Spy Radio and the encryption methods used by the MfS
(Ministerium für Staatssicherheit of the former German Democratic Republic, “Stasi”)

Detlev Vreisleben

Part 1

Many readers interested in the field of radio will already have heard voices on shortwave announcing groups of numbers in German, English or other languages. That’s what I have already heard as a child twiddling the knobs of the radio set. Back then I found it very mysterious but could not explain its context. There are still many rumours around this procedure. Meanwhile I have a Speech-Morse Generator in my collection which has announced those numbers for the HV A (Hauptverwaltung Aufklärung, foreign espionage department of the MfS).

Agents received encrypted information and tasks in the shortwave radio range. This was also done by secret services of other states, as shown e.g. in the instructions “Zum Empfang unserer Funkmitteilungen” (About the Reception of our Radio Messages) found by the MfS at agents of the BND (Bundesnachrichtendienst, secret service of the Federal Republic of Germany).

Until the end of 1958 the MfS used a Soviet encryption method.[3]

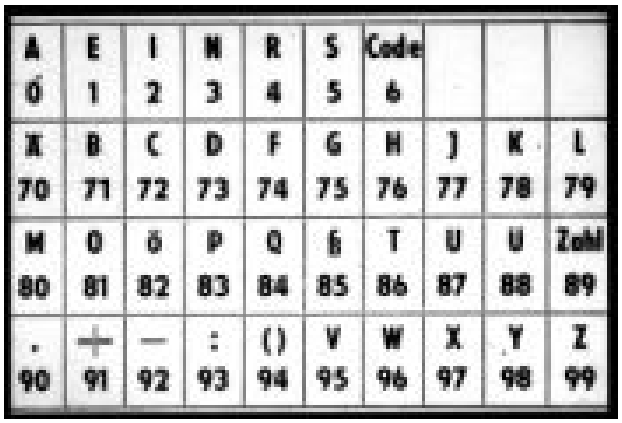
Each agent received a mnemonic verse, e.g. "Welken muß die Blüte in der Zeiten Flucht, aber im Gemüte bleibt die reife Frucht" and several agents a common mnemonic word. The text was encrypted and decrypted by means of both mnemonic verse and word.[1]
According to Wagner/the same source, the employment of American supercomputers enabled the Bundesamt für Verfassungsschutz already in 1961 to break the method, determine the mnemonic phrases and hence decrypt MfS radio messages.

The spy Günter Guillaume was allegedly uncovered by decryption of old radio messages with congratulations to his birthday and to the birth of his son.[2]

Illustration 01 Sealed encryption booklet for the central office with OTPs

Illustration 02 OTPs from the encryption booklet in the central office

From 1959 on the MfS used the secure block cipher method. A computer generates random numbers by means of a noise generator which were printed twice: in a postcard format (illustration 1 and 2) and as a small 2.7 cm wide paper strip for the agent.
These numbers were used only once, hence the name “One Time Pad (OTP).” See http://scz.bplaced.net/index.html



A Ó	E 1	I 2	N 3	R 4	S 5	Code 6			
X 70	B 71	C 72	D 73	F 74	G 75	H 76	J 77	K 78	L 79
M 80	O 81	Ö 82	P 83	Q 84	ß 85	T 86	U 87	Ü 88	Zahl 89
. 90	+ 91	— 92	: 93	() 94	V 95	W 96	X 97	Y 98	Z 99

Illustration 03 Block cipher conversion table of the HV A

Each agent also received a small conversion table (illustration 3) and the individual numbers keys in the shape of a wafer-thin paper strip, folded many times, for encryption and decryption. The strip for encryption can be recognized by a wider gap between the 2nd and 3rd column and was stored in a yellow cover (illustration 4).

The agent’s case officer encrypted his messages in the central office. At first the text was converted into numbers by means of the block cipher conversion table, then the numbers from the encryption booklet were added without carry. To obtain complete groups of five numbers, the message was filled with periods (“90”). The resulting five-number groups were then transmitted to the “Objekt Kesselberg” (at Wernsdorf near Berlin) over a secured teletype connection. In the fifties and sixties of the last century the numbers have been recorded to tape in a recording studio and played back at transmission time. Near the studios was a training area of the NVA (Nationale Volksarmee, the army of the GDR) from where disturbing noise entered into the studio in spite of acoustic insulation.

From around 1965 on, a talking machine dubbed "Schnatterinchen“ (diminutive noun from "to chatter“) was used, constructed from stripes of magnetic tape, recorded with the numbers and announcements, which were attached to a cylinder and played back in the required sequence by a control logic. Back then the numbers were recorded only in German language in a studio in the Funkobjekt Kesselberg, later also in Spanish language in a studio of the DDR radio broadcasting station in Berlin, Nalepastrasse.

[1] Wagner, Klaus: Spionageprozesse. 2000. ISBN 3-930732-58-0

[2] Günter Guillaume: In April 1974 the West German public prosecutor announced the arrest of a staff member of Chancellor Willy Brandt on suspicion of espionage for the GDR. Günter Guillaume came to the FRG as alleged refugee from the GDR in 1956. In fact he was an OibE (Offizier im besonderen Einsatz, Officer on special mission)of the MfS. He worked for intelligence chiefly in the SPD (Social Democratic Party in the FRG). He entered the chancellor’s office in 1970 and was as a close aide responsible for the party related appointments for the chancellor and the correspondence with party divisions and members. In May 1974 Brandt took the responsibility for negligence in the context of the Guillaume affair and stepped back.

[3] Wolf, Markus: Spionagechef im geheimen Krieg. 1999. ISBN 3-612-26482-6

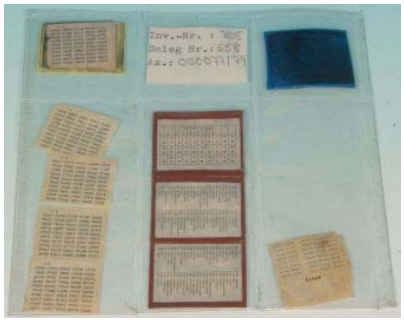


Illustration 04 Encryption documents for an agent consisting of block cipher conversion table, table of code words, encryption- and decryption-stripes

Illustration 5 shows the announcer of that voice heard by so many. In the beginning of the eighties, programmable microprocessor-controlled (Z80) Speech-Morse generators were developed, see illustration 6.
Illustration 7 shows a block circuit diagram of the machine

There were many reasons for the development of these devices: work relief of the announcers, rationalization of the process of radio operation and replacement of western technology from Hell company for the A1- (unmodulated carrier telegraphy) and A2- (modulated carrier telegraphy) operations. Further they strived for a better voice sound quality than that of the synthetic speech used by the BND.

Illustration 05 Face of the announcer

These newly developed Speech-Morse generators announced with a female voice for receivers in the European area, and Morse code for receivers outside Europe; hence the name Speech-Morse generator. They could be programmed by keyboard, by tape reader or via a computer interface. The numbers which had formerly been recorded to tape have been digitized (pulse code modulation with 8 bit resolution and a 8 kHz sample rate) and stored to EPROMs. Besides the German recording we presently know a recording in Spanish for the Cuban secret service.

Illustration 06 Speech-Morse generator for the modulation of a SW transmitter. It can be programmed via keyboard, punched tape or computer interface.
It is labeled in English since it was delivered to several “Bruderorgane” (brother states’ agencies).

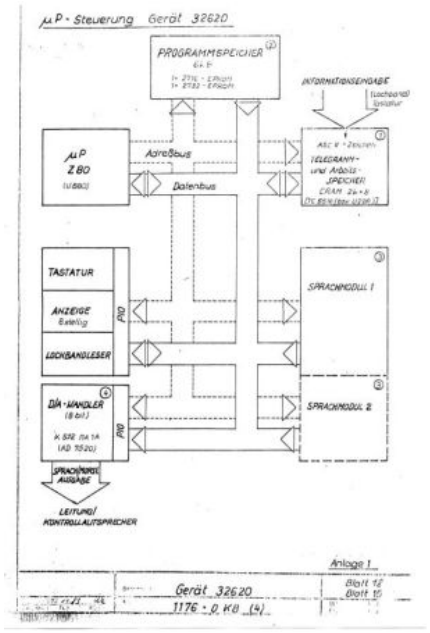


Illustration 07 Block circuit diagram

The data transfer from the central office to the Objekt Kesselberg for intermediate storage was via teletype in the beginning, later in the eighties over a secured data line. The punched tapes were produced in the Objekt Kesselberg and checked there before the transmission.

We continue with Part 2 of this splendid article in Newsletter Issue 61

Spy Radio and the encryption methods used by the MfS
(Ministerium für Staatssicherheit of the former German Democratic Republic, “Stasi”)

Detlev Vreisleben

Part 2

Illustration 08 A map showing Wernsdorf and Zeesen southeast of Berlin, Berlin-Lichtenrade in the upper left corner

The first transmitter site in the fifties was in Berlin-Schöneiche in Kurze-Strasse 11. Later, the transmissions came from the transmitter site (Sendestelle) Zeesen southeast of Berlin (illustration 8). There were transmitters with 1, 5 and 20 kW made by the Funkwerk Köpenick and transmitters with 5 and 25 kW from the Soviet Union (illustration 9). A part of the antenna installation can be seen in illustration 10.

<<< **Illustration 09** West side of the transmitter hall of the Funkstelle Zeesen

Illustration 10 Part of the antenna installation of Funkstelle Zeesen >>>

The Sendestelle Zeesen is described in detail in the book "100 Jahre Funktechnik in Deutschland Band 1 - Funksendestellen rund um Berlin," by Gerd Klawitter (editor).

Intermediate signals, sequences of tones or station identifiers preceded the transmissions to enable the agent to tune in the correct station. The agent received the numbers groups intended for him on the guidance channel („Führungsweg“, „Welle 1“) with a shortwave receiver, wrote the five-number groups of the decryption strip below the received groups and subtracted the decryption numbers without carry. The result was translated into plaintext using the conversion table.
There was a table with 100 code words to allow for the transmission of common terms by only three figures. In course of time, the conversion tables were updated three times and extended with new code words. Illustration 11 shows an example of a decryption. The plaintext is: „Erwarte Nachricht über TBK Peter“ (expect message via TBK Peter). TBK stands for „Toter Briefkasten“, dead drop for handing over material without personal contact.

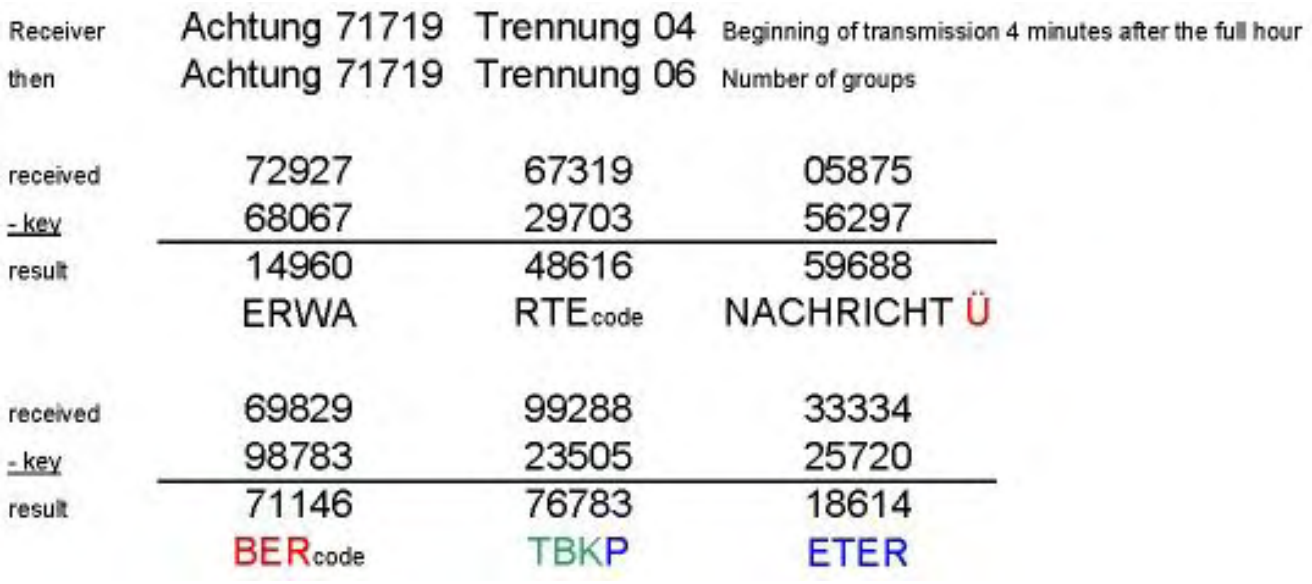


Illustration 11 A decryption example
[See Illustration 3]

The “used” groups of numbers were cut off as complete rows and destroyed. The first group of the (now) first line was the new agent’s number. This method had the advantage that the opposite side was not able to establish statistical data on which agent received how many messages (countermeasure against traffic analysis). Frequencies and transmission times could also not be assigned to a particular agent’s number.

The HV A dubbed the shortwave transmission methods „Welle 1 (Führungsweg)“ and „Welle 2 (Meldeweg)[3].”

The transmissions for Europe were made in voice (A3 = amplitude modulation without carrier suppression, as a normal broadcasting station, hence audible with normal SW receivers) and in telegraphy for countries outside Europe.

On „Welle 1“ the agent’s number and the time shift to the beginning of the messages were announced, e.g. 71719 Trennung 04 means that the message for agent number 71719 would start 4 minutes after the full hour.

At the beginning of the message the agent’s number and the number of groups were announced, e.g. 71719 Trennung 06 means that six groups of five numbers were to follow.

Usually the agent transferred his information via mail, dead drop, courier or phone. In times of crisis, if this would not have been feasible, he would have had to get his buried SW transmitter and transmit directly.
With the „Welle 2“ method the agent transferred the five-number groups with a SW transmitter with a burst encoder(punched tape, tape recording or electronic device). He could also transfer messages via phone with an acoustic coupler from a public telephone. Later, modified commercial DTMF dialers were used. Of course he could also transfer via VHF („Horizont“) or invisible ink (GSM, Geheimschreibmittel).

Since the block cipher method (OTP) is secure, it is still in use until today.

[3]Ordnung Nr. HV A 1/86 für die Arbeit mit operativ-technischen Mitteln - OTM-Ordnung

We continue with Part 3 of this splendid article in Newsletter Issue 62

Spy Radio and the encryption methods used by the MfS
(Ministerium für Staatssicherheit of the former German Democratic Republic, "Stasi")
Detlev Vreisleben
Part 3

Finally, some remarks on the technology.

Illustration 12 SW receiver for agents, with low spurious radiation

Commercial SW receivers made by Sony, Grundig etc. were used. There was also a special receiver with low spurious radiation (illustration 12) for areas in which commercial receivers were not available.

Illustration 13 Old SW transmitter with burst encoder (scanning of a punched tape)

Illustration 14 SW transmitter SE 25 with burst encoder (playing a pre-recorded audio tape)

The first transmitters (illustration 13) were equipped with vacuum tubes, beyond them the SE 25 (cover name „Ems/Elbe“, illustration 14) which resembles the SP15 of the BND amazingly (illustration 15). Later, the agents were given the transistor–based WSA-1 (Weitverkehrs-Sende-Anlage, long range transmitter) (illustration 16).

Illustration 15 SE 25 (HV A) on the left side of a SP 15 (BND), SE 25 (HV A) on the right

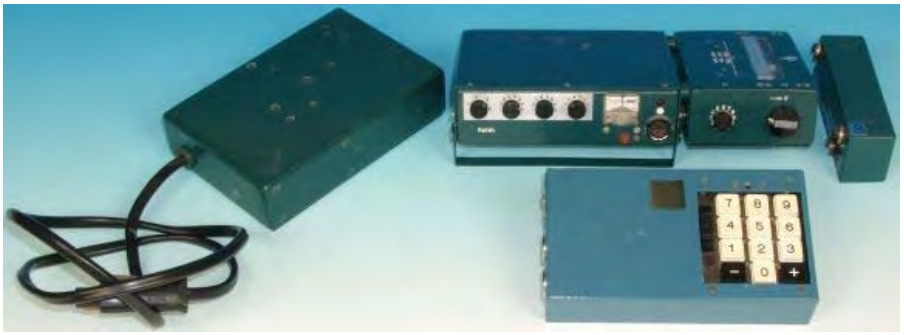


Illustration 16 WSA 1 with power supply unit, antenna matcher and electronic fast coding device

Illustration 17 WSA 6 compact version with burst encoder

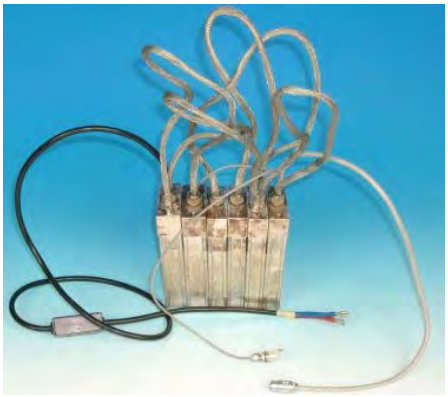


Illustration 18 WSA 6 module version for covert installation eg in a car

In 1988 the WSA 6 was completed but it probably did not come into use. This is a device for a frequency range of 4 to 18 MHz with 20 W transmission power which used for the first time no longer morse code but a 5-bit constant weight code. The transmission mode is FSK with +/- 300 Hz and 900 Bd. This means that with this Frequency Shift Keying mode (FSK) the transmission frequency is being shifted by + or – 300 Hz 900 times per second. Bd (Baud) is the unit for the transmission step speed; 1 bd is 1 step/second, hence 900 Bd 900 steps per second. This device existed in a compact version (illustration 17) and a module version (illustration 18), to install it covertly.

To minimize the risk of discovering the transmitters, burst encoders were used. Firstly an audio tape was punched with the information to be transmitted and then read mechanically; later an audio tape loop was used as well as electronic keyers or programmable calculators with a serial interface.

Dipole and rod antennas were used as well as an “umbrella antenna” as seen in **Illustration 19** [Left] installed in a hotel room and, in part in **Illustration 20** [Above] were provided for the use in hotel rooms and also a “ground antenna”.

There was another transmission mode described in the „OTM-Ordnung“. It is the „Horizont“ method which allows sending from a private car or a portable container in the UHF range over a distance of up to 150 km (depending on the ground profile) to the border of the GDR. The receivers were situated e.g. on the Brocken (a mountain in the Harz highlands on GDR area) (illustration 21).

Illustration 21 High-gain reception antenna for the „Horizont“ system on the Brocken mountain, Harz highland

.**Illustration 22** TSS-2 (transmitter) right, TSE-2 (receiver) left

In the late 1980s as the technology had aged over the years it was planned to replace it with a new system TSS-2/TSE-2 (illustration 22) with the following features: frequency hopping in the 440 to 465 MHz range, channel remain time 4.5 to 28 ms, 38.4 kBd DPSK. TSS stands for „Terrestrische Sendestelle“ (terrestrial transmitter station), TSE means Terrestrische Empfangsstelle (terrestrial receiver station). With differencial phase modulation DPSK the information is carried in the difference of subsequent steps: no phase difference = 1, phase difference = 0.

A sincere thanks to Detlev and Daniel for their hard work on producing this document and sharing it with ENIGMA 2000.

Translation: Daniel E2Kde, DetlevE2Kde

Picture credits:
01 – 07, 11 – 20: Detlev Vreisleben
08: Google Maps
09, 10, 21: Eberhard Jauch

© Remains with the authors 2010