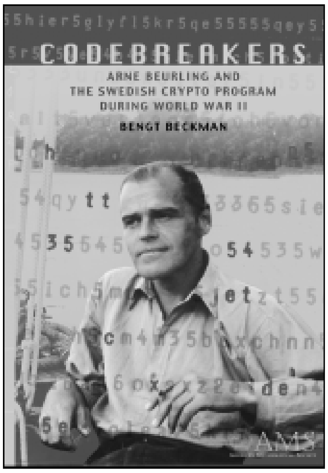
Codebreakers: Arne Beurling and the Swedish Crypto Program During World War II

Reviewed by F. L. Bauer

Codebreakers: Arne Beurling and the Swedish Crypto Program During World War II
Bengt Beckman
Translated from the Swedish by Kjell-Ove Widman
AMS, 2002, ISBN 0-8218-2889-4

The author of this book, Bengt Beckman, started in 1946 to work as a conscript for the *Försvarsväsendets radioanstalt* (abbreviated FRA), which is the cipher bureau of the Swedish *Försvarsstaben* (Defense Staff Headquarters). By that time the war was already history, but the young Beckman was told stories by some who took part in and carried out very important and impressive cryptanalytic feats. Now, more than fifty years later, this information is no longer classified. In fact, the story of the breaking of the German *Geheimschreiber* by Arne Beurling can be told—at least to the extent that Beurling disclosed it.

For many years Bengt Beckman, who retired in 1991, was head of the cryptanalysis section of the FRA. Thus he is equipped with comprehensive knowledge about many aspects and details of cryptology. While such a person usually remains behind a screen of inaccessibility, in 1993 Beckman was allowed to appear in a Swedish television documentary about cryptology. He was also permitted to publish in 1996 a revealing and generally intelligible book, *Svenska kryptobedrifter* (*Swedish Codebreaker*). Credit is due to the American Mathematical Society that now an English translation, carried out with great competence by Kjell-Ove Widman, has appeared. The translation allows a wide general public with no knowledge of the Swedish language to compare the Swedish successes with the Polish and British cryptanalytic achievements against the communication lines of the German *Wehrmacht*.


CODEBREAKERS
ARNE BEURLING AND THE SWEDISH CRYPTO PROGRAM DURING WORLD WAR II
BENGT BECKMAN
AMS

The book provides evidence that the Swedish achievements are remarkable. Just as Poland had Marian Rejewski and Great Britain had Alan Turing, Sweden had a hero: Arne Beurling, whose name appears in the subtitle of the book. Like Turing, Beurling (1905–1986) was a mathematical genius whose posthumous fame in mathematics has long been well established—after all, after the war he became a permanent member of the famous Institute for Advanced Study (IAS) in Princeton. Thus the AMS had good reasons to support the translation into English. The preface by Peter W. Jones, whose own

F. L. Bauer is professor emeritus of computer science and mathematics at the Technische Universität München.

This is a new version of Bauer's review of Codebreakers *that originally appeared in German in Mitteilungen der Deutschen Mathematiker Vereinigung, 2-2003.*

work is quite distant from cryptology, provides with judicious conciseness an impressive picture of the mathematical work of Arne Beurling.

Beckman's book naturally concentrates on the cryptanalyst Beurling. In this field, among a number of Beurling's astounding successes requiring great analytic aptitude and an almost prophetic gift, one result stands out because of its eminent importance for Swedish security in World War II: The cracking of enciphered communications traffic on the *Wehrmacht* line between Berlin and occupied Oslo. This line ran for some distance on a cable lying in Swedish territory.

In mid-1940, without having more than a slight inkling of the nature of the encryption used on the line, without ever having seen and investigated the machine (a Siemens *Chiffrierfernschreiber* T 52a), Beurling discovered the principles of the encryption after just two weeks of work. While the British codebreakers at Bletchley Park were familiar with the relevant patents—the German one by Jipp and Rossberg (1930) and the American one by Jipp, Rossberg, and Hettler (1933)—the FRA apparently was not aware of the importance this information would have for Beurling.

Beurling entered Uppsala University in 1924 and was a young mathematics postgraduate student when in 1931 he was conscripted and sent to a course in general cryptology and cryptanalysis conducted by Captain Erik Anderberg. One day Anderberg showed Beurling a new crypto device the military had bought and encouraged him to take the machine home over the weekend. After finding a weakness, Beurling asked Anderberg to give him a ciphertext containing a not-too-short "probable word". Anderberg enciphered a message starting with the word *överbefälhavaren* (supreme commander). Beurling came back and showed the full deciphered text to the surprised Anderberg, who could barely believe what he saw. (The device was the Swedish B21, the first machine constructed by the Swedish inventor Boris Hagelin.)

One can guess that this event made Anderberg remember Beurling. Beurling started a mathematical career after completing in 1933 his doctoral thesis, which became immediately famous and earned him a docentship (a kind of time-limited assistant professorship) at Uppsala University. In 1937 he was appointed to a chair for mathematics. On the first day of World War II, Beurling was drafted into the Defense Staff Headquarters under the assumption that for the Russian and German section a certain amount of mathematical cryptanalysis would be needed. Beurling first struggled successfully with the traffic of the Russian navy, in particular that of the Baltic navy, which used a five-digit code book, encrypted again by a polyalphabetic letter substitution, with a periodic key of length 300. While he was trying to use his results with the Red Army and the Arctic navy traffic, Beurling was called to help with a completely new and strange cipher: It had a 32-character alphabet, the 26 letters of the Latin alphabet having been supplemented by the numerals 1 to 6. Other signs that this cipher was unusual piqued Beurling's curiosity, and only then was he told the great secret, that Sweden had leased telex lines to the Germans and that naturally these lines were being tapped. In fact, this had started a few days after the German assault on Denmark and Norway on April 9, 1940, and by April 20 the eavesdroppers had established that standard teletype transmission of messages was involved. Frequently, the traffic consisted of the trivial chattering of idle operators, but increasingly, incomprehensible text was interspersed. It always started and ended with the sequence UMUM, and one could guess that this meant *umschalten* (switchover), i.e., that a transition involving an encryption machine was taking place.

By mid-May 1940 the necessary recording devices were set up, and Beurling started work. With the signals of May 25 and May 27, he was lucky. A German operator repeatedly committed a "sin": he retransmitted a message using the same initial setting. This would have been harmless had the transmissions been letter-for-letter absolutely identical. But because of the comfort the teletype machines offered, carelessness was frequent, and Beurling, who was waiting for such an occasion, spotted it. Some stupid regulations the German operators had been taught also helped Beurling, e.g., that for technical reasons a space symbol, 5, should always be followed by a letter shift symbol, 3, and that frequently internationally standardized technical terms were used, like QEV ("Did you understand?"). These small slip-ups, caused by the negligent habits of the German operators and by the ignorance of their supervisors, were later exploited on a daily basis by the Swedish codebreakers and by the Polish and British ones as well. Still, to the layman and even the hobby-cryptologist, this looks like a miracle. Beurling did not correct this impression; he never revealed exactly how he found the initial break and used to say, "A magician does not reveal his tricks." But, according to Jones, Beurling at least gave the enigmatic hint that "threes and fives were important."

Beurling finally was able to reconstruct completely the Siemens machine and had a great number of replicas built. He also organized the reconstruction of the keys that were changed from day to day. The information the Swedish government thus gained was vital for the survival of Sweden.

Beckman's book has completed the picture of the great cryptanalyst Arne Beurling given in the 1967 book by David Kahn and the 1993 *Mathematical Intelligencer* article by Bo Kjellberg. But for years

Beckman also knew Beurling the man, and he hints that his colleague had some remarkable facets, similar to those of Alan Turing. Both of them were eccentric. Young Beurling hunted alligators in Panama with his father, Ahlfors reported. Beurling loved hunting in the mountains of Lapland and sailing Sweden's archipelago. And with affectionate clarity Beckman reports that Beurling was a "ladykiller", attracted by intellectual women; in this regard his orientation differed from that of Turing. Kjellberg wrote that Beurling was one of the most charming persons one could meet and was helpful to his friends, but at the same time he scared some less gifted people. He was not averse to alcohol—understandable in the cold Swedish winter—and suffered from time to time from persecution mania.

Although Beurling was appointed a professor at the IAS in 1954, he never felt fully at home in the United States and did not become an American citizen. It was difficult for him to find the right social environment: He could hurt people without really meaning to, and, being suspicious, he could unexpectedly react in a hurt way himself. He mellowed as time went by, but for most of his life mathematics meant more to him than anything else. He was a perfectionist and loved to surprise people with a deus ex machina. He considered his mathematical results almost like private property. And he had no sense for public relations. As a result, despite the charisma he emitted he did not find in his lifetime the full recognition his genius deserved.

Bengt Beckman has produced a well-written, fascinating book showing the mathematician Arne Beurling in the Scandinavian world of Lars Ahlfors, Harald Bohr, Bo Kjellberg, Rolf Nevanlinna, and Lennart Carleson, as well as the part-time cryptologist Beurling in the depressing atmosphere in Sweden during the Second World War. This is an unforgettable book, even for those not addicted to cryptology.