Breaking the German Geheimschreiber during WW2

On the morning of April 9, 1940, the Swedish people and government, including the signal intelligence branch, were stunned by the news that the nazi-German Wehrmacht had launched a successful lightning attack on the Swedens Nordic neighbours. Thanks to one of the greatest cryptographic feats ever, the Swedes were never to be surprised again by the Germans during WW2. To an inadequately armed country largely sour-rounded by German armed forces, the ability to tap and crack the high-level German Geheimschreiber-communications was of princeless value to the Swedish government. On the morning after the attack on Denmark and Norway the German Minister in Stockholm called on the Ministry of Foreign Affairs. He requested permission for Germany to use the Swedish West Coast cable for communications between Berlin and Oslo. The Swedish answer came after some delay, but was affirmative. In order to hide the fact that Sweden intended to tap the cable some objections were stated. From April 14 the Germans used the cable throughout the rest of the war.

Just a few days later, Swedish technicians found that the German signals on the cable were tone telegraphy used for 5-channel teleprinter traffic. After modifying the Swedish receiving equipment, it was possible to record the signals using Creed teleprinters. The text was printed on paper tapes. The German operators wrote in plaintext about "the Geheimschreiber" which would soon be in use. And soon it was. By the end of April a new type of traffic appeared. Obviously this was a teleprinter with simultaneous encryption. Two Geheimschreiber could talk to each other in dialogue and the operators could change from plaintext to ciphertext whenever they wanted. The change was marked by five two-digit numbers followed by the word "umum" (umschalten) from the sending party, and "veve" (verstanden) from the receiving party.

The teleprinter alphabet consists of 32 five-bit combinations, and in order to record all combinations the Swedish receiving teleprinters were adjusted to print the 26 letters of the international alphabet plus 6 digits (1-6) representing the non-printing functions (carriage return, line feed, letter shift, figure shift, space and a nul function).

On May 21 a group consisting of technicians to handle the receiving equipment, as well as five ladies to paste up tapes, was established in a squalid building at Karlaplan 4, in the otherwise elegant eastern part of Stockholm. The flow of message was intercepted and duly printed, some of them in plaintext and others in a strange type of cipher.

But who could analyse and solve this type of cipher, which was totally new to Sweden? The problem was entrusted to Swedens most eminent cryptanalyst, Arne Beurling, Professor of Mathematics in Uppsala, at that time on voluntary military service. And - much to everybodys surprise - after only a few weeks Beurling could present fragments of plaintext. Studying the tapes, Beurling realised that the operators often made the mistake of sending several message using the same key, and he combined this with analysis of how the characteristics in the teleprinter alphabet matched those in the enciphered texts. By the middle of June he could present a mathematical model for the principles of the secret Geheimschreiber.

Beurling did not realise it, but he had cracked a teleprinter cipher constructed by the firm Siemens & Halske during the thirties and kept top secret by the German counter- intelligence. The authentic name of possible key configurations. It had ten wheels with number of positions - relatively prime - between 47 and 73 (a) and the number of steps until a given wheel setting reappeared was 893 622 318 929 520 950 (cf the 17 576 of the Enigma). Each wheel had a cam and the cam profiles represented pseudo-random binary digits (b), repeated when the wheel had completed a revolution. The wheels were connected with the rest of the machine by ten cables (c) which could be placed in 10! or 3 628 800 diffrent ways. Five bits derived from five of the wheels changed the input letter (d) by a binary addition (e). A permutation of the resulting bits was performed by five relays controlled by five bits derived from the remaining wheels (f). The relays could be placed in 719 diffrent ways(2 609 107 200 including the cable connections). From April 1, 1942, only one connecting scheme (Fig 1) was used. For every character each wheel moved one step.

During the summer of 1940 the message were deciphered manually. That was tedious work and the traffic increased all the time. Clearly a special machine would have to be built which could decipher in the same manner as the Geheimschreiber. A graduate engineer, Vigo Lindstein, was assigned to build such a devise called an "app", (appartatus) according to Beurling´s directions. Eventually more than 30 "apps" were built by the Ericsson Corporation.

Before deciphering with the "app", some basic cryptological work had to be done. Each day the Germans used a new key setting for five of the ten wheels, and these com-binations must be solved by the Swedish cryptanalysts every morning. The remaning wheels were initiallt given by a message key chosen by the operator and sent in plain.

More and more people were recruited to work on the German G-Schreiber traffic. They worked around the clock and the flow of material kept increasing. The German Legation in Stockholm also used the machine, and from midsummer 1942 the German communi-cations to FInland were also picked up. The cryptological succsess reached its peak in November 1942. During that month more than 10 500 message were delivered to the Defence Staff and the Ministry of Foreign Affairs. However, the Germans eventually learned about the Swedish ability to read their top secret messages - it is assumed that this was through their Finnish allies. Gradually the cryptology in the machines was strengthened.

The A/B model became C, then CA, then D, then E and the routines be-came extremely disciplined. In the beginning of 1944 the traffic was no longer readable. By then 300 000 message had been solved and delivered to eager Swedish readers.

A second type of Geheimschreiber manufactured by Standard Elektrik Lorenz was also solved by the Swedish cryptoanalysts starting 1943. It was the SZ40/SZ42 (SZ=Schlüsselzuzats, another name is GZ=Geheimzuzats): This equipment was always used together with a Lorenz teleprinter and the message were sent by cable as well as by radio.

Of course, the information extracted from the Geheimschreiber-trafic was of priceless value to the Swedish Government and the Defence Staff. Largely surrounded by German armed forces in the neighbouring countries. The German HeadquarterÕs summary also gave situation reports of the war on other fronts. Also, reports to and from the German Legation made it possible to follow German reactions to various Swedish foreign policy iniatives.

At the time Sweden had advance knowledge of the most secret German plans. One example was Oparation Barbarossa (the attack on the Soviet Union in 1941). The troop movements were reported in the messages and one message talked about the double pay which the soldiers would receive after entering Russia. In negotiations the delegates had got from Berlin.

The decrypts were also of very high value for Swedish counter-intelligence. Sweden had a good insight into affairs of "Abwehr" - the German intelligence service - thanks to the G-Schreibertraffic. Thus, the security police was able to closely watch and act against German agents in Sweden.

During the war in Sweden was a such frequented area for the secret service of the belligerent countries and the Germans diligently gathered and reported information to Berlin on condisions in the enemy countries as well as Sweden.

The Swedes never broke the Enigma machine. This was deemed impossible without accsess to an authentic machine, and from Swedish point of view it was much more significant to be able to solve the G-schreiber. The G-schreiber was used for stragetic communications between the highest authorities in Berlin and its subordinate military headquarters and thereby of immense value to a surrounded Sweden. The Enigma on the other hand was used at all echelons from the high commands to front-line tactical units, and gave intelligence of the greatest value to the allies on operational and tactical levels.

Finally - how should Beurling´s achievment be valued ? It should be borne in mind that Beurling had no information about the Geheimschreiber, knew nothing about teleprinter ciphers and not even about teleprinters. Yes he succeeded in reconstructing the most advanced German cipher machine, using only intercepted material. That was indeed a brilliant feat. The mathematician Arne Beurling was widely regarded as a genius. When visiting FRA in 1976 he was asked what had led himto the solution.. "A wizard does not tell his tricks", came the laconic reply. His is the outstanding name among Swedish cryptoanalysts. Born in 1905 in Gothenburg, he became Professor of Mathematics in Uppsala in 1937. He was a charismatic and sometimes difficult person and a legendary teacher who made a deep impression on his students. During the 30´s , 40´s and 50´s he was a leading international figure in Mathematical Analysis. In 1948 he became visiting professor at Harvard, and in 1952 he was given a prominent position at the Princewton Institute for Advanced Study, where he stayed until his death in 1986.

Publicerat 2003-06-05.