(U) CRYPTOLOGIC ALMANAC

(U) The Breaking of *Geheimschreiber*

(U) Along with breaking the Japanese diplomatic cryptosystem, usually referred to as "PURPLE," probably the greatest example of Allied cryptanalytic success in World War II was the breaking of the German Enigma machine. This cryptodevice was used by all of the German armed forces as the primary cryptosystem for all units below Army level or the equivalent. As D-Day approached, however, other German cryptodevices assumed greater importance. Under the general name of *Geheimschreiber* (Secret writer), the Germans used two devices for enciphering high-level (Army level and above) radioprinter communications. These were the "T typ 52," built by Siemens & Halske, and the "SZ-40/SZ-42," built by Standard Elektrik Lorenz. The "SZ" meant Schluesselzusatz (key attachment), so-called because the essential encryption mechanism was in a box that could be detached from the radioprinter machine.

(U) On the morning of 9 April 1940, the German army attacked both Norway and Denmark and quickly defeated them. The next day, the German minister in Stockholm, Sweden, 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, Norway. After some delay, the Swedes agreed. Some objections were stated, however, in order to hide the fact that Sweden intended to tap the cable. The Germans used this cable from 14 April to the end of the war.

(U) Swedish technicians quickly found that the Germans were using five-channel teleprinter on the cable. The German operators wrote in plaintext about "the *Geheimschreiber*" which would soon be in use. By the end of April a new type of traffic appeared, teleprinter with simultaneous encryption. On 21 May a Swedish group consisting of technicians to handle the receiving equipment, as well as five ladies to paste up tapes, was established in a squalid building in an otherwise elegant eastern part of Stockholm. The flow of messages was intercepted and duly printed, some of them in plaintext and others in the new cipher.

(U) The problem of breaking this traffic was entrusted to Sweden's most eminent cryptanalyst, Arne Beurling, professor of mathematics in Uppsala, at that time on voluntary military service. And - much to everybody's surprise - after only a few weeks Beurling could present fragments of plaintext. Studying the tapes, Beurling realized that the operators often made the mistake of sending several messages 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 *Geheimschreiber*. Beurling did not realize it, but he had cracked a teleprinter cipher constructed by the Siemens & Halske Company during the thirties and kept top secret by German counterintelligence. The authentic name of the machine was "T typ 52 A/B." It had an incredible number of possible key configurations. It had ten wheels with between forty-seven and seventy-three positions per wheel, all relatively prime. The number of steps until a given wheel setting reappeared was 893,622,318,929,520,950 (or 8.9x10^{17}) versus the 17,576 of the Enigma. Each wheel had a cam, and the cam profiles represented pseudorandom binary digits repeated when the wheel had completed a revolution. The wheels were connected with the rest of the machine by ten cables which could be placed in 10! or 3.6x10^{6} different ways. Five bits derived from five of the wheels changed the input letter by binary addition. A permutation of the resulting bits was performed by five relays controlled by five bits derived from the remaining wheels. The relays could be placed in 10! different ways (3.6x10^{9} including the cable connections). From 1 April 1942, only one connecting scheme was used. For every character each wheel moved one step.

(U) During the summer of 1940 the messages were deciphered manually. That was tedious work, and the volume of 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 machine according to Beurling's directions. Eventually more than thirty of these machines were built by the Ericsson Corporation.

(U) Before submitting the material to the machine, 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 combinations had to be solved by the Swedish cryptanalysts every morning. The remaining wheels were initially given by a message key chosen by the operator and sent in the clear.

(U) More and more people were recruited to work on the German *Geheimschreiber* 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 1941 the German communications to Finland were also picked up. The cryptological success reached its peak in November 1942. During that month more than 10,500 messages were delivered to the Swedish Defence Staff and the Ministry of Foreign Affairs. However, the Germans eventually learned about the Swedish ability to read their top-secret messages presumably through mutual allies. Gradually the cryptology in the machines was strengthened. The A/B model became C, then CA, then D, then E, and the routines became extremely disciplined. In the beginning of 1944 the traffic was no longer readable. By then 300,000 messages had been solved and delivered to eager Swedish readers.

(U) A second type of *Geheimschreiber* manufactured by Standard Elektrik Lorenz was also solved by the Swedish cryptanalysts starting in 1943. It was the SZ40 / SZ42 (SZ=Schluesselzusatz, or key attachment). This equipment was always used together with a Lorenz teleprinter, and the messages were sent by cable as well as by radio.

(U) Of course, the information extracted from the *Geheimschreiber* traffic was of priceless value to the Swedish government and the Defence Staff. Largely surrounded by German armed forces, the main Swedish objective was to keep the country out of the war. Through its secret source, Sweden got detailed and reliable information about the deployment and size of the German forces in the neighboring countries. The German Headquarters' summary also gave situation reports of the war on other fronts. In addition, reports to and from the German legation made it possible to follow German reactions to various

Swedish foreign policy initiatives.

(U) At the time Sweden had advance knowledge of the most secret German plans. One example was Operation 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 with the Germans, it was of great value to know in advance what instructions the delegates had gotten from Berlin.

(U) The decrypts were also of very high value for Swedish counterintelligence. Sweden had a good insight into the affairs of the *Abwehr* - the German intelligence service - thanks to the *Geheimschreiber* traffic. Thus, the security police were able to closely watch and act against German agents in Sweden. During the war Stockholm, as the capital of a neutral country, teemed with agents of the secret services of the belligerent countries, and the Germans diligently gathered and reported information to Berlin on conditions in the enemy countries as well as in Sweden.

(U) It should be borne in mind that Beurling had no information about the *Geheimschreiber*, knew nothing about teleprinter ciphers and not even about teleprinters. Yet he succeeded in reconstructing the most advanced German cipher machine, using only intercepted material. As a mathematician, Arne Beurling was widely regarded as a genius. Born in 1905 in Gothenburg, he became professor of mathematics in Uppsala in 1937. During the1930s, '40s and '50s, he was a leading international figure in mathematical analysis. In 1948 he became visiting professor at Harvard, and in 1952 he was given a position at the Princeton Institute for Advanced Study, where he stayed until his death in 1986.

NOTE: (U) The above information comes from the brochures "A Swedish Success: Breaking the German *Geheimschreiber* during WW2 (U)" Foersvarets Radioanstalt, Stockholm, Sweden: 1997; and "German Cipher Machines of World War II (FOUO)," soon to be published by the Center for Cryptologic History.

[(U//~~FOUO~~) David P. Mowry, Center for Cryptologic History, 972-2893s, dpmowry@nsa]