A Tribute to the Memory of

Arne Beurling

1905–1986

By Professor Pontus Johnson, KTH
and Fredrik Wallin, historian FRA

Royal Swedish Academy of Engineering Sciences (IVA)

A Tribute to the Memory of

Arne Beurling

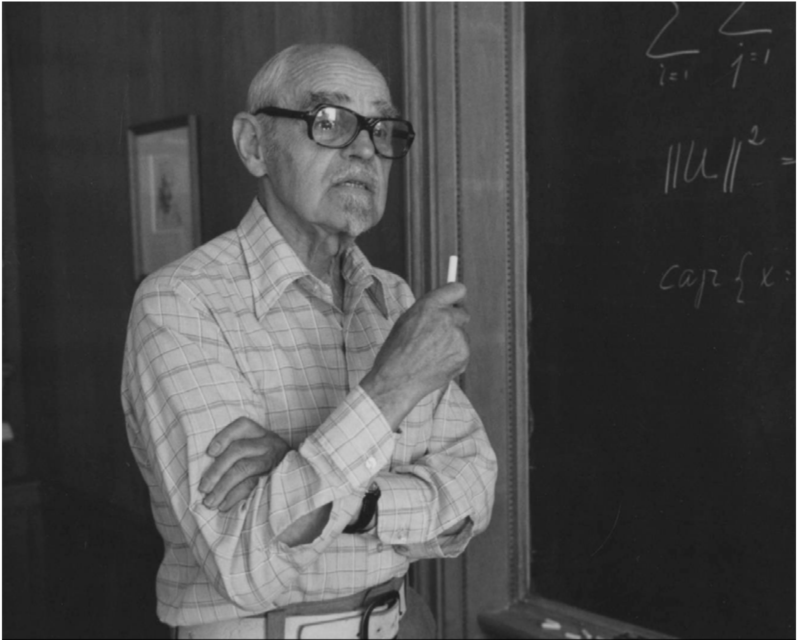
1905–1986

Presented at the 2022 Annual Meeting of the
Royal Swedish Academy of Engineering Sciences

By

Professor Pontus Johnson, KTH
and Fredrik Wallin, historian FRA

Contents



Arne Beurling at Princeton University 1981. Photo: Hermann Landshoff

Foreword

Each year the Royal Swedish Academy of Engineering Sciences (IVA) produces a booklet commemorating a person whose scientific, engineering, economic or industrial achievements were of significant benefit to the society of his or her day. The person recognised in the booklet must have been born at least 100 years ago. The Commemorative Booklet is published in conjunction with the Academy's Annual Meeting.

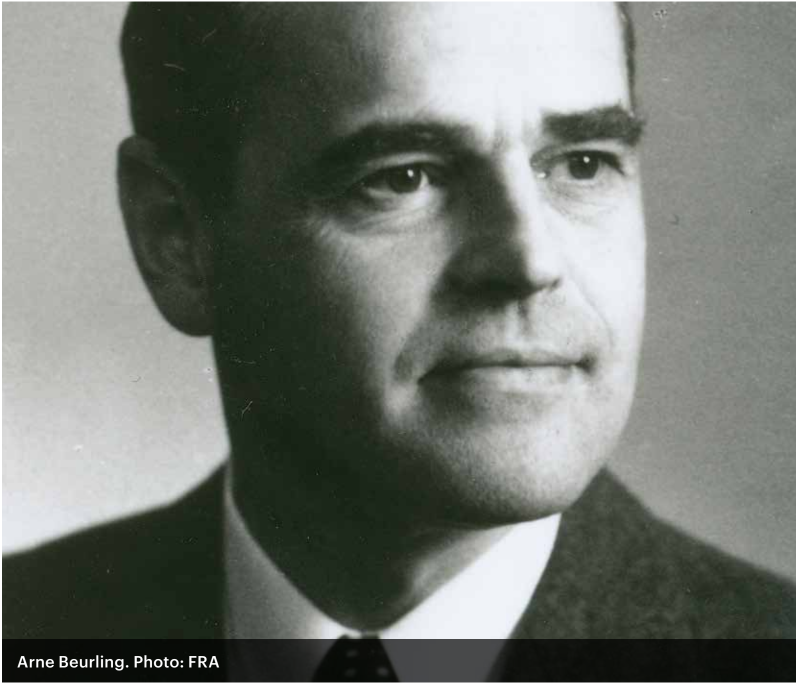
This year we acknowledge Arne Beurling, "the Swede who cracked the German code", for his crucial work in cryptology during World War II, in particular in breaking the T-52 Geheimschreiber. His contributions to the development of Swedish cryptology are of significant importance for Swedish cybersecurity today.

We would like to extend our sincere gratitude to Professor Pontus Johnson for the time and effort he, Ola Billger and Fredrik Wallin, both at the Swedish National Defence Radio Establishment (FRA), has dedicated to this year's Commemorative Booklet.

Tuula Teeri
President of the Academy

Camilla Modéer

Camilla Modéer
Chairperson of the Medals Committee



Arne Beurling. Photo: FRA

Introduction

Society's dependence on connected, computer-based systems has increased rapidly over the past few decades. Our energy supply, healthcare, financial system, food supply and transport system are all examples of critical, computer-controlled infrastructure. The systems that monitor and control such infrastructures can, however, be exposed to cyberattacks aimed at disrupting society or stealing information.

Cryptography is one of the most vital techniques to protect computer-based systems from cyberattacks. It is used to protect communication from unauthorised access and to ensure its authenticity, but also to verify the identities of communicating parties. Today, almost all communication over the internet is encrypted. Cryptography is crucial in securing messaging services, but also for secure control of critical infrastructure, for secure banking transactions, and to unlock car doors and smart locks. Blockchain technology, which is the basis for BitCoin etc., is based on cryptography. Cryptography is also used to ensure that the apps we use in our smart phones come from legitimate developers. Without cryptography our modern society would not be able to function.

Cryptography has an ever-present adversary in the form of cryptanalysis, the purpose of which is to break the cipher or code. In the same way as crash tests are vital for the construction of safe vehicles, cryptanalysis is crucial for building secure cryptographic systems. Just like vehicles, systems for encryption need to go through extensive testing before they can be considered reliable.

Cryptanalysis is also crucial when an opponent's cryptographic system needs to be broken. Knowledge is key in both military conflicts and in civilian competition. The ability to protect one's own communications and access an opponent's secret communications can be crucial. Arne Beurling did very important work for Sweden by breaking one of Germany's most important, strategic encryption systems during World War II. This gave Swedish decision-makers unique information about German plans and intentions during a critical period of the war. Beurling's work was also important for the development of cryptology at Sweden's National Defence Radio Establishment (FRA).

During the years in which Beurling was active, cryptology was a narrow field. Cryptosystems were used by military and other government agencies to protect the content of military and diplomatic communications, but for the wider public, encryption was more of a curiosity. In today's increasingly digitalised society, encryption is used in many contexts to protect information or to identify us as users, often without us even thinking about it.

Background – Encryption and signals intelligence

Ever since ancient times, there has been a need to conceal the content of letters and messages. Various methods have been invented to encrypt the content of a message, in other words to make it illegible for unauthorised persons but legible for the correct recipient with the knowledge and the key to solve the encryption. With the development of the telegraph and radio, it became even more important to use encryption to conceal the content of communications.

At the beginning of the 20th century encryption was carried out manually using code books and tables. This was a time-consuming process that required precision and well-trained users. The 1920s saw the development of various types of cipher machines that could automatically encrypt text typed into them. This provided better encryption and was also significantly more expedient. The most well-known of these is the German Enigma machine, but there were several other types of cipher machines produced in various countries, including Sweden.

Solving someone else's encryption system without knowledge of how it works is called breaking the code. Code-breaking makes it possible to access the content of an opponent's communications, which can enable crucial successes in warfare or diplomacy.

Intelligence is a term that is used to describe information on an enemy's or opponent's plans and intentions. It usually involves military or diplomatic information but can also apply to technical know-how. Intelligence usually needs to be fresh – if it gets too old it is no longer relevant.

Obtaining intelligence from foreign radio and telegraphic traffic is called signals intelligence, and the Swedish armed forces understood its potential early on. Signals intelligence was already being used in Sweden during World War I. At the beginning of the 1930s there were code-breaking courses available for "suitable conscript students" because the ability to break an opponent's cryptosystem is a vital aspect of signals intelligence. This would prove to be very useful in WW II, when one of these conscript students, Arne Beurling, took the lead in breaking one of Nazi Germany's most important cryptosystems, providing Sweden with highly important intelligence during the war.

Upbringing, studies and private life

Arne Beurling was born in Gothenburg in 1905. Beurling's father, Konrad Beurling, was a sea captain whose family owned land in Dalsland. In 1900 Konrad married Elsa Raab and they went on to have two sons, Åke and Arne. The couple divorced in 1908 after which the brothers were mainly raised by their mother and her companion Titti Winberg. Arne graduated from upper secondary school in Gothenburg in 1924 and the same year he travelled to Uppsala to study mathematics at the university there. He received his PhD in Mathematics in 1933 and continued to do research and teaching in Uppsala.

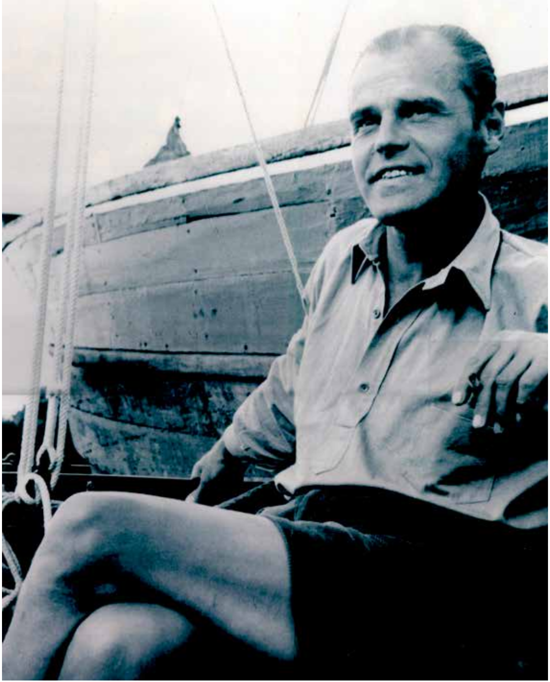
During the years 1930–31 Beurling did his military service. He was one of the "suitable conscript students" who was selected for the course in code breaking. He distinguished himself as a code breaker, including by cracking a coded message encrypted on the B21, the Swedish military's newest cipher machine.

After completing his military service Beurling resumed his work in Uppsala and from 1937 he held one of two professorial chairs in mathematics at Uppsala University. Beurling's lectures were described in glowing terms by many of those who attended them.

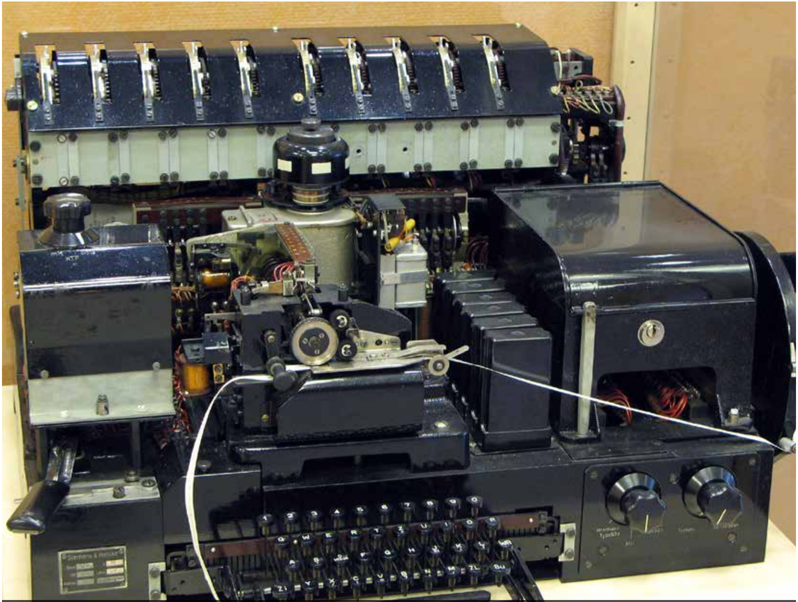
Beurling was usually described as a handsome man. He was in good physical shape, he loved nature and enjoyed various outdoor activities such as hunting, hiking in the mountains and sailing. He was usually quiet in a crowd, but he was also charismatic. As is often the case with geniuses, he had some difficult and erratic sides to his personality. Those around him have testified to his short temper. It was not unusual for him to quarrel with colleagues or acquaintances. On the other hand, he could often be generous and sympathetic.

In August 1930 Arne Beurling met Britta Östberg, a young medical doctor who was completing her education at Uppsala University. They started spending time together and became engaged in 1931. In 1936 Britta became pregnant and they got married later that same year. The couple had two children, Pehr (1936) and Christina (1938). Their relationship has been described as stormy even during their engagement. They were two individuals with strong personalities who were both quick-tempered. The marriage was dissolved in 1939.

Beurling remarried in 1950. His second wife, Karin Lindblad, was also an Uppsala academic. She accompanied him to USA where she did research in chemistry.



Arne Beurling on his yacht. The photo was taken after the war. Photo: Anne-Marie Yxkull



The Siemens & Halske T-52 in the museum of the FRA. The machine normally had a black hood. In the photo the hood has been removed to show the inner workings. FRA obtained this machine after the war. Photo: FRA

Arne Beurling and the Swedish Defence Staff's Crypto Department/FRA

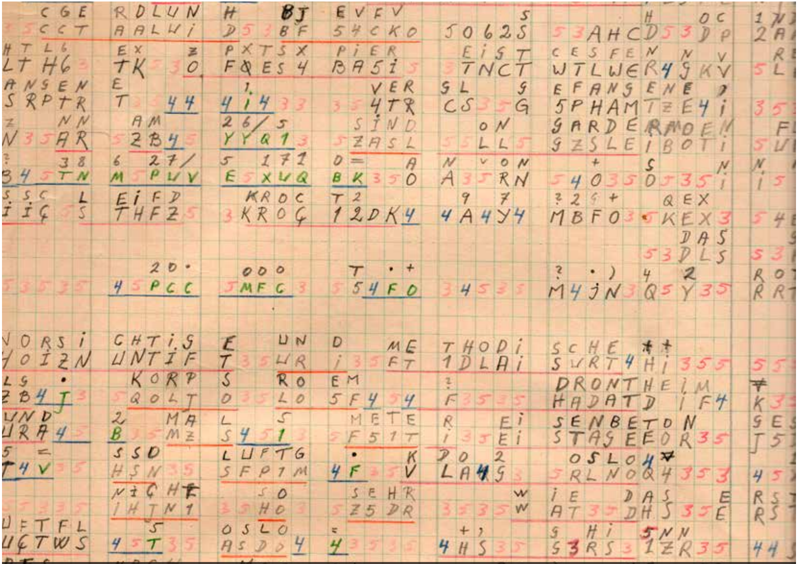
When the war broke out in 1939 Arne Beurling telephoned the head of the Defence Staff's Crypto Department, Eskil Gester, and said that he was willing to be called up to serve. Beurling was initially made responsible for the work against Soviet codes, which at the time had highest priority. He worked at first on analysing Soviet diplomatic encrypted messages and later on the Soviet Baltic fleet's encrypted traffic. Beurling and his colleagues achieved significant success in breaking various Soviet cryptosystems. One of his colleagues, the cryptologist Åke Lundqvist, says: "Everything seemed infinitely simple when Beurling explained it. He worked as far as possible with the least complex methods possible – both in his teaching and in his work."

In spring 1940 Beurling started working on deciphering traffic encrypted by the German T-52 Geheimschreiber cipher machine. The background was that, after occupying Norway, Germany demanded that the Swedish Government should allow them to use telegraph cables running through Sweden to Norway. After some deliberation, Sweden agreed to this but naturally saw an opportunity to intercept the traffic. The Germans were aware of this risk and protected their communications by encrypting the traffic. The cipher machine they used was called Siemens & Halske T-52, nicknamed "der

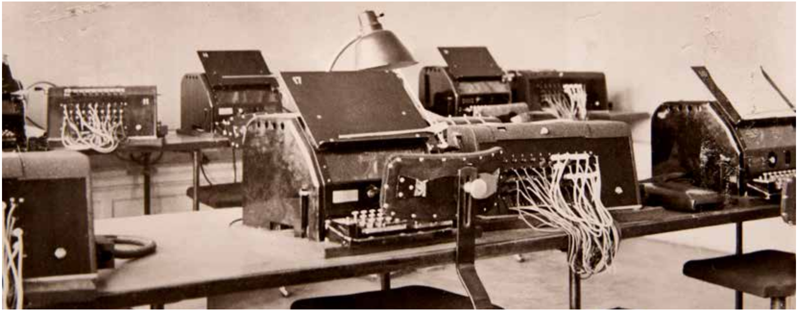
Geheimschreiber" ("secret printer") by the German operators. This became G-skrivaren in Swedish (the G-printer). The Swedish Defence Staff and Telegrafverket (the telecom agency in Sweden at the time) worked together to intercept the traffic. The T-52 was an encrypted teleprinter, and the material that the Swedish interception produced was incomprehensive sequences of letters and numbers on paper strips. The interception work was carried out in a run-down building at Karlaplan 4 in Stockholm, called Karlbo, which had been at the disposal of the Defence Staff since the beginning of the war.

At Karlbo they were having difficulties deciphering the German material and the task was given to Beurling. At that time he worked on Soviet traffic at the Rabo facility located on the island of Lidingö outside Stockholm. The new material he received consisted of bundles of paper strips glued to paper sheets. This was the traffic from the T-52. One problem was that the material was often not gathered in a way that matched the sender traffic with the recipient traffic. Eventually, however, he found material from two days where sender and receiver matched. With this as his starting point, he was able to break the code after just two weeks of work. Although Beurling was the one whose analysis produced the crucial results, he was assisted in parts of the work by mathematicians Hans Rudberg and Bertil Nyman.

Beurling himself never described how he managed to crack the code. When asked, his answer was evasive: "A magician never reveals his tricks." One important clue is that when the T-52 was used in traffic it was common for the operator to insert an alpha shift (the character in the teleprinter traffic indicating a switch from numbers to letters) at each



Part of an original document that was used in breaking the T-52 Geheimschreiber code, possibly by Arne Beurling himself. In the document pictured, we can see parts of the German communication in plain text and the names of locations in Norway. On a paper printout the alpha shift was registered as 3 and space as 5. In the decoding process these were written with a red pen because they were particularly important. Photo: FRA



Decoding devices at Karlaplan 4. The decoding devices were connected to teleprinters and young women sat at each device typing the ciphertext into the teleprinter. Plain text was then printed out on paper strips. Photo: FRA

space to avoid it getting stuck in the number mode. This meant that the combination alpha shift + space was very common. Carl-Gösta Borelius, who himself worked on the T-52 traffic during WW II, has written a credible explanation showing that this was most likely Beurling's approach in his code-breaking work.

Even though the principle of the code had been cracked, it was not easy to go from there to reading the plain text in the regular traffic. The process of decoding material in a complex code by hand is extremely time-consuming. Initially it took three weeks to manually decode material produced in one day. It was obviously difficult to use the material for intelligence purposes because it was often too old when the plaintext was ready.

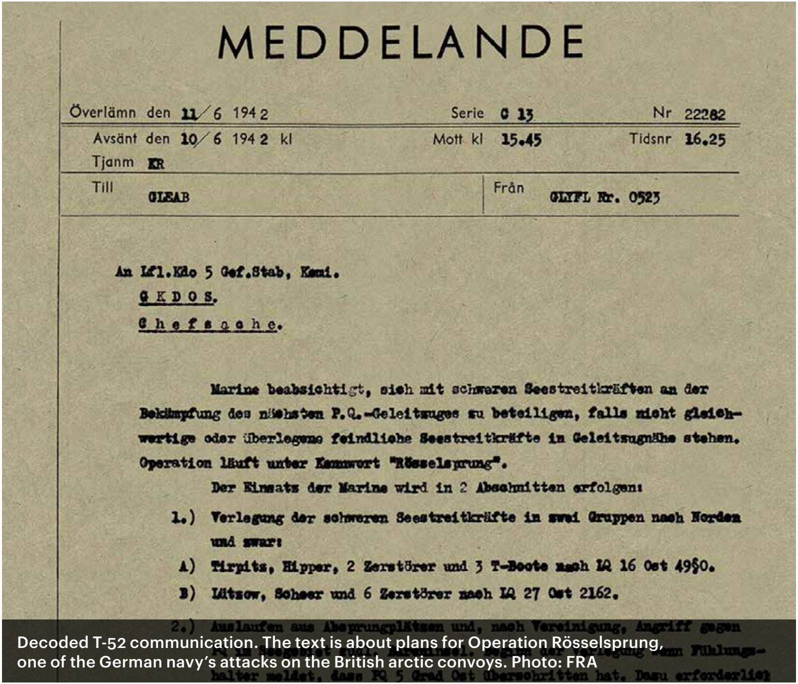
It became necessary to automate the decryption process. Working with Vigo Lindstein, an engineer from LM Ericsson, Beurling developed a device to decode the traffic mechanically, the design of which was in some ways the reverse of the T-52 design. Although at that point no one in Sweden knew what the T-52 looked like, Beurling had worked out how it functioned from a purely mathematical perspective. The decoding devices were manufactured under great secrecy by the Swedish Cash Register Company (Svenska Kassaregisteraktiebolaget), a subsidiary of LM Ericsson.

Using these devices, it was possible to start almost real-time intelligence production from the German traffic from autumn 1940. The devices were not fully automatic; someone had to type the ciphertext into a teleprinter connected to the device, after which the plain text was printed out onto paper tape. Since at that time typing was a typically female skill, this task was carried out by young female employees. When work with the T-52 was at its high point at FRA – at the end of 1942 and the beginning of 1943 – there were around 175 persons working on this traffic, which was almost half of FRA's workforce at the time.

With the decryption devices it was possible to produce timely intelligence that gave the Swedish government information on an ongoing basis about Germany's plans and intentions, not only concerning Sweden and Scandinavia, but also about the course of the war in general. A few examples were intelligence on Operation Barbarossa, the German invasion of the Soviet Union, which Sweden was aware of a few weeks before it took place by deciphering T-52 traffic. Other examples included important information concerning various negotiations with Germany. The German Embassy reported back to Germany on meetings between German diplomats and Swedish representatives. By reading the telegrams that were sent, Sweden was able to glean what the Germans thought about Sweden and how the conversations were perceived.

By 1943 the Germans realised that Sweden was able to read the T-52 traffic, possibly tipped off by their ally Finland. This led to Germany introducing newer models of the T-52 with improved encryption. By the end of 1943, FRA was no longer able to decode the newest model. By then, however, Germany was on the defensive and the threat of a German invasion of Sweden was not as imminent. The information obtained from the T-52 traffic was undoubtedly Sweden's most vital source of intelligence in the years that were the most perilous for Sweden during WW II.

From 1942 Beurling's work at the Defence Staff/FRA was terminated and he returned to Uppsala University's mathematics department to continue his work there. After that he would only be called in from time to time to solve cryptology problems. Beurling himself referred to the new commander of the FRA and what he described as a "small-town intrigue". The reason for his departure is not entirely clear, but in 1942 the Defence Staff's Crypto Department became the National Defence Radio Establishment (FRA), an independent government agency, with Torgil Thorén as the new commander. Beurling had some difficult sides to his personality; he often had disputes with people, and he had a problem with authority and complying with what he considered to be "stupid"



MEDDELANDE

Överlämn den 11/6 1942 Serie C 13 Nr 22282

Avsänt den 10/6 1942 kl Mott kl 15.45 Tidsnr 16.25

Tjanm KR

Till GLEAB Från GLYFL Nr. 0523

An Lfl.Kdo 5 Gef.Stab, Kemi.

GKDOS.

Chefsache.

Marine beabsichtigt, sich mit schweren Seestreitkräften an der Bekämpfung des nächsten P.Q.-Geleitzuges zu beteiligen, falls nicht gleichwertige oder überlegene feindliche Seestreitkräfte in Geleitzugnähe stehen. Operation läuft unter Kennwort "Rösselsprung".

Der Einsatz der Marine wird in 2 Abschnitten erfolgen:

1.) Verlegung der schweren Seestreitkräfte in zwei Gruppen nach Norden und zwar:

A) Tirpitz, Hipper, 2 Zerstörer und 3 T-Boote nach LQ 16 Ost 49§0.

B) Lützow, Scheer und 6 Zerstörer nach LQ 27 Ost 2162.

2.) Auslaufen aus Absprungplätzen und, nach Vereinigung, Angriff gegen PQ im Seegebiet südl. Bäreninsel. Beginn der Verlegung wenn Fühlungshalter meldet, dass PQ 5 Grad Ost überschritten hat. Dazu erforderlich

Decoded T-52 communication. The text is about plans for Operation Rösselsprung, one of the German navy’s attacks on the British arctic convoys. Photo: FRA decisions. An intelligence organisation does not dismiss its most gifted employee in the middle of a war without good reason, and we can only assume that once the pioneering spirit dissipated and the organisation became more established, Beurling's obvious genius and achievements could no longer outweigh his difficult traits. It is also important to remember that, during his tenure at the Defence Staff Crypto Department, Beurling was newly divorced and in the midst of an infected legal procedure about custody of the children, which must surely have affected him.

Beurling and mathematics

Beurling's work in the field of mathematics focused primarily on three areas of mathematical analysis: the theory of analytic functions, harmonic analysis and potential theory. In Beurling's thesis from 1933 he introduces the concept of extremum, which would come to play a key role in the theory of functions and potential theory.

His lectures were described as awe-inspiring, clear and elegant. Lennart Carleson, a mathematician who studied under Beurling in 1945–46 and later became professor of mathematics at the Royal Institute of Technology (KTH) and Uppsala University, described him as "an impressive figure; powerful and charismatic and an extraordinary teacher".

Beurling served as a guest professor at Harvard University, USA from 1948 to 1949. He subsequently returned to Uppsala, but in 1952 moved permanently to the USA and in 1954 took up a professorship at the Institute for Advanced Study at Princeton University. At that time Princeton was a place where mathematicians from all around the world gathered. His lectures were also acclaimed and praised at Princeton. The mathematicians Beurling worked with included Paul Malliavin from France and Finnish mathematician Lars Ahlfors, who was a friend of Beurling from the past. The work published jointly by Beurling and Ahlfors includes papers on extremal methods in geometric function theory.

The Swedish mathematics tradition had been focused on analysis. This was also the case in Beurling's work. But in the 1950s mathematics became more focused on abstraction. In the USA in particular, classic analysis was no longer as popular. This was probably one of the reasons why, according to some of his colleagues, Beurling never really received the recognition that his genius and scientific achievements deserved.

Lennart Carleson writes the following: "His relationship with his findings and his colleagues was also complicated. As I have said before, he was extremely generous with his ideas, but only on his own terms. These terms included him retaining a kind of ownership of his results and ensuring that they were never misused. He did not allow any unfinished work to be used. … This relationship he had with his work was also a source of serious conflict, even with close friends and colleagues, when he considered they were not following the rules, and this was one of the tragedies of his life."

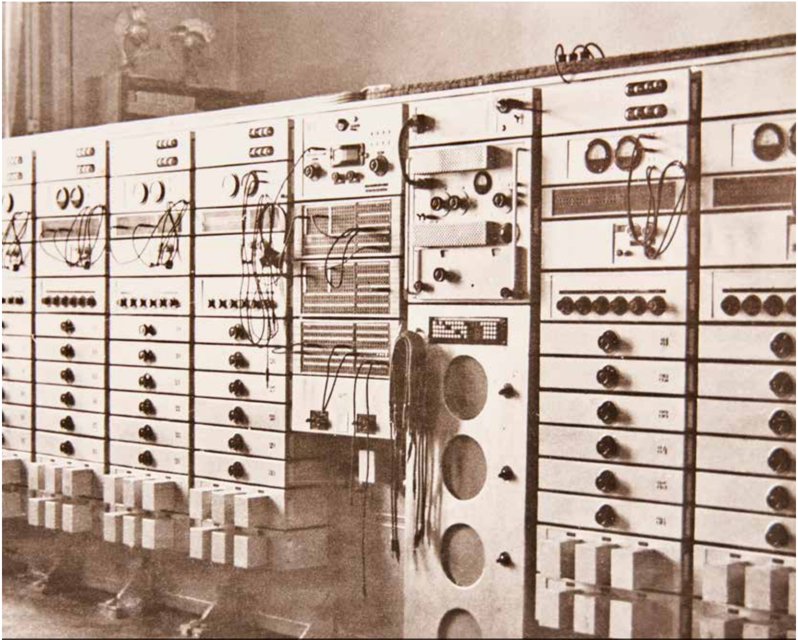
Beurling was particular about achieving perfection and did not publish his results before all of the details were fully ready. This meant that much of his work was never published. His colleagues Lars Ahlfors and Lennart Carleson write the following in an article remembering him in Acta Mathematica: "Arne Beurling was a highly creative mathematician whose work will influence mathematics for many years to come, perhaps for generations."

Conclusion

Arne Beurling made important contributions to the field of mathematics, but his name came to be mainly associated with his achievements in cryptology during World War II, and above all breaking the code of the Siemens & Halske T-52 "Geheimschreiber". The significance of his achievements was that with only limited means he managed to break the code of a foreign cipher device without knowing what it looked like or how it worked, and that he achieved this at a time when it was of the greatest importance for Sweden.

Beurling himself is alleged to have been a little irritated that he spent his life working in mathematics but became famous for something he accomplished in just two weeks, and which was beyond the realm of his real work. But Beurling's achievement in breaking the code of the German cipher device was of great significance for Sweden and for the development FRA's cryptology department.

When Beurling was doing his work, Europe was at war and Sweden needed intelligence to inform it's foreign and security policy. Eighty years have passed without another war in Europe, but at the time of writing, we are once again seeing an aggressive great power starting a war in Europe. Intelligence from the world around us is more important than ever, and those following in Beurling's footsteps at FRA continue their work in his spirit – for Sweden's security and integrity.



Reception of Geheimschreiber traffic at Karlaplan 4. Photo: FRA

Sources

Svenska Kryptobedrifter: Bengt Beckman
Arne Beurling som matematiker:
Lennart Carleson, FRA's archives
Carl Gösta Borelius minnen, FRA's archives.
Also available on FRA's website.
Jubileumsskrift Arne Beurling 100 år,
Department of Mathematics, Uppsala University
Acta Mathematica, Arne Beurling in memoriam:
Lars Ahlfors and Lennart Carleson
Kärlekens kod och krigets: Lasse Eriksson
and Kristina Östberg Eriksson

The Royal Swedish Academy of Engineering Sciences (IVA) is an independent, learned society that promotes the engineering and economic sciences and the development of industry for the benefit of Swedish society. In cooperation with the business and academic communities, the Academy initiates and proposes measures designed to strengthen Sweden's industrial skills base and competitiveness. For further information, please visit IVA's website at www.iva.se.

Published by the Royal Swedish Academy of Engineering Sciences (IVA),
Professor Pontus Johnson and Fredrik Wallin, Historian, FRA,
Swedish National Defence Radio Establishment

IVA, P.O. Box 5073, SE-102 42 Stockholm, Sweden
Phone: +46 8 791 29 00
E-mail: info@iva.se
Website: www.iva.se

IVA-M 538 • ISSN 1102-8254 • ISBN 978-91-89181-33-5
Editor: Johanna Theander, IVA
Translation: Diane Högsta
Layout and production: Pelle Isaksson, IVA
Printed by EO Grafiska, Stockholm, Sweden, 2022

IVA

Royal Swedish Academy of
Engineering Sciences

IVA-M 538 • ISSN 1102-8254 • ISBN 978-91-89181-33-5