5.4.61

Cryptograf typ HR-61. Kort, preliminär beskrivning.

Chiffreringsmekanismen i maskinen HR-61 består av en sats om nio genomgångshjul, med 41 genomgångar. Av genomgångsledningarna äro vid ändstyckena 26 förbundna med tangentbord och tryckverk, medan de övriga 15 in-, resp. utgående ledningarna äro parvis förbundna med varandra. Beroende på kopplingarna inom resp. genomgångshjul samt dessas inbördes lägen kan, när en strömkrets sluts från en tangent fram till tryckverket, denna i det enklaste fallet passera genomgångshjulen endast en gång, medan det i det mest komplicerade fallet kan bli sexton genomgångar. Denna anordning med återföringar (ibland kallat reinjektion) komplicerar givetvis chiffreringsmönstret.

Matningsrörelsen för genomgångshjulen sker enligt vårt s.k. M-system, vilket medför att periodlängden, trots möjligheten att ändra karaktären hos frammatningsmönstret inom synnerligen vida gränser, alltid blir densamma, och i förevarande fall 41^9, dvs. C:a 1.63×10^{15}. Rörelsemönstret ändras genom olika anordning av de stift, som finnas placerade utefter genomgångshjulens periferi.

Genomgångshjulens kontakter äro på hjulens ena sida fasta (plana), och fjädrande på den andra. De fjädrande kontakterna kunna lätt frigöras från sina platser, och bringas att intaga nya platser. I princip levereras maskinen med de fjädrande kontakterna anordnade så att direkta genomgångar erhålls, detta tillåter en enkel kontroll av maskinens strömkretsar. Kunden kan, sedan maskinen underkastats leveransprov, anordna strömkretsarna inom genomgångshjulen enligt egna önskemål. Sednare omflyttningar av kontakterna torde knappast vara behövliga, då följande ytterligare möjligheter till modifikationer — utöver användningen av nya utgångslägen - finnas: 1) Hjulens ordningsföljd sinsemellan kan lätt varieras, varvid antalet olika lägeskombinationer utgör $9!$, dvs. 362,880. 2) Dem inkommande ledningarna från tangentbordet till genomgångshjulen föras över en omkopplare (modifikator) som består av 41 kontakt skivor, med 41 lägen. Medelst denna omkopplare kan man åstadkomma $41!$, dvs. C:a 3.3×10^{49} olika ledningskombinationer. 3) Genom olika inställning av stiften erhålles, som ovan nämnts, ett mycket stort antal olika mönster för genomgångshjulens matningsschema.

Det är givetvis även möjligt att genom att anskaffa ett antal extra genomgångshjul införa ytterligare variationsmöjligheter.

Att i tal ange summan av inställnings- och omställningsmöjligheter saknar mening, då endast ett försvinnande litet antal av dessa möjligheter kan komma till användning. Normalt torde val av nytt utgångsläge, och evt. nyinställning av modifikatorn vara tillräckliga för att säkerställa chifferhemligheten.

Maskinens fördelar, utöver en högklassig chiffreringsmekanism, äro följande:

1. Funktionshastighet minst 8 tecken per sekund.
2. Dubbeltryck, dvs. såväl klartext som chiffer erhålles tryckt, den ena under den andra på en remsa, som låter sig dela mitt itu. Chiffret innehåller endast 26 bokstäver, medan (den tryckta) klartexten kan innehålla även siffror och andra tecken. Härtill

kommer även möjligheten att skriva klartext på båda remshalvorna, t. ex. för adresser och tjänsteanmärkningar.

3. Motorn och det elektriska systemet kan anslutas såväl till växelströmsnät 40–60 per, och normala spänningar från 110 till 250 volt, som till en 12 volts likströmskälla (batteri).
4. Maskinen har samma dimensioner som en normal skrivmaskin.

Konstruktion. Maskinen utförs enligt bygglådeprincip, där de olika delarna utgöra självständiga enheter, som följer:

a) Bottenplatta, med nätaggregat och motor.
b) Treradigt tangentbord, med mellanslags- och skifttangenter, samt omkopplare.
c) Tryckverk.
d) Konverter (Genomgångshjuls-sats).
e) Modifikator.

Genomgångshjulen äro tillverkade enligt ett nytt system, där kontakterna äro skyddade för smuts och damm, och där nednötning av kontakterna nedbringats till ett minimum genom att en isärskjutning äger rum mellan hjul som matas fram och stillastående hjul. Utgångslägena kunna avläsas genom ett plastfönster, och inställning av utgångslägena sker med motorkraft, genom att trycka på knappar framför resp. genomgångshjul.

Source: Boris Hagelins Privatarkiv, Vol. 6:3, Krigsarkivet (The Military Archives of Sweden), Riksarkivet, Stockholm, Sweden.

5.4.61

Cryptograph type HR-61. Brief, preliminary description.

The Cyphering Mechanism in the HR-61 machine consists of a set of nine permutation wheels, with 41 connections. Of the connections, 26 are connected at the end plates to the keyboard and the printer, while the other 15 input and output lines are connected to each other in pairs. Depending on the connections within the respective permutation wheels and their relative positions, when a current circuit is closed from a key to the printer, in the simplest case, this may pass through the permutation wheels only once, while in the most complicated case there may be sixteen passes. This device with re-entry (sometimes called re-injection) naturally complicates the encryption system.

The feed movement for the permutation wheels takes place according to our so-called M-system, which means that the period length, despite the possibility of changing the character of the feed pattern within extremely wide limits, always remains the same, and in the present case 41^9, i.e., about 1.63×10^{15}. The movement pattern is changed by different arrangement of the pins, which are placed along the periphery of the permutation wheels.

The contacts of the permutation wheels are fixed (flat) on one side of the wheels, and springy on the other. The resilient contacts can be easily released from their places and made to occupy new places. In principle, the machine is supplied with the resilient contacts arranged so that direct feedthroughs are obtained, this allows an easy check of the machine's circuits. The customer can, after the machine has been subjected to delivery tests, arrange the circuits within the permutation wheels according to their own wishes. Later relocations of the contacts are unlikely to be necessary, as the following additional possibilities for modifications — in addition to the use of new starting positions — exist: 1) The order of the wheels among themselves can be easily varied, whereby the number of different position combinations is $9!$, i.e., 362,880. 2) The incoming wiring from the keyboard to the permutation wheels is passed over a switch (modifier) consisting of 41 contact disks, with 41 positions. By means of this switch one can achieve $41!$, i.e., about 3.3×10^{49} different wire combinations. 3) By different setting of the pins, as mentioned above, a very large number of different patterns for the feed scheme of the permutation wheels are obtained.

It is of course also possible to introduce additional variations by acquiring a number of extra permutation wheels.

Stating in numbers the sum of setting and adjustment possibilities makes no sense, as only a vanishingly small number of these possibilities can be used. Normally, the selection of a new starting position, and possibly resetting the modifier will be sufficient to ensure cipher secrecy.

The advantages of the machine, in addition to a high-class encryption mechanism, are as follows:

1. Operating speed of at least 8 characters per second.

2. Double printing, i.e., both plaintext and cipher are printed, one under the other on a strip, which can be divided in half. The cipher contains only 26 letters, while the (printed) plaintext may also contain numbers and other characters. In addition, there is also the possibility to write plain text on both halves of the strip, e.g., for addresses and service notes.
3. The motor and the electrical system can be connected both to AC mains 40–60 period, and normal voltages from 110 to 250 volts, as well as to a 12-volt direct current source (battery).
4. The machine has the same dimensions as a normal typewriter.

Construction. The machine is made according to the construction box principle, where the various parts form independent units, as follows:

a) Bottom plate, with power supply and motor.
b) Three-row keyboard, with spacebar and shift keys, as well as switches.
c) Printer.
d) Converter (Permutation Wheel Set).
e) Modifier.

The permutation wheels are manufactured according to a new system, where the contacts are protected from dirt and dust, and where wear and tear of the contacts is reduced to a minimum by a separation taking place between wheels that are fed forward and stationary wheels. The wheel positions can be read through a plastic window, and the setting of the wheels is done with engine power, by pressing buttons in front of the respective permutation wheel.

Source: Boris Hagelins Privatarkiv, Vol. 6:3, Krigsarkivet (The Military Archives of Sweden), Riksarkivet, Stockholm, Sweden.