

The Hagelin Cryptographers — a review and a program

It was forty years ago, when I was a young man, that I first met the Swedish inventor A.G. Damm. He had originally been a textile engineer but had for many years been interested in cryptography. He and his brother — who was a mathematician — had on some occasion developed a secret language, in which they used to correspond. This led to the study of cryptography in general and ciphering devices in particular, and in the year 1916 AB Cryptograph was formed in Stockholm, for the exploitation of A.G. Damm's inventions. His brother had in the meantime died.

A special homage must here be given to the memory of A.G. Damm. He must justly be considered as the foremost pioneer of the ciphering machine industry, and we have to thank him for most of the fundamental construction principles, on which the modern ciphering machines have been based, including the ciphering commutator ("rotor"), which became widely known through the German Enigma machine.

A large number of different devices were designed and built under Damm's supervision over the years, but very few came into practical use, Damm's tragedy was that he was a pioneer; he had to start from scratch with his constructions, he did not have a designer's mind and had therefore difficulties in arriving at practical solutions. And what was still worse the market for ciphering machines was as yet practically non-existent and had to be developed. It will therefore be easily understood that AB Cryptograph did not become the financial success which its enthusiastic backers had expected, and very large amounts of money were used up for experiments and the manufacture of prototypes. In 1922 Mr. Emanuel Nobel, then head of the famous family of industrialists, and his colleague (my father) Mr. K.W. Hagelin, were persuaded to finance the company, and I was given the responsibility to act as observer.

A unique collection of these machines is intact, and may become the object of a special separate treatise. My contacts with Damm were to the begin with neither frequent nor intimate, but as the years wore on, it became necessary for me to devote more time to this venture — additional means had to be procured almost continuously to keep the work going, with no end in view. Most unfortunately, Damm's health began to deteriorate, he died in 1927 after a long illness, and something drastic had to be done if the work were to continue. I had in the meantime become fascinated by this for me completely new technique, and I decided in 1926 to try my hand at the construction of a ciphering machine, as the Swedish General Staff was then considering the purchase of portable ciphering machines. I had at the time no qualifications as a designer of ciphering machines, but I had at my disposal a number of different Damm machines to study, and also the conviction, that to be a success, a ciphering machine should be as simple as possible, and rely on mechanical processes in the widest possible extent. I found that I could utilise one of Damm's last inventions, "Simplified ciphering commutators", which I put to use for a portable machine, with keyboard and lamp indication, with its exterior fashioned after the Enigma machine, which was at that time manufactured in Berlin. This machine, called B-21, was in due time accepted by the General Staff, and became the first type to be commercially produced by AB Cryptograph, more than ten years after the formation of that company. This offered some hope for commercial success, but before this could materialize, Mr. Nobel died, and

AB Cryptograph having lost its principal backer had to be liquidated in 1932. At this point, I made a bold decision: I took on the work and the financial responsibility myself and was with much luck able to carry on. Although the difficult years up to 1939 seemed long at that time the ensuing development can be stated very briefly:

The B-21 was succeeded by a tape-printing machine with motor drive, the B-211, of which was a small number made in Sweden. This machine was then put into production in France for the French Army and Air Force, and an appreciable number of these machines was built both before and after the last war. In 1934 I was asked by my French clients to design a small portable mechanical tape-printing machine. This machine came on the market in 1935–36 and was manufactured both in France and in Sweden where I had formed a new company, AB Cryptoteknik. The construction of this machine, originally called the C-36 was made possible by one of those improbable but not unique inventor's chances, where designs, developed for a certain purpose, were found to suit, through that undefinable process called "inventing" some utterly different purpose. This machine was introduced by me in 1940 in the USA, where during World War II more than 140 000 machines were built. In the meantime, the corresponding Swedish model C-446, and its companion machine, type BC-543 with keyboard and motor drive, were manufactured by AB Cryptoteknik, and sold to a large number of countries.

With the end of the War in sight, it became my belief that the call for ciphering machines would diminish, and I acquired other interests which took most of my time. In 1948, I was however persuaded to collaborate with a Swiss firm, for the development of a ciphering type of telewriter, and moved to Switzerland.

I need not dwell on this interlude; the telewriter in question and with this the ciphering device did not meet with the expected appeal, and in the meantime, I had to turn my attention again to my own business. The demand for ciphering machines which had slipped during the first post-war years, began to mount again, and calls became frequent, not only for improvements on my old machines, but also for machines of other types.

It should be realized that in 1948 when I began to plan for the reactivation of my ciphering machine business, the "Hagelin" machines then in use were based on a design which was years old. These machines had stood the brunt on many fronts during World War II, and the need for improvements as well as for new constructions became obvious.

In planning for the future, I could well have limited my activities to the same kind of machines as heretofore: i.e., portable machines with mechanical ciphering functions. It became however very tempting to try to cover as much as possible of ciphering machine field, which had at that time become fairly familiar to me, especially as I had now some experience with electromechanical cryptographers, and with ciphering devices for telecommunication use.

I finally decided to go in for an as complete as possible line of machines and during the time from 19— when my first post-war machine became available to the users, to date (1961) the following new machines have been designed and built:

- The pocket machines of the types CD-55 / 57,
- the hand machines of the types C & CX-52,
- the electric drive for the C & CX machines of the type B-52, and
- the teleciphering machines of the T-52 & T-55 series.

The Hagelin Cryptographers — a review and a program

As the use of "random Tape" became an imperative for certain services, I found ways, if possible, to adapt the different machine types for tape ciphering as an alternative to the normally offered mechanical ciphering mechanism. Not only the teleciphering machines of the T-55 series could be equipped with tape readers but also the pocket and hand machines of the CD-57 & CX-52 types.

The use of random tape led to the design of random pulse generators (types [missing]) for the production of such key tape, and of a numbering device (type, MN [missing]¹) for the identification of the starting positions.

The demand for high operating speed and for still more sophisticated ciphering mechanisms has finally led to the construction of rotor machines. This work was started in [missing] and was pursued intermittently until [missing] when a decisive phase began.

The first operational prototype of this new machine type HR-61 is nearly in completion and further samples will be ready in the summer of 1962. With this machine, and the possible future variations of the cipher mechanism used for it, it is my belief that an ultimate has been reached at least as far as myself & my collaborators are concerned.

BH/Hü
11.12.1961

Source: The NSA Friedman Collection, REF ID:A2920126, pp. 56–60, [Unauthorized Declassification - Trip to the Marshall Library, Lexington, VA.](#)

¹ Editor: Most likely the MN-56 (1957–1960)