gerhard Damm, had a rather obstinate personality, Nobel and K.W. Hagelin needed a trustworthy person to monitor his activities. Because I was then living in Stockholm where I had opened my small engineering office, Mr. Nobel asked me to watch over A.B. Cryptograph.

When I joined the company, Damm's interests in cipher machines were concentrated in the field of radio telegraphy. When I first appeared at the company offices a complete layout was on display: a typewriter for the input of text, a cipher machine, and a typewriter equipped with electromagnets for the output of enciphered or deciphered text. Damm had succeeded in arousing the interest of the major radio telegraph companies in his machine and prototypes were to be built by one of these companies in Paris. After I joined the firm Damm moved to Paris, and I had to look after the business side of the firm and its technical development more than I had originally expected.

In the end Damm succeeded in winning the "big four" to his project: Marconi, Telefunken, TSF and Western Union. They financed the construction of four prototypes. But these did not appear to be reliable enough and were too slow, so the project failed.

In the meantime, however, Damm had developed a system with so-called simplified rotors, and some prototypes of these were built for wireless traffic. The machines consisted of three units: The keyboard, the ciphering portion with motor drive, and the output unit -- either an electromechanical tape punch (a Creed Morse code punch), which was equipped with a magnetic control or an electric typewriter.
Fig. 8 shows under (a) the ciphering unit, under (b) the tape punching machine, the keyboard and the ciphering unit, and under (c) an electric typewriter, keyboard and ciphering unit. This machine was Damm's Electro-crypto B-18.

The principle of the simplified rotor later became the salvation of the faltering business. But this came only after Damm's death in 1927.

In 1925 I was able to make my first positive contribution to the A.B. Cryptograph, and this proved to be of decisive importance for the future of the company. I happened to hear that the Swedish General Staff had received an "ENIGMA" machine for study and I rushed to visit the officer concerned with this matter. I explained to him that the A.B. Cryptograph already had ten years of experience in the field of cipher machines and that I would be able to offer something possibly superior to the "ENIGMA".
The General Staff wanted our machine to be the same size as the ENIGMA and to operate in the same way. Time was short and I had only six months to produce the new machine. At the time we had only Damm's earlier constructions on hand, and they did not fill our needs. Nevertheless I promised to deliver. In those days I had no experience whatoever about cryptography but I had a certain talent for tinkering: I believed I would be able to build a comparatively compact machine on the basis of Damm's "simplified rotors". This design made use of a 5 x 5 grid, whose principle is shown in a simplified diagram in Fig. 9.

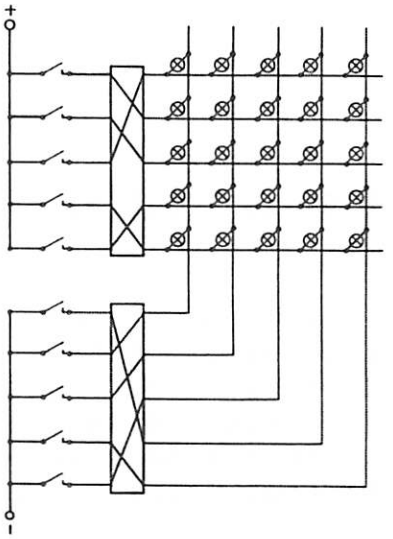


FIG. 9 5 x 5 MATRIX

To build the first model of the machine Emanuel Nobel allowed me the sum of 500 kronor, about $ 134.-- (!) I succeeded in producing a prototype within the size limitations and in the time authorized, a somewhat primitive model but still adequate for the evaluation. This machine had a keyboard, 2 rotors whose stepping was controlled by two separate pairs of pin-wheels (keying-wheels) with different divisions on their periphery, and with a display of 25 electric lamps which served to indicate the output letters for encipherment or decipherment (Fig. 10). This prototype was analyzed by a mathematician, and approved instead of the ENIGMA for use by the General Staff.

FIG. 10 B.C.W. HAGELIN'S B-21 (PROTOTYPE)

Because Damm used a 5 x 5 grid, it was necessary to eliminate one letter of low frequency or to use the same signal for two letters, e.g. for i and j.
The keyboard was connected with two groups of 5 contacts each. By operating a key, one contact was closed in each of the two groups, forming one of the 25 possible combinations. After the closing of two circuits through the two rotors, and a further circuit through a relay system, one of the 25 electric lamps lighted up and indicated the resulting letter. The relay system was necessary because at that time there were as yet no devices like modern diodes, which would have simplified the construction considerably. In order to be able to vary the enciphered alphabets, so-called modificators were added in series with the rotors, i.e., interchangeable leads which could be plugged in as desired. This provided 5! = 120 combinations for each group and for both groups together yielded 14,400 possibilities. It should be noted that after the Second World War I developed a new modificator system which could generate all 25! - 1.55 x 10^{25} possibilities, but at that time this machine had been superseded by my C-Type machine.

The designation "pin-wheel" mentioned above needs to be explained since the pin-wheel came to be used later in many other machines. It is a disk which carries on its periphery a number of axial holes or slots in which pins are located. These pins are movable and are so arranged that they can protrude on one side or the other of the pin wheel. One side of the wheel is the "active" side, i.e., pins which protrude on this side exert a controlling effect. The pin-wheels are stepped with each operation, each wheel moving one pin position during each operation. The cyclic length of the wheels have no common factors. Thus as several wheels work together, a very long period for the key is obtained.

The prototype had four pin-wheels, with cyclic length of 17, 19, 21, and 23, which yielded a combined keying cyclic length of about 1.5×10^5, or 1'500'000 operations.

By using different combinations of pin settings theoretically $2^{17} \times 2^{19} \times 2^{21} \times 2^{23} = 2^{80}$ or approximately 10^{24} different period characteristics could be obtained. This meant that an enormously large number of variations was possible.
The prototype of the machine (Fig. 10), which was given the name B-21, is still in the possession of the CRYPTO AG.

FIG. 11 B-21 WITH SOLENOID MAGNETS (SERIES)

Fig. 11 shows the final model, in appearance quite similar to the "ENIGMA". It used a power supply of 110 or 220 volts for a solenoid magnet which operated the stepping of the rotors. For the lamp display a flashlight battery was utilized.

For the convenient use of this machine in central offices with extensive operations, it was connected to a Remington electric typewriter instead of the lamp display (Fig. 12). Typewriter keys were activated by small electromagnets and the lamp display was shut off.

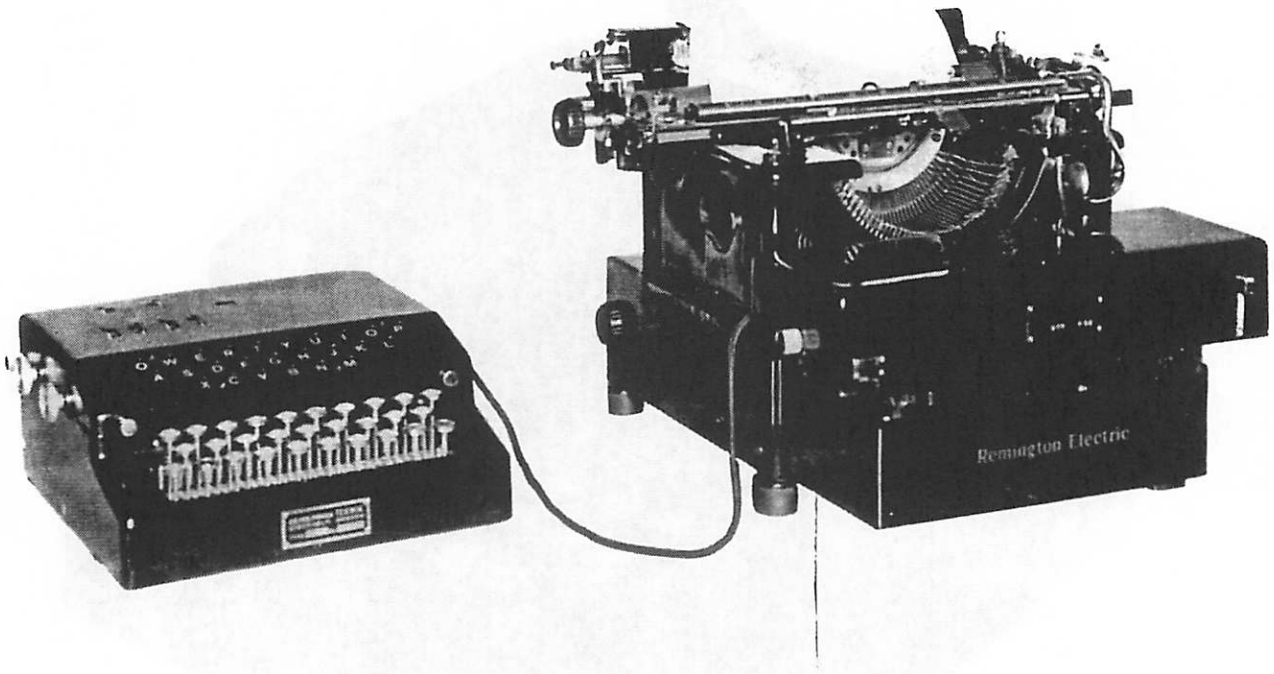


FIG. 12 B-21 WITH ELECTRIC TYPEWRITER

III. The B-211 Machine

After Emanuel Nobel died in 1932 his heirs did not want to make any more funds available for A.B. Cryptograph. I myself had been working without pay because the firm's income had been very meager. In spite of the limited possibilities I was able to make several trips to other countries where I found buyers for the B-21. The decisive success, however, came from the interest of the French Army in our machine. Before the machines could be sold two requirements had to be fulfilled: the machine had to be able to print the text and should also be portable. This called for the implementation of an electromechanical drive. I succeeded in solving this problem in a short time by replacing the lamp display with a special type wheel printing mechanism, (Fig. 13), which I had designed.

Fig. 13 B.C.W. Hagelin's B-211

Since the machine, which we called the B-211, was to be built in France, we got as manufacturer the French subsidiary of the Telefon - AB L.M. Ericsson located in Colombes just northwest of Paris.

The B-211 was provided with shift keys like those on a typewriter. During encipherment only letters were printed, but during decipherment letters, numbers and symbols were printed. The machine also had a crank so it could be operated by hand in case the electric power failed. For the ciphering circuits a flashlight battery was used, as in the B-21 machine.

Before the outbreak of World War II about 500 B-211 machines were built and delivered. It was through the financial support of my father, who lived in Paris at the time, that this business could be carried through. It would not have been possible without his encouragement and funds, and it was not easy for him.

When the war broke out, my father at the last moment succeeded in transferring the profits from France to Sweden. The amount was large enough to pay for his expenses and install and equip a modern workshop. It was our first workshop since the founding of the A.B. Cryptograph in 1915. The shop was dedicated at New Year's eve of 1940 by the heirs of the A.B. Cryptograph and was renamed the "A.B. Ingeniörsfirman Cryptoteknik".

It may be mentioned that the French army after the War bought an additional 100 B-211 machines.

I also might mention that I was obliged before the War to sell "two cipher machines" to the Russian Trade Commission in Stockholm (according to the purchase order). I sold them two B-211 machines which we had in stock in Stockholm.

The machines were copied in Russia and used during World War II. They were provided with a 5 x 6 grid. The Cyrillic alphabet had more than 30 letters but a few of them occurred very seldom, and could be omitted. Also the modificators were plugged in outside of the machine, probably under locked cover so that the operator would not know which inner settings were in use at any given time (Fig. 14).

FIG. 14 COPIED B-211 FOR CYRILLIC ALPHABET

IV. The C-Machines

Quite soon after the beginning of our business relationship with the French "Deuxième Bureau" I was asked in 1934 if I could develop a compact "pocket" cipher machine that printed. As good luck would have it, I had already a few years before received from two Swedes an order to design a coin changing machine. After I had built a functioning prototype, I got the idea that it should be possible to insert any amount in coins, to enter the invoice amount by a key, and finally to get back the change. This machine was equipped with a unique calculating mechanism but it was never built because we had not been reimbursed for our development effort. We agreed to cancel the debt and retained the rights for our designs.

Trying to find a solution for the "pocket device" for the French, I got the idea to incorporate the calculating mechanism for the money changer into such a device. The "revolutionary invention" (in the opinion of distinguished cryptologists) consisted in a pure association of ideas that were transferred from one to another completely different field of application.

The calculating mechanism of the money changer consisted of a drum with displaceable axial bars around its circumference which could be affected by operating the keys. Those bars which were affected in an operation were displaced to the left as the drum turned. A type wheel meshing with the drum was turned exactly the same number of steps as the number of bars moved to the left. I replaced the keys of the money changer with pin-wheels, and the type wheel carried letters now instead of numbers. In this way I obtained a cipher machine. In order to estimate the dimensions desired, I cut out a wooden block to fit snugly into the pocket of a jacket. For the first models I used a drum with 25 bars and five pin-wheels of the same construction as those in the B-21. These wheels were provided with pins around their circumferences, which could be placed axially in two different positions, either "active" or "inactive". "Active" pins worked upon the drum by means of a control arm.

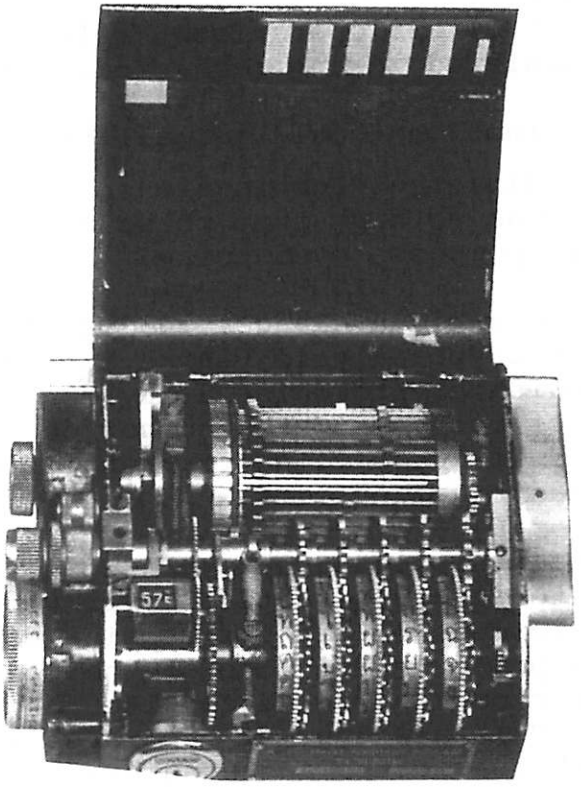


FIG. 15 B.C.W. HAGELIN'S C-35

The bars of the drum are provided with cams, i.e., raised areas on their edges, of such a design that the first bar would be moved by the control arm of the first pin-wheel, the next two bars by the second wheel, the next four by the third, the next eight by the fourth, and the remaining ten bars finally by the fifth wheel (Fig. 15).

Depending on the number and the arrangement of active pins in the pinwheel in question the control levers will be pushed against the periphery of the drum, or remain in their inactive positions. When the drum is revolved during an operation the active levers push the corresponding bars (from 0 up to 25 bars) to the left and so engage the gearwheel connected to the typewheel. The typewheel is therefore displaced a number of steps equal to the number of the active bars. The drum thus acts like a gearwheel with a variable number of teeth. As the number of pin divisions on the pinwheels has not any common denominator, the length of the key period, i.e., the number of operations which are needed before the pinwheels return to their common starting position, is very long.

For the first machines the divisions, or cyclic wheel lengths selected were 17, 19, 21, 23 and 25, which resulted in a period length of 3'900'225 operations, a length which until then had not been achieved in any mechanical ciphering machine.

Moreover, since one could set all the pins theoretically in about 10^{29} different combinations, the number of possible variations was so high that these machines are fully adequate for certain purposes even today.

Later I made various changes in direct response to the steady progress in cryptanalysis, which included the significant work of the Swedish cryptologist Y. Gylden. The main improvement consisted of increasing the number of pin wheels from five to six, and to introducing rearrangeable lugs on the drum-bars instead of fixed cams.

When the machine began to be produced in larger quantities, a bottom plate and a protective cover were added. The bottom plate was formed so that the machine could be used in the field strapped over the knee of the operator. If necessary the operator could even march with the machine strapped to his thigh. This new type of apparatus was given the designation C with one letter and a numeral suffix which originally designated the model year but after 1952 defined the specific model of the machine: e.g., CX-52.

The opportunity to establish a modern workshop with the royalties from our French sales occurred just before the outbreak of World War II. It thus became possible for us to make and sell a considerable number of machines during that War. Our first large customer were the Swedish defence forces with whom I had maintained connections since 1925. From France we received an order for over 5000 machines, which were to be manufactured by Ericsson at Colombes, but this order could not be completed.

To promote the C Machine I made several trips, first within Europe, but in 1937 I went again to the USA where the wish was expressed to have an electrically powered machine with a keyboard. In the summer of 1939 I took a prototype of the so-called BC Machine to Washington. Unfortunately the construction needed improvement and I returned to Sweden the same autumn after the outbreak of War with matters still unsettled.

I made another trip to the USA at the beginning of March 1940 on my own initiative without any request from Washington. I was able to leave on the last ship from Europe at Genoa on May 10, 1940 with two machines in my luggage before the Italians entered World War II. This trip was to lead to the largest sale of C Machines ever made.

The American business began with an initial order for 50 machines which were shipped airfreight from Sweden to Washington. After extensive testing the machine was accepted. The Americans selected it for tactical use, as they did not have any comparable machine at that time. The C Machine, designated in America as the M-209, was manufactured by the Corona plant of the L.C. Smith typewriter company, with a daily output of up to 500 units.

I remained in America during the war and had a small shop in my home for servicing BC Machines which were used by an American organization during the war.

When it became possible for me to return to Sweden in 1944, more than 50'000 machines had been built. By the end of the war over 140'000 units were made in America.

During my four year stay in the States the workshop in Stockholm was kept busy with orders from several foreign countries. One delivery went by an extraordinary way to Japan. The machines were smuggled out by the Japanese military attache in a night boat passage and picked up by a U-Boat off the coast of Sweden. But very few machines reached their intended destination in Japan.

It seems worth mentioning that the German authorities, who years before the war showed no interest in the demonstrated C Machine, began, toward the end of the war, in the Wanderer works at Chemnitz to manufacture a copy of the BC Machine for their own use because the "ENIGMA" machine had been broken by the British (Fig. 18).

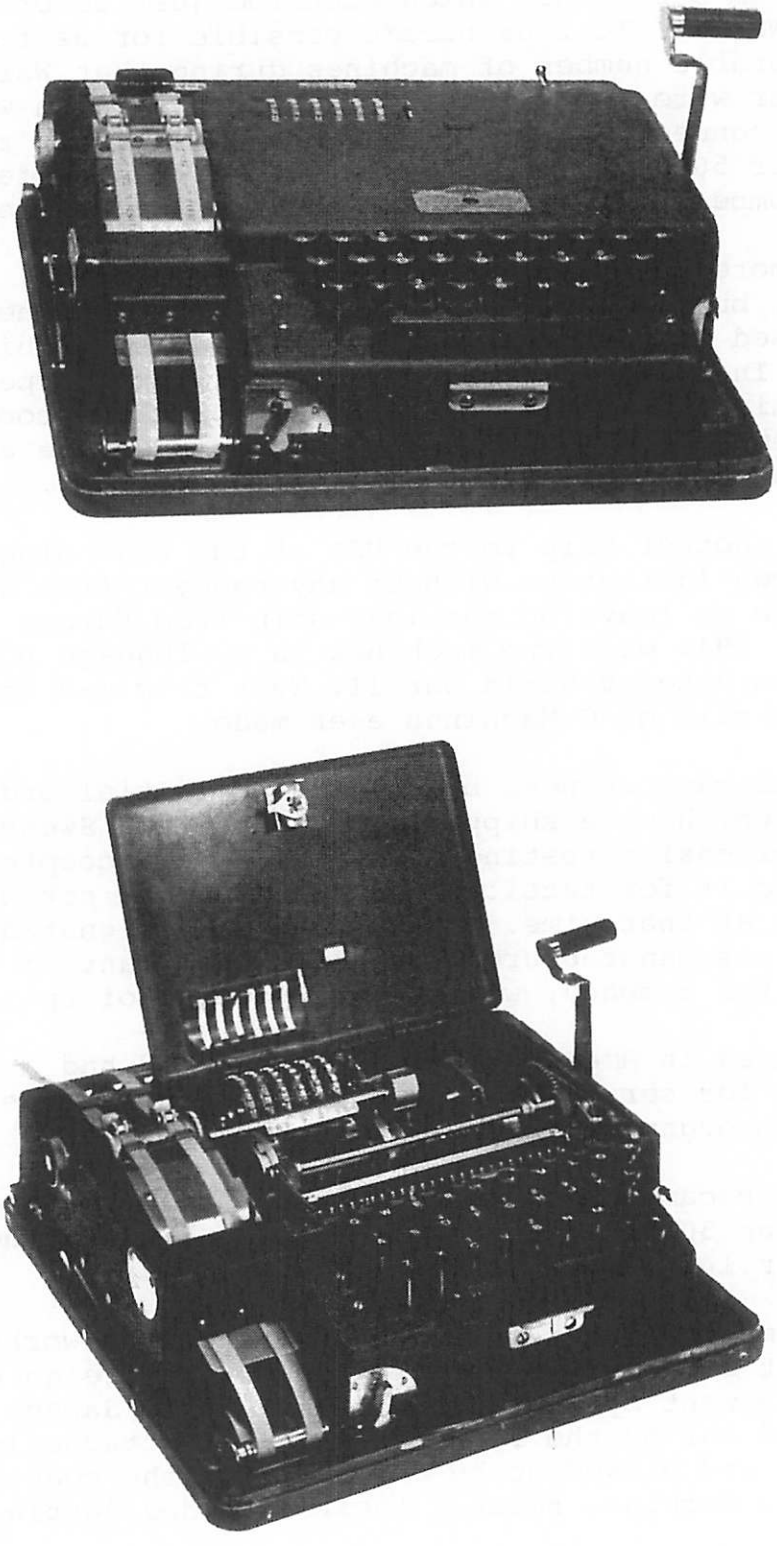


FIG. 16 B.C.W. HAGELIN'S BC-543

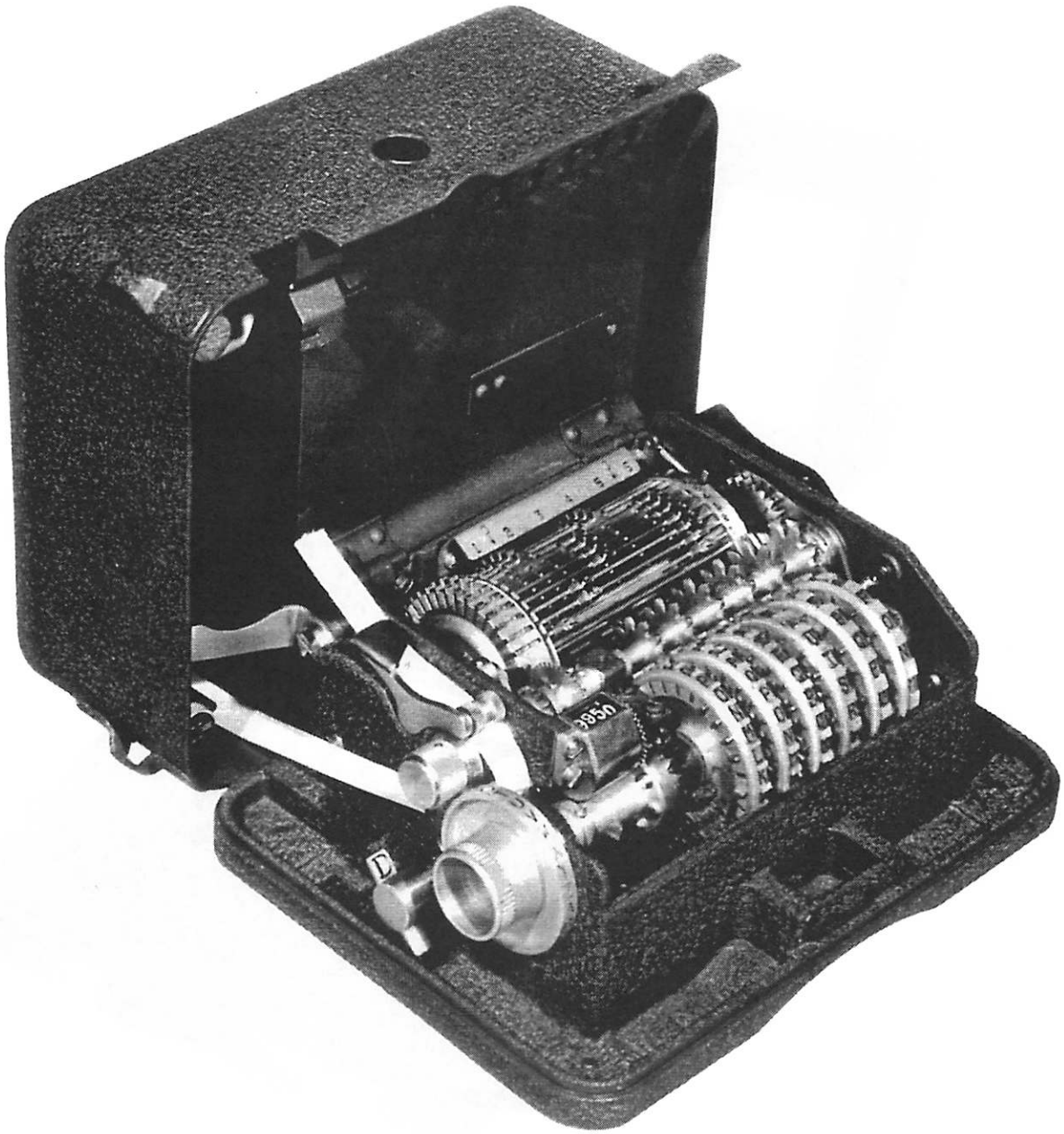


FIG. 17 USA-VERSION OF THE C-36: M-209

FIG. 18 C-41 (GERMAN COPY OF THE BC-543)

When the third Reich collapsed they had only been able to manufacture about 700 machines. It is even more interesting to note that in the 1950's postwar variation of the C Machine was built in Germany under licence. About 10'000 machines are said to have been produced. France also obtained the manufacturing rights for the C Machine for the francophone community.

It should be stressed that the C Machine was planned for tactical purposes, i.e., for use at the front. When, because of its simplicity and portability, the machine also proved to be interesting for use in the diplomatic service, improvements were needed to attain a higher degree of security.

I first got the idea of modifying the machine so that the rotation of the pin-wheels would be irregularly. Other improvements were introduced as well. The new type brought no large changes in the basic structure of the original C Machine. This new machine was first given the designation CX-52 but later, after different pin-wheel movement variations were made, new model numbers were used (Fig. 19).

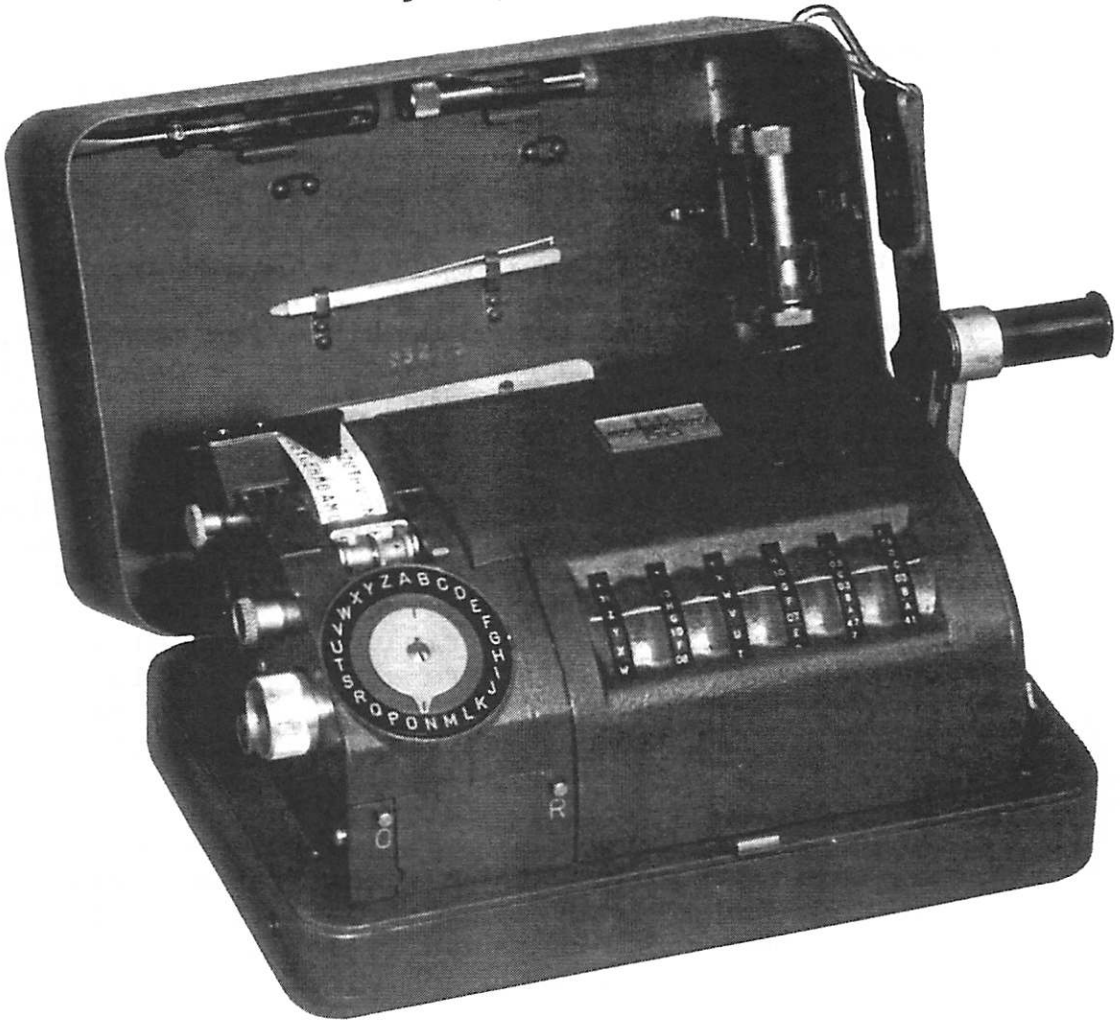


FIG. 19 THE C(X)-52

Before going into the details of the various improvements, it is important to emphasize that the requirements of our customers led in two opposite directions. One group required very long key periods, while the other wanted a movement of the pin-wheels that was as irregular as possible. It required great mathematical competence to compile keys which would assure that sufficiently long periods were obtained. In order to satisfy our customer we also developed hybrid systems where usually one pin-wheel was stepped regularly and the others irregularly.

The further development of the C Machine, which even today, in the age of electronics, is being used, can now be followed in some detail:

a) The number of pin-wheels was increased quite early to six. Instead of the original five wheels with divisions of 17, 19, 21, 23 and 25, 12 pin-wheels became available with divisions of 25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46 and 47, of which six were to be used at one time, preferably those with no common factors. The wheels were inserted easily without using a tool.

b) The number of slide-bars was increased to 32. In place of the fixed cams on the bars which caused the type-wheel to turn, movable lugs were installed on each bar so that the movement arrangement for the type wheel could be changed as desired. For other ways of using the machine, some bars with fixed cams which control irregular forward movement of the key wheels were manufactured.

c) Even in the very first C Machines reciprocal alphabets were utilized. With a letter sequence on the type-wheel running in the opposite direction to that on the indicating disk, the same machines could be used both for enciphering and deciphering without any modifications. In later models a second type-wheel was introduced, which was permanently connected to the indicating disk, and which printed the same letters which were set with the indicating disk. They were called "primary" and secondary" type-wheels, where the primary type-wheel is connected to the indicating disk. There are also available indicating disks and type-wheels, where the letters can be rearranged at will, and without removing them from the assembly.

   One model printed the plaintext in the characters of a non-European language (e.g. Arabic) and the ciphertext in Latin letters, and one text (Arabic) read from right to left and the other text from left to right. This arrangement was indispensable for Arab countries using the international telegraph service.

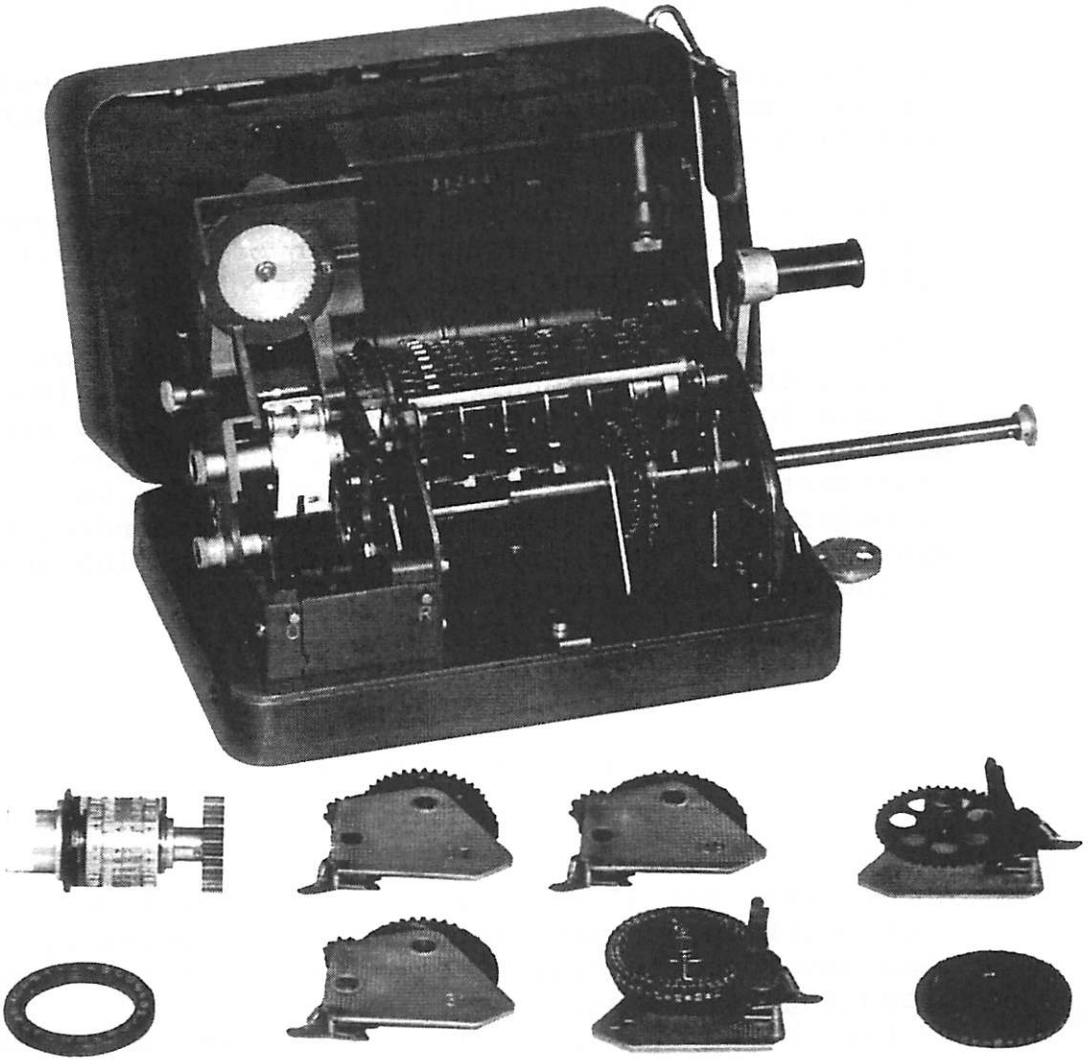


FIG. 20 CX-52 (DISASSEMBLED)

d) Between the indicating disk with the primary type-wheel and the secondary type wheel was a disconnectable clutch It could either retain the chosen relative positions between the primary and secondary type-wheels during a series of messages or change each time at the start of the next letter in the text.

e) For the easy setting of the pins on the pin-wheels a special tool was provided. This tool set in a single operation all the pins in one wheel.

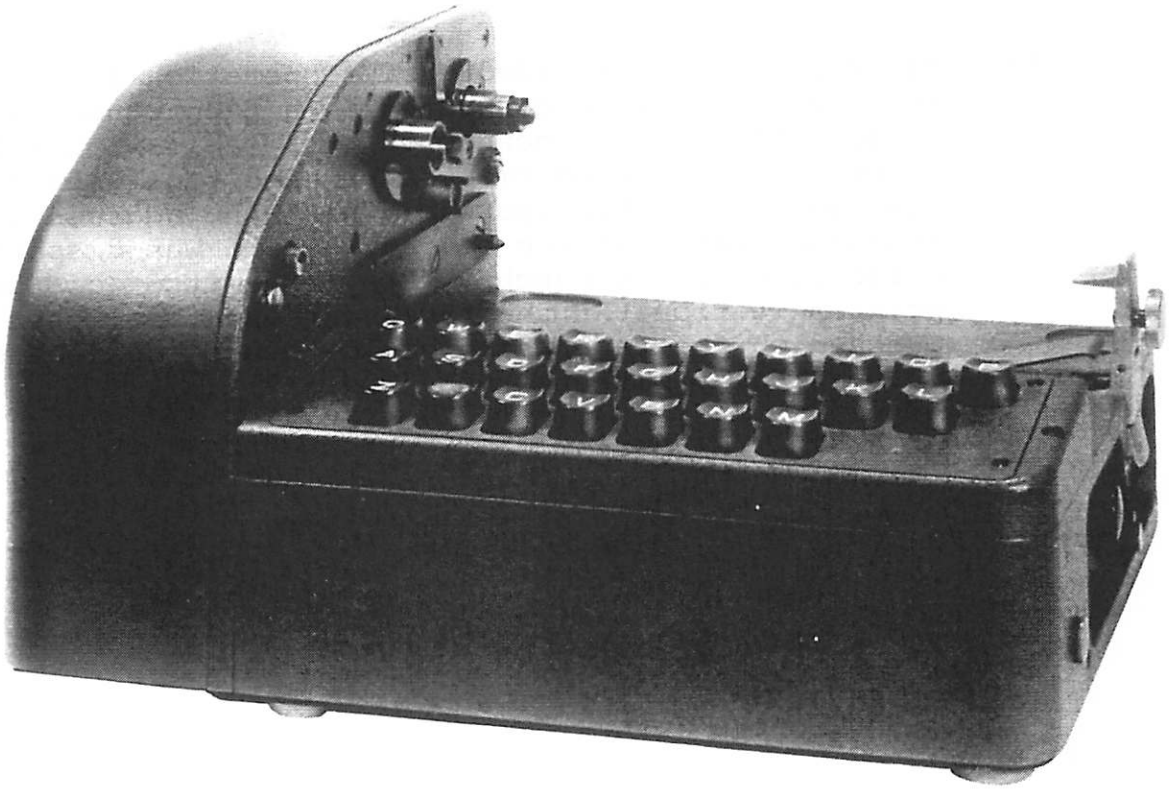
f) A special device which was developed at the request of one customer was the mechanization of the "one-time pad" system which had been a slow hand procedure.

Near the end of World War I the American Vernam made the first attempt to mechanize this system for telegraph use. He used for the key-tapes punched paper tapes with random sequences of teleprinter signals. The characters of the plaintext in the standard CCITT No. 2 code were combined by means of relays with the key-tapes according to the system of the "exclusive-or" associating plus and minus in the following way:

+ and + results in +,
+ and - results in -,
- and + results in -,
- and - results in +.

After World War II we learned that special devices had been built to generate such tapes. Consequently our firm also developed special electronic random generators for producing key-tapes.
In Part VI below, as a curiosity, I have described two of my designs for the automatic production of "one-time pads".

g) While the pre-war C Machine was supplemented with the keyboard BC-machine, for the modern C Machine we developed a separate attachment, named B-52 ... B-62, which was provided with keyboard and electrical operation. In smaller message centers the C Machine alone was sufficient, while in large ones the C Machine was mounted on this device (Fig. 21).



a

b

FIG. 21 A: B-62 B: BC-62

h) The PEB Machine provided easier operation for telegraphic traffic. The device consisted of a tape punch and a tape reader and could be connected by a cable with a BC Machine. During encipherment a punched tape with ciphertext was made on the PEB (possibly with the address in plain language placed at the beginning) and was dispatched directly over the punched tape transmitter of the teleprinter station. At the receiving end the cipher was punched on the tape which could then be deciphered automatically with the PEB (Fig. 22).

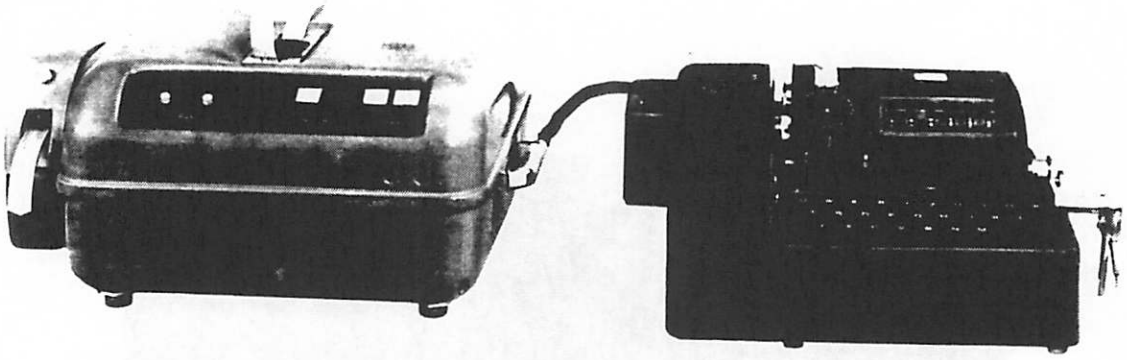


FIG. 22 LEFT: PEB-61 RIGHT: BC-621

The various improvements caused the C Machine to outgrow its pocket-size format. Now I wished to build a "pocket machine" in the true sense of the word. I was able to introduce a model which, because of its small size, could not print but nonetheless allowed an easy read-off of the text letter by letter. The cipher mechanism was quite different from that in the C Machine but the device was fully compatible with a contemporary variation of the C Machine, which worked with regular stepping of the pin-wheels.

The French gendarmerie urged us to build this pocket machine and assured us of an order of at least 4000 units. Although this quantity was not actually reached, lots of these machines were sold, which came on the market under the designation CD-55 and CD-57 (Fig. 23). About 12'000 have been delivered.

The input and output elements of the device consist of a ring inscribed with an alphabet and rotatable disk inside the ring. A levergrip pressed by the left thumb causes the displacement of the alphabet disk in each operation. With the right hand the resulting text can be copied letter by letter. If the letters are not in sequence the encipherment must be done from the ring to the disk and the decipherment from the disk to the ring. For convenience users normally use reciprocal alphabets and then can go from the fixed ring to the movable disk for the output. Even these machines can be equipped with a keytape reader.

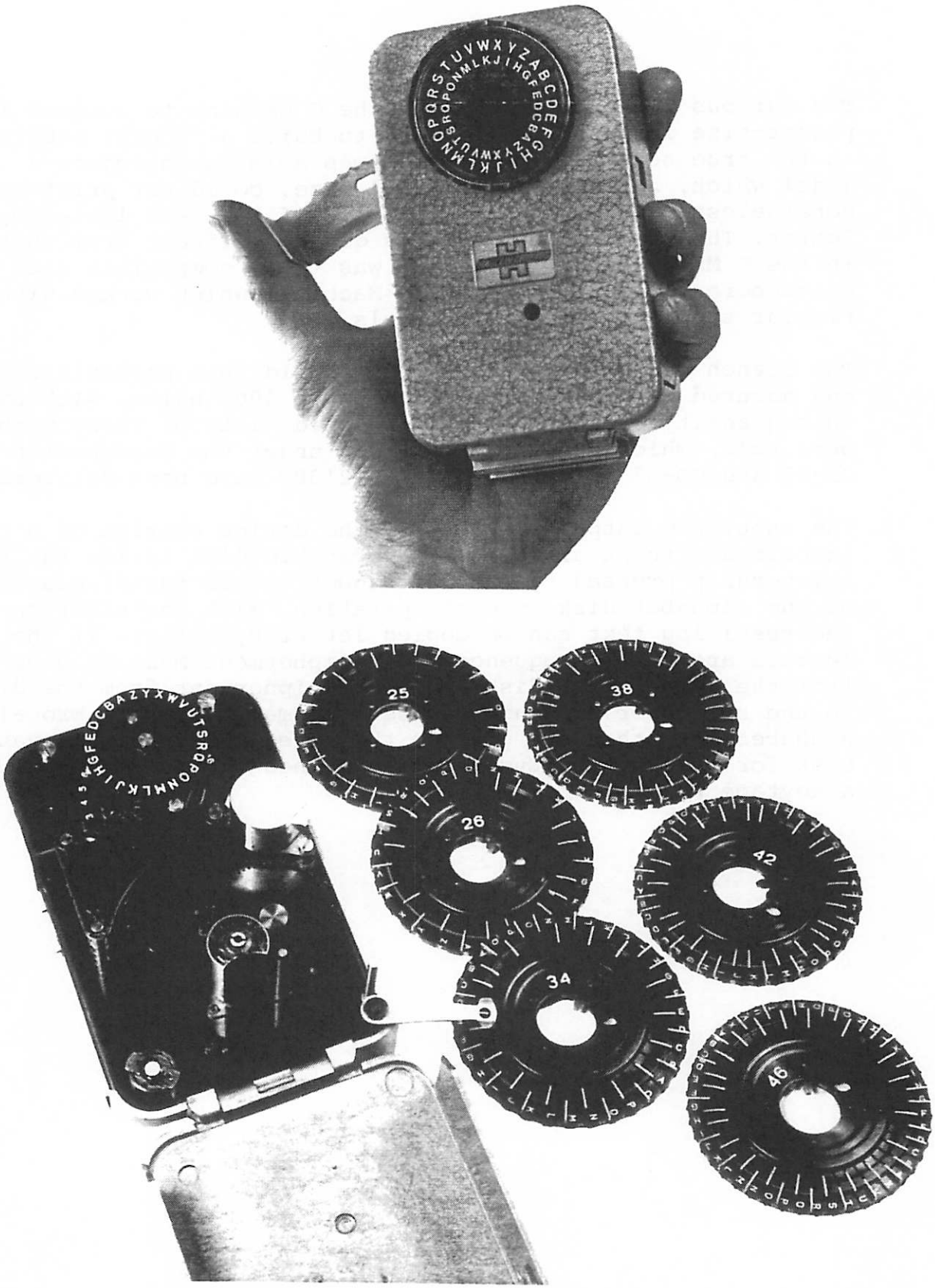


FIG. 23 CD-57, CLOSED AND DISASSEMBLED

V. The Telecrypto Machines

In 1948, as mentioned in the Introduction, I settled in Switzerland where I worked for a short time with the Swiss inventor Dr. Edgar Gretener on the development of machine for automatic enciphering and deciphering of teleprinter messages. These "on-line machines" were connected between the ETK teleprinter, designed by Dr. Gretener, and the line. Our cooperation did not last very long and I decided to build my own machine for use with all standard teleprinters. Dr. Gretener's machine is no longer in production. My preliminary work on a comparable machine was done in my workshop in Stockholm, but the manufacture took place at CRYPTO AG in Zug where some improvements were added to the original design.

Two types were built under my direction: Type T-52 and Type T-55. Both were installed between the teleprinter and the line, so that the teleprinter personnel worked only with plaintext while over the line only ciphertext was transmitted. Both types used for their "key-generator" the C Machine drum and six pin-wheels. The T-55 model was also equipped with two tape readers, one for the text tape and the other for a random key-tape. It was possible to work either with the key-generator or with the random key-tape.

The T-52 machine (Fig. 24) was produced in series in Zug in 1953 - 1954. It worked with six fixed pin-wheels and a drum with 2 x 12 slide-bars, using the principle of the C-36 Machine.

The T-55 was designed in 1955 - 1956. It used six interchangeable pin-wheels and a drum with 22 slide-bars like the system in the C-52 series. The keying sequence was generated in both types mechanically, the information processing electrically by relays.

In the T-52 each telegraph signal resulted from a function-step in which each telegraph signal was processed directly and passed forward. The keying signals produced were passed into the five keying signal relays, combined with the incoming telegraph signals according to the "exclusive-or" rule, and sent out. The T-52 could be set by hand to "Send", "Receive", or "Punched Tape Operation".

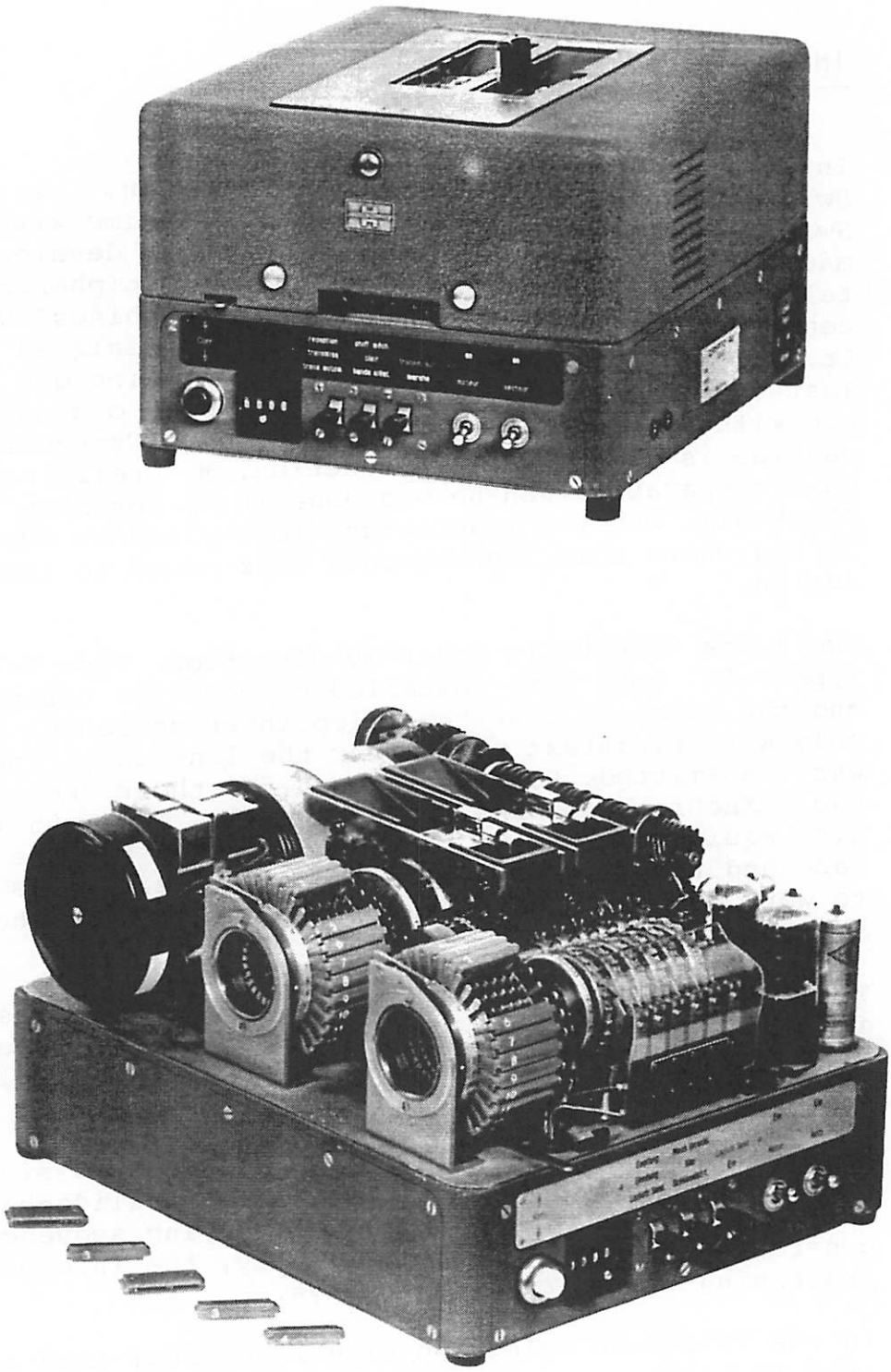


FIG. 24 TELECRYPTO T-52 WITH AND WITHOUT HOOD

In contrast to the T-52, in the T-55 (Fig. 25) the keying signals were not stored but were produced continuously as five keying signal elements during one cycle of the machine and combined according to the "exclusive-or" rule with each binary element of the telegraph signal. Therefore the slide-bar drum had to run synchronously with the teleprinter signal, and consequently the five keying information elements always coincide with the text elements.

In addition the T-55 was equipped with a tape reader by means of which a superencipherment, i.e., mechanical keying generator plus random key-tape was obtained. As an important improvement over the T-52 Machine the T-55 offered automatic direction reversing.

Another important feature of the T-55 was the remote lock for the answer-back unit of the teleprinter. When the T-55 was not in use it remained on "plain language operation". Should this machine be called, then after operation the WRY-Key at the transmitting teleprinter a "Call" button at the T-55 was pushed which locked the sending loop of the remote station. By this action the incoming transmission could not be jammed by an answer-back sent during the transmission.

Later the tape could be deciphered in a local loop. The answer-back lock was released automatically when the lines were disconnected, and the station was then ready to operate in both ways again.

To produce the key-tapes for these machines we constructed a three-part apparatus: an electronic random number generator, a punch, and a labeling machine. The punch, of American design, could do up to 120 characters per second. It produced two identical tapes at the same time, which were printed upon at regular intervals with consecutive identification numbers according to customers' specifications.

The use of random key-tapes became very popular. But after some years the use of this system declined because of the problems of supplying and distributing key tapes. Key tape machines were then replaced by electronic telecrypto machines.

Both machines were single-shaft regenerators in terms of telegraphic technique. They delivered error-free telegraphic impulses, which left no possibilities whatever for electronic cryptanalysis by means of pulse analysis.

a

b

FIG. 25 T-55, A: OFFICE VERSION, B: FIELD VERSION

VI. Miscellaneous Machines

Some machines are described which were built only as prototypes or in small numbers.

1. An Autokey Machine of the C-Type

Customers have always looked for cipher systems which are not only secure but also simple to operate. As an example of such a system the autokey cipher will be described. The correspondents utilizing this system used a list of code words to indicate the starting point in the keying sequence. It soon appeared that this system was not absolutely secure since "Probable Words" could help to analyze the ciphertext, i.e., to make decryption trials in order to discover where such words or sentences are located in the secret message. This system was thus discarded.

But the idea to integrate the text into the keying sequence was very attractive to me, and in 1948 I designed a machine which was built only as a prototype. The basic principle of this machine was to combine the text to be enciphered with a classical cipher system in such a way that the text component of the keying sequence would not be vulnerable to analysis. The keying sequence of a classical machine was thus changed into a pseudo-random keying sequence. I use the expression pseudo-random since the sequence of letters in plain language can not be considered completely randomly distributed. However, from a practical viewpoint the combination of a continuous keying sequence combined with this text to be enciphered could in practice be called randomly distributed.

For the classical cipher machine I used a normal pre-war C Machine with five pin-wheels and a drum with 25 slide-bars. This machine was modified so that in place of the toothed wheel drive, a drive using a latch drive for the regular movement of the pin-wheels was used. A drum equipped with 26 slide-bars was placed in front of the latches (Fig. 26).

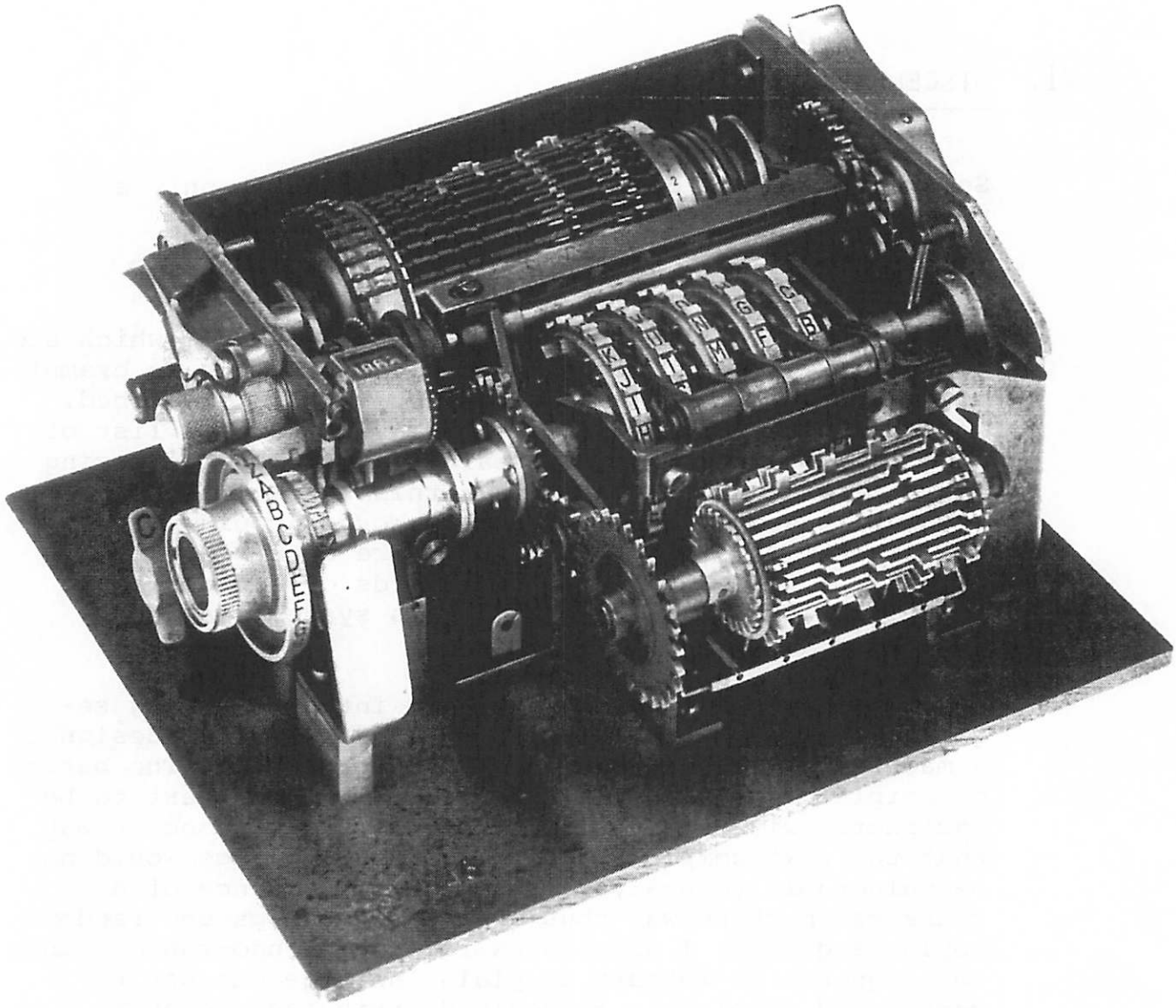


FIG. 26 C-36 WITH AUTOKEY (PROTOTYPE)

This auxiliary drum was connected via gears to the indicating disk, so that for each change of the indicating disk a corresponding auxiliary slide-bar came into active position before the latches. The auxiliary slide-bars were provided with fixed lifters. As an example the latches for pin-wheels 1 and 3 of one slide-bar could correspond to the letter A of the setting disk and could be found in the input position. They could then be brought into an active latch position by a movement of the drum, so that in the succeeding operation the pin-wheels 1 and 3 would be moved one step forward. These slide-bars were interchangeable, so they could be set into 26! different sequences in their drum.

The machine functioned as follows:

Before starting an encipherment the pin-wheels were set into their specified positions. Then the letter to be enciphered was brought by a turn of the indicating disk into its input position. The slide-bar on the auxiliary drum corresponding to the letter was advanced to the active position. Then the rotation of the main drum followed, which turned the setting of the indicating disk/type wheel unit the same number of steps determined by the pin arrangement on the pin-wheels and the distribution on the main drum. The resulting cipher letter was printed and the auxiliary drum directed against the latches in order to advance those pin-wheels affected by the active latches one step forward at the end of the operation.

In decipherment the active time for the movement of the latches was shifted to the beginning phase of the operation. After setting the cipher letter into the input position the turning movement was performed first, then the readjustment of the type wheel unit, and finally the printing of the deciphered plaintext letter.

However, I reluctantly discarded this device because transmission errors and garbles causing the keying to get out of step could lead to considerable delay in recovering the message. Today this objection is no longer valid since transmission technique, either by wire, radio, or even via satellite, has been improved immensely.

I regret that this simple and good machine came too early, and today has been outdated by its electronic successors.

2. The Ciphering Teleprinter

In 1953 an experimental ciphering teleprinter, Type TMX, was built.

It had four input possibilities: keyboard, text tape, key-tape, and incoming signals, and three outputs:
print-out, tape-punch and outgoing signals (Fig. 27).
I soon realized, however, that CRYPTO AG possessed neither the financial nor the technical means to compete with such a machine against the major teleprinter firms. We still have the prototype, but we dropped this large project and undertook something more suitable to our capabilities: the manufacture of a telecrypto machine which could be connected to normal teleprinters.

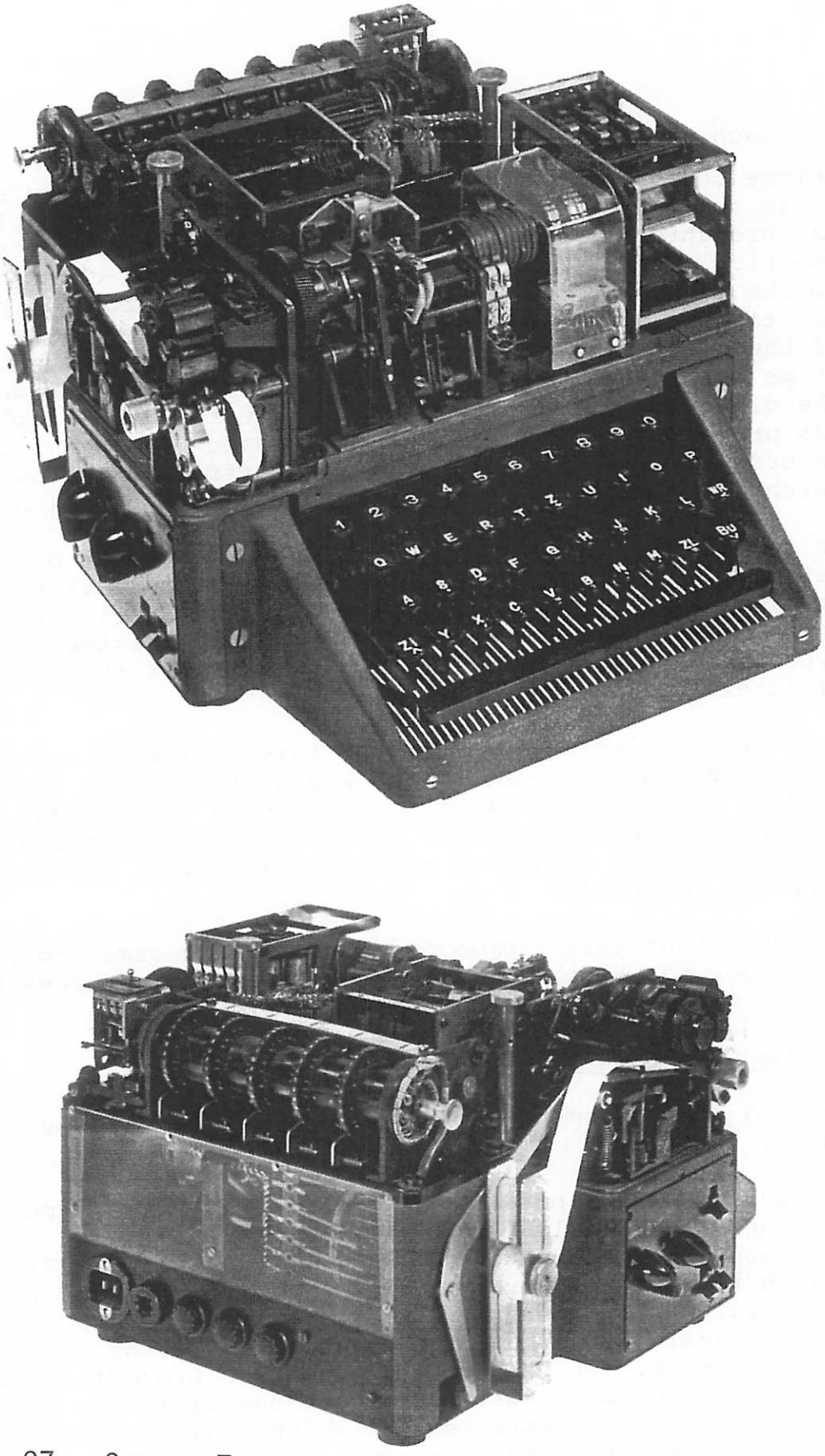


FIG. 27 CIPHER TELETYPE TMX-53 (PROTOTYPE)

3. "One-Time Pad" Machines

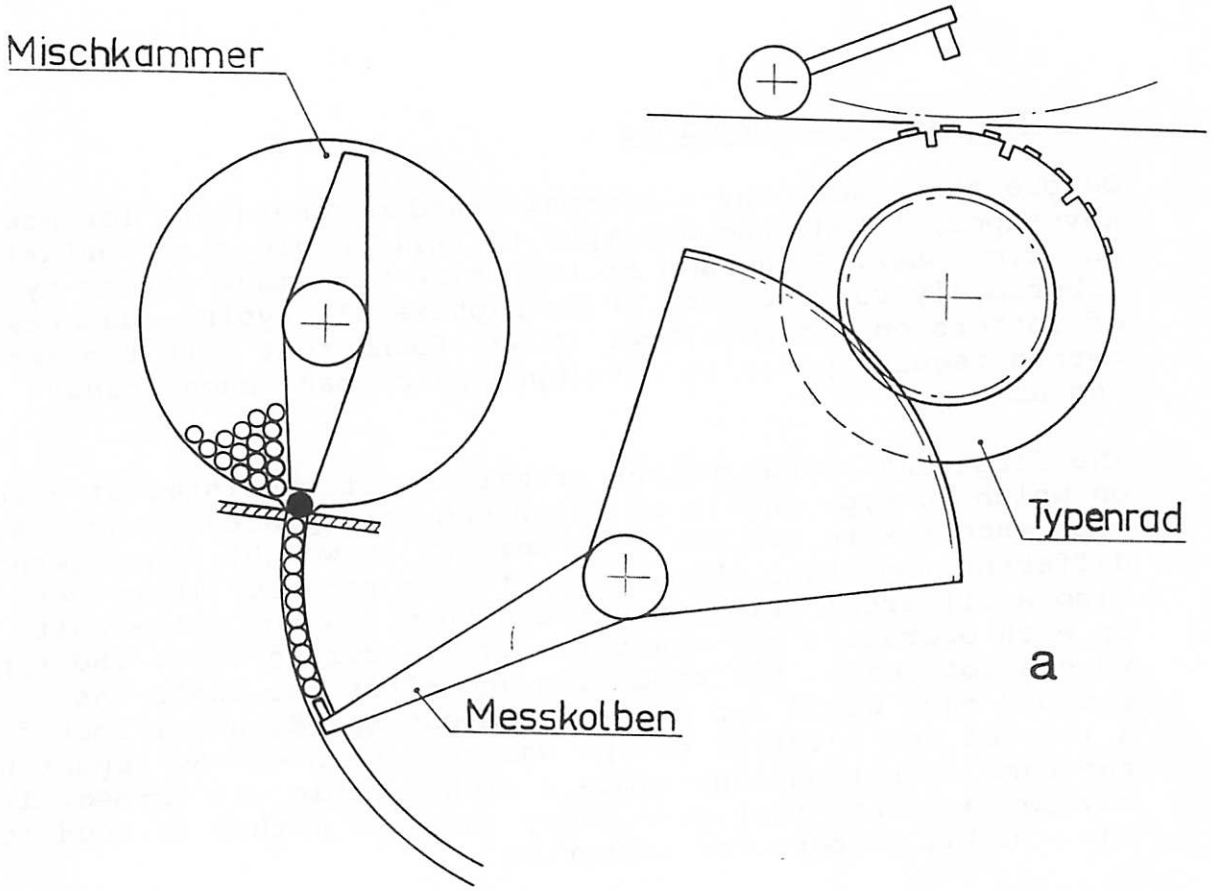
Before there were any electronic random generators for making key-tapes, I made two attempts to build devices for printing one time pads. Such pads at that time were made either by laboriously rolling dice or by haphazardly typing sequences of letters on a typewriter. It was found that with the latter method regular patterns developed which made such "pads" unusable.

The first device was rather primitive. It consisted of a shaft on which 50 type wheels in 10 groups were placed. Since these type wheels were not strictly uniform in weight, they gathered different momentums when the shaft was rotated. There was also a different friction between them and the axle-shaft. In each operation the shaft received a strong turn. The type wheels rotated at the same time and after the shaft was stopped they would run on at different speeds until locked. A line of ten 5-letter groups was then printed. By repeating the same operation many times a cipher table was formed. It may be mentioned that even today the same method is used for the winning numbers for lotteries.

The second design was even more unique. 8 x 5 type wheels were used with each wheel coordinated to a mixing chamber which held 26 steel balls of which one ball was somewhat larger than the other 25 balls (Fig. 28a).
For each operation the balls were mixed and run into a tube until the thick ball blocked the gate to the tube. A blocking arm obstructed the tube just below the thick ball. Then the number of free balls was determined in such a way that the associated type wheel received a corresponding turn. A sequence of 40 letters was printed on the paper, the balls were expelled from the tube back into the chamber, and the operation could restart.

Each operation required about 7.5 seconds for the printing of one row and this speed corresponded to the capacity of a normal teleprinter. About 10 machines of this type were built, and some of them are still in use (Fig. 28b).

The chamber system as well as the type wheels could be changed for either 26 letters or 10 digits 0...9 so that either letter or number tables could be produced (Fig. 28).



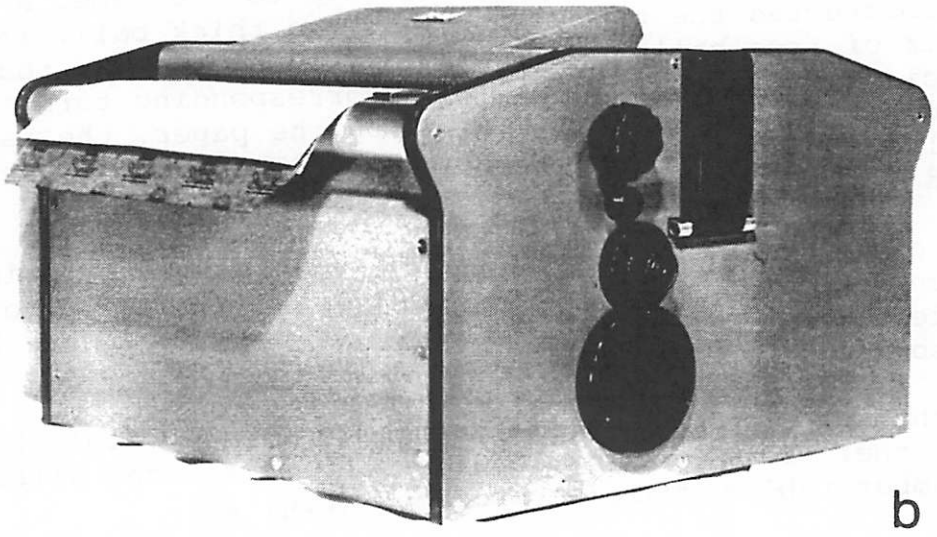


FIG. 28 RANDOM NUMBER GENERATOR WITH PRINTER CBI-53,
A: PRINCIPLE B: UNIT

4. Rotor Machines

Even when mechanical and electromechanical machines became obsolete the rotor machine was still surrounded by a certain aura. We knew that such machines were being used by the great powers, and we decided to build a "super" version. Because all machines of this type had the same weakness -- rotors with fixed wiring and simple motion. In 1952 we begun the first attempts to produce a different machine with special rotors. One feature in our development was the use of feed back. While only 26 circuits are needed for the input (keyboard) and output (printer), the rotors have 41 circuits of which the surplus wires are looped back outside the rotors.

All circuits could be rearranged by the use of modificators, so that 26! x 15! choices could be obtained (around 5.2×10^{38}).

The nine rotors were such that the connections within each rotor could easily be changed in 2^{41} different ways. Furthermore, the rotors could perform every desired combination of movements like those used in the modern C Machine. The program choice was enhanced greatly by the use of electrical switches. A complete block diagram is shown in Fig. 29.

A number of these rotor machines were supplied together with the tape punch device PEH-61 (Fig. 30) to a French government agency. The inconceivably large number of 10^{600} variations was theoretically possible with this machine. Due to the development of electronic machines, the manufacture of the HX-63 and the PEH-61 machines was discontinued. We manufactured for another firm a sizeable number of high-speed printers and tape readers originally developed for this machine.

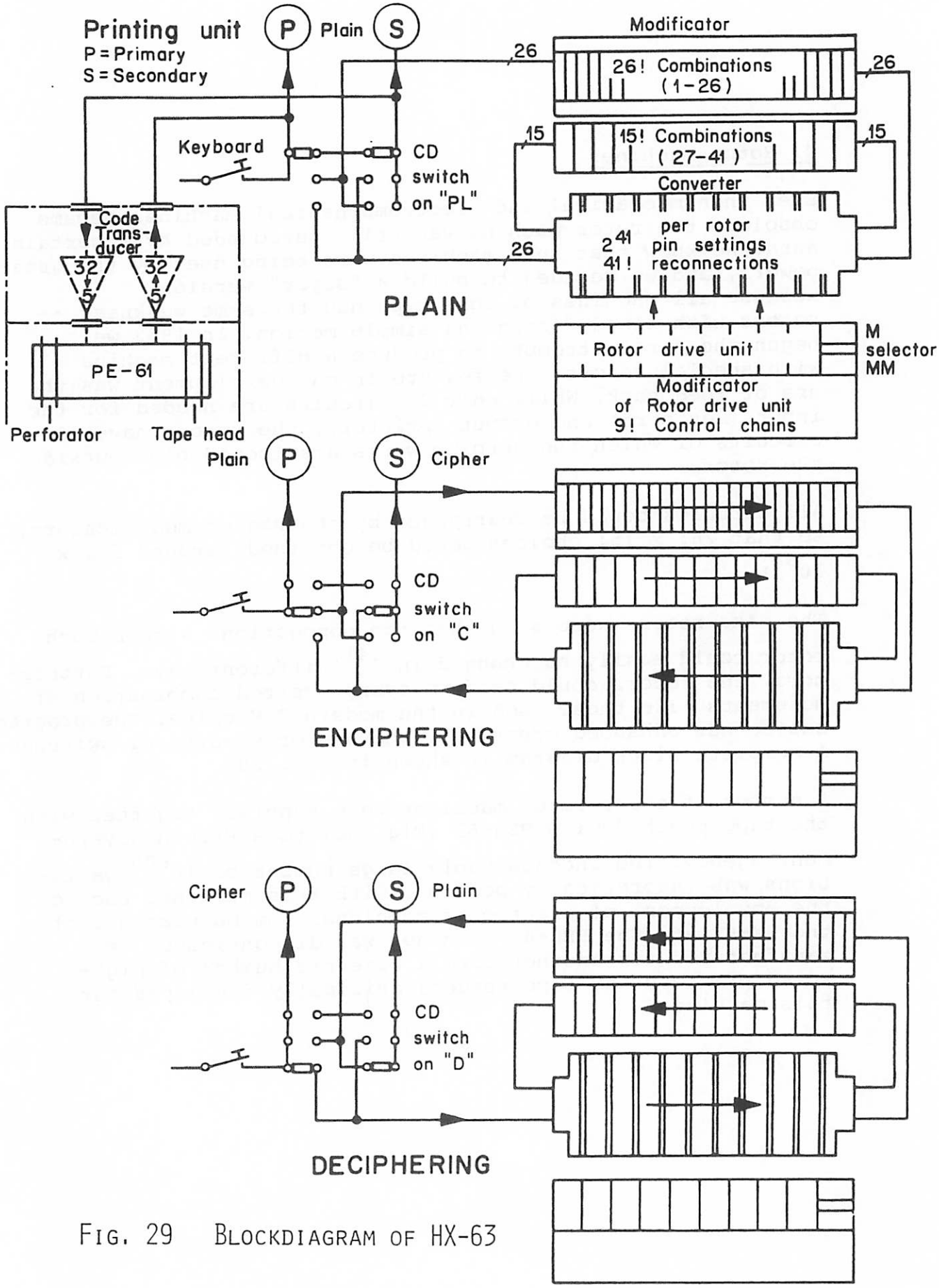


FIG. 29 BLOCKDIAGRAM OF HX-63

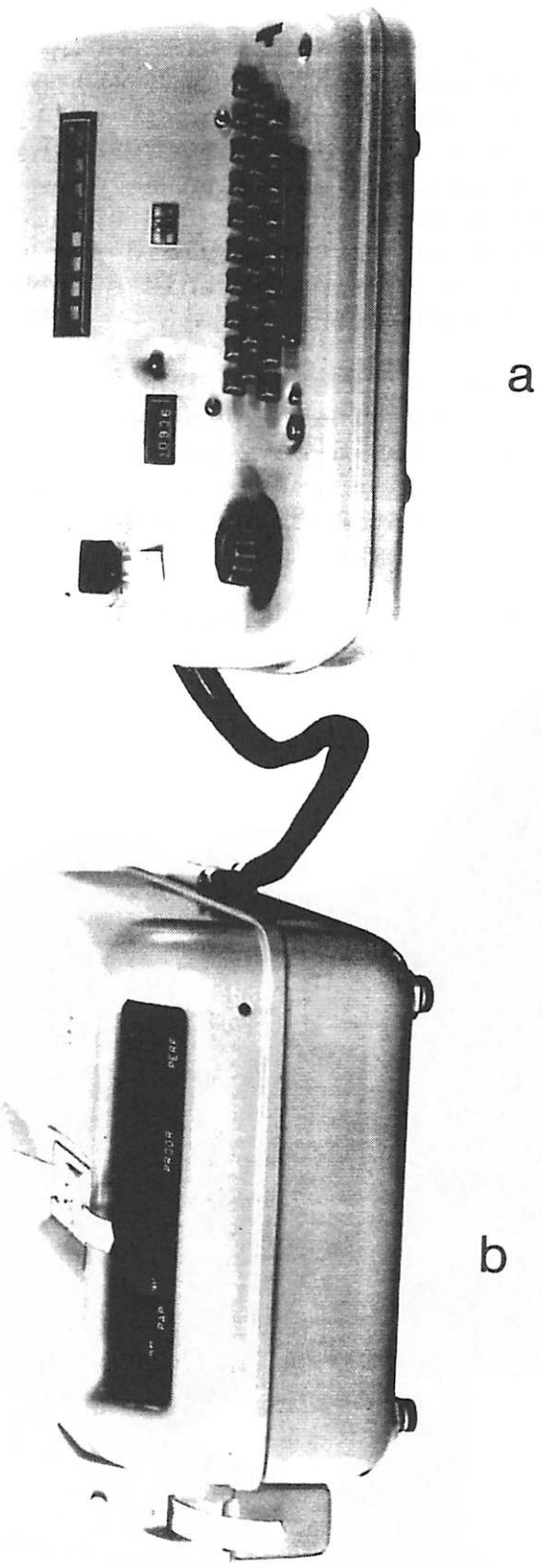


FIG. 30 A: ROTOR-MACHINE HX-63 B: PAPER TAPE UNIT PEH-61

5. The CDS-62 Machine

Since 1955 I had the idea of improving the CD pocket machine further by the addition of a multi-alphabetical attachment. In 1950 the renowned cryptologist William F. Friedman had once suggested I redesign the C Machine in order to enhance its applicability. This was to be done by the use of 16 different types of wheels which would engage in an irregular manner. This suggestion unfortunately did not work in practice. I used, however, a version of this suggestion as an improvement for the CD-57 machine.

In Sweden I made a first attempt by mounting on the turnable shaft of the CD machine a cylinder on which 32 alphabets were inscribed. These could be read off against a fixed reference alphabet. One could say that this was simply an improvement of A.G. Damm's first machine, but with a vastly longer period (Fig. 31).

I changed the design and introduced interchangeable cards carrying random alphabets (Fig. 32).

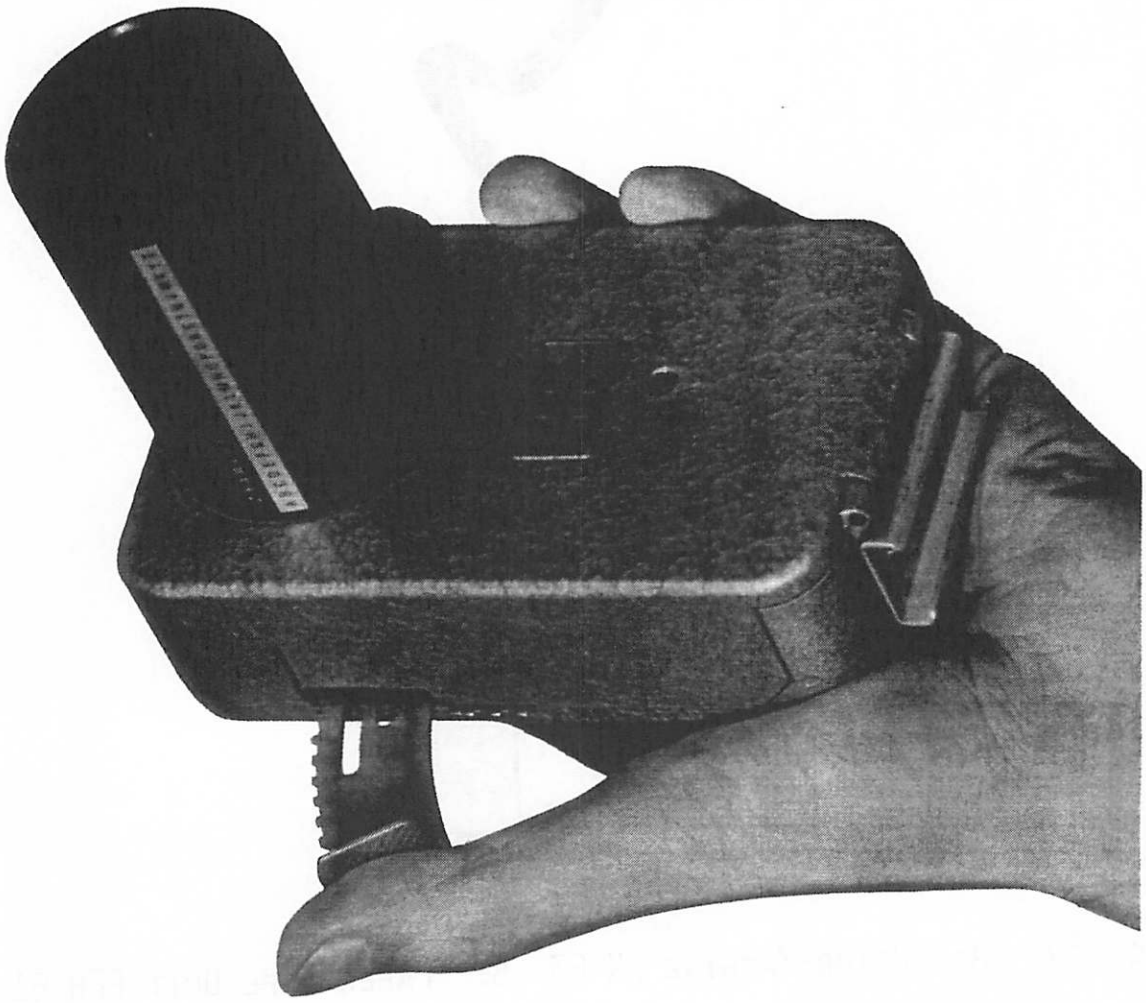


FIG. 31 CDS-62: CD-57 WITH MULTI-ALPHABET ATTACHMENT

The alphabet ring of the CD-machine was removed, the turnable alphabet disk was replaced by a wheel with a control cable which could shift the positions of the strip which carried the reference alphabet from top to bottom over the 32 different alphabets of the card. On the back of the card were the corresponding reciprocal alphabets to be used in decipherment.

So that the machine could be used even if separate alphabet cards were not obtainable, there was imprinted under the removeable cards a fixed Vigenère table whose alphabets were written in reverse sequence to the reference alphabet with rows 1 to 6 repeated.

Unfortunately, this course of development did not lead to manufacture of this device since at the time we were fully engaged with the development of electronic machines.

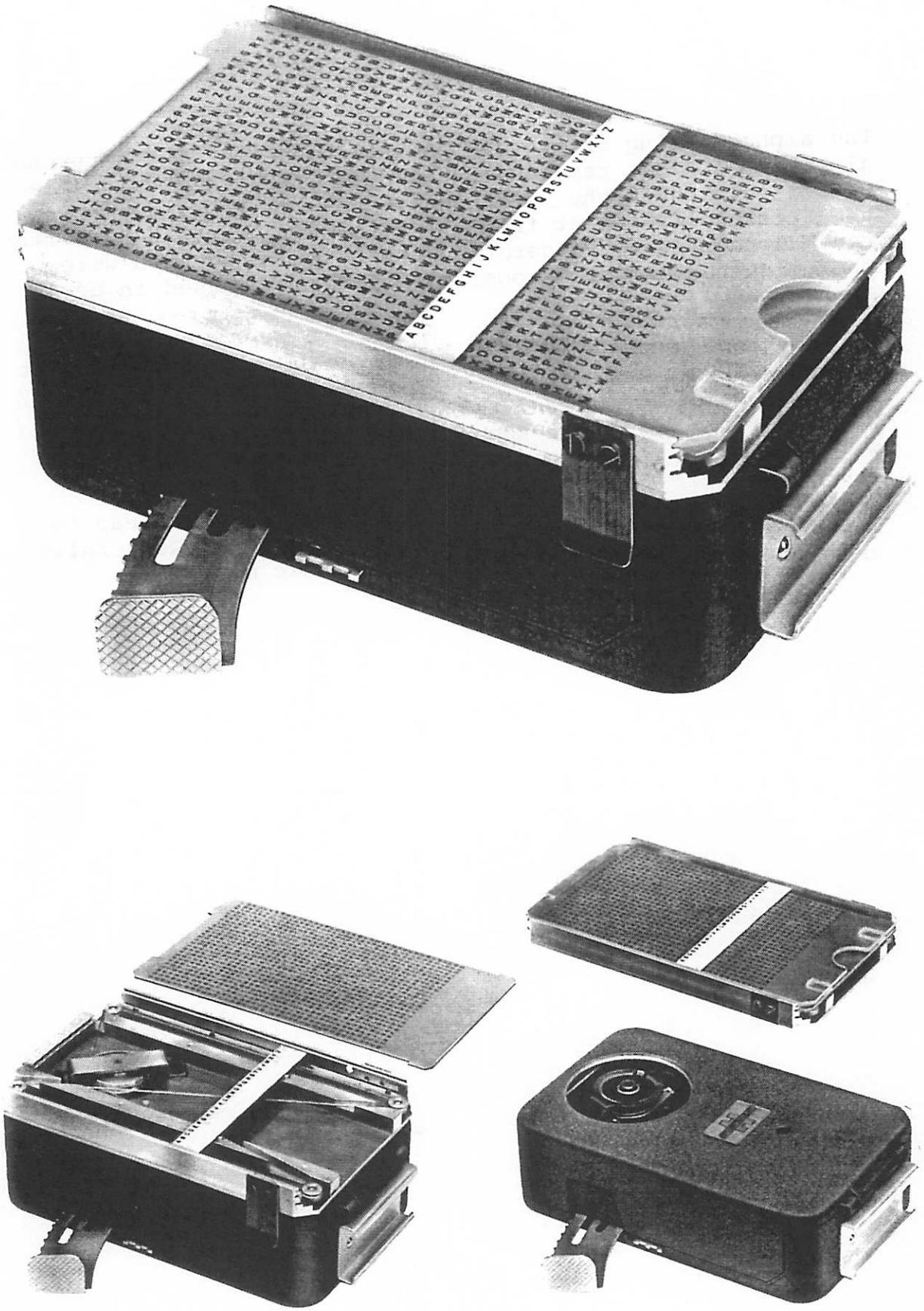


FIG. 32 CDS-78 (SAMPLE UNIT)

Closing Observations

The literature of cryptography and cryptanalysis up to now was primarily concerned with manual systems which were developed during the last five centuries. Although cipher machines have been used more and more during the past fifty years, the subject literature is scarcely informative. It is clear that the large countries with their unlimited material and technical resources have done much work in this specialized field. It is equally obvious that the results of such efforts are not published.
Each nation has to look out for its own security and does not want to disclose any useful data to its adverseries.

The use of computers for the cryptanalysis of cipher machines was developed by the British during the Second World War, and has steadily been refined. It is now daily routine.

For cryptanalysis it is mandatory to know the characteristics of the machine. In addition the cryptanalyst gets considerable help from poor operational practices of the machine. Human errors can simply not be eliminated. On the other hand the cryptanalyst today still has the chance of success through his own intuition as he depends on the "probable word", i.e., on stereotyped, often used expressions. Direct betrayal or unintentional indiscretion naturally do not belong to the technique of cryptanalysis. This art depends mainly on statistical methods, which allows the recognition of repetitions of chosen machine settings which arise through overlaps of keying periods.

For this reason secure cipher communication requires not only good equipment but also cryptologically trained personnel to prepare the operating instructions for the machine, and very trustworthy, well trained operators who strictly observe these instructions.

Because the C Machines have been sold in more than 50 countries and are still being sold, the characteristic components of these machines can be described in more detail. These parts are as follows:

1. Setting disk or keyboard plus type wheels. When the alphabet consists of 26 letters, these letters can be arranged in 26! or about 4.3×10^{26} different sequences. Moreover the indicating disk can be put into 26 different positions relative to the type-wheel. There is also a mechanism which allows this relative position to change between the primary and secondary type wheels continuously during the processing of a message.

2. 32 slide-bars in the drum. Here 6×10^{24} possible arrangements of the lugs are available when all steps from 0 to 25, i.e., 26 steps, are included. These can be permuted in 720 different ways. Special cams on the drum bars can also be used to effect the movement of the pin-wheels. These particular slide-bars are equipped with cams which work as teeth.

   There are 4 possibilities of action by such teeth:

   a) The tooth moves the associated pin-wheel when the slide-bar has moved into active position.

   b) The tooth moves the wheel when the slide-bar has remained in inactive position.

   c) The tooth moves the wheel no matter what position the slide-bar is in.

   d) The tooth does not move the wheel no matter what the position of the slide-bar (see more below on the performance of the CX and CXM). The possible actions just described make $4^6 = 4096$ possibilities for one slide-bar or $(4^6)^{32}$ = about 4×10^{115} possibilities for the 32 slide-bars.

3. Pin-wheels. Here we have the largest number of possible variations. There are 12 different pin-wheels to choose from, and 6 wheels are used at one time in the machine. The 12 different wheels, used 6 at a time, make 663,280 different combinations, giving period lengths between 10^8 and 2.7×10^9. The number of starting positions for the pin-wheels is the same as the number of different combinations, but the number of possible different pin combinations reaches astronomical numbers. Assuming half of the pins on each wheel are active, which has been found to be most secure, we get for example with the wheels 29, 31, 37, 41, 43 and 47 about 10^{67} different pin combinations.

The C Machines, as already mentioned, were originally designed for tactical use but gradually began to be used in the diplomatic services. Every cipher service has to set its own rules; nevertheless the numbers given above showing the abundance of different possibilities for setting the machine may be of general interest.

There are three main varieties of the C Machine:

The normal C Machine (as well as the CD-57) when using regular movement of the pin-wheels displays very long periods before the key repeats, but there are subperiods. For this reason messages with the same pin settings on the same wheels should not be too long, and the pin settings on the pin-wheels for the important traffic should be changed frequently. In addition all other possible variations should be kept in mind and used.

The CX Machine with irregular movement of the pin-wheels brings the advantage that non-linear movement sequences can be obtained. If certain mathematical conditions are met in the compilation of the material for the keys, then the periods occuring will be sufficiently long. In simple terms it can be said that the length of the period is determined by the number of pin-wheels which control another pin-wheel.

The CXM Machine is a compromise between the other two machines (C and CX). The movement scheme for the pin-wheels here is as follows:
The wheel I (from the left) turns regularly one step in each operation. This wheel controls wheel II. Wheel III is controlled by wheels I and II, wheel IV by the three preceding wheels, wheel V by its preceding wheels, and wheel VI by its preceding wheels. All six wheels have the same number of divisions, the length of the period will be n^6, or with six wheels with 47 divisions will have a length of about 10^{10}. With this system only the first wheel has subperiods which affect the drum slide-bars which are controlled by this wheel, while the remaining pin-wheels get an irregular movement. With this machine somewhat simpler keying instructions can be used than with the C or CX machines without endangering security.

The three machines offer various advantages, and each user has to decide for himself which machine he wants. He has also to set up the instructions for the safe use of his machines, which is dependent on their deployment.

The numbers given in this section are hard to comprehend. Even the number 10^{15} corresponds approximately to the distance from the earth to the sun in milimeters. The numbers cited have significance only as far as they show that the possibilities for all machines of the C-type are practically inexhaustible. But these numbers are meaningless if the user does not carefully accept and exercise the instructions and does not make full use of the possible variations.

The old rule is still true:
the quality of a machine depends largly on its user.

vp-kk-ak

AHB