

THE KL-7 AT NATO IN WEST GERMANY

Electronics Technician's Story on OTT Mixers and the TSEC/KL-7

Mo Davies

I joined the British Army in 1963 as Electronics Technician, but we called ourselves "Cypher Mechs", because our job was actually the repair and maintenance of online and offline cypher machines. During training, we had been shown the BID/570/1 "DERBY", a UK manufactured one-time tape Mixer, but apart from its pretty light green-greyish glossy colour, the machine was identical to the black crackle finish ETCRRM that I met later, and was told that it was obsolete and we would never have to work on the DERBY.

Other machines that I recollect seeing in training were the BID/30 5-UCO, one of which exploded whilst powered down (capacitor burst) whilst one of us trainees was working inside the machine. He never went near one again. The BID/08/05 "ROCKEX" and BID/610 "ALVIS", which I later saw in use in the back of a Land Rover whilst I was at the Apprentices College, God only knows how it all got in there, along with a single operator and a T100, or how it was all operated without 240 Volt Supply. By that time, I was out of the cypher loop, and did not even know we had any BID/610's at the College.

Incidentally, the manufacturers of the BID/610, when planning early prototype machines, asked for an initial supply of a handful of diodes, to be followed by a large order later, as being ideal "because we require a specifically cheap and nasty type of noisy diode" to produce an encryption key. I paraphrase the order but "noisy" was one of the actual words used in the request, which is not regarded as a good characteristic in most diodes. The order was denied by the manufacturer of the diode, presumably due to this insult to their product. The diode finally used was the second cheapest and nastiest, but the request this time was for "a diode with particular characteristics, and your product is ideal for our purpose". I cannot now recollect either of the diode types.

After just over a year of training, I was posted to 28th (BR) Signal Regiment in Nordrhein-Westfalen, Germany. With our regiment being part of the Northern Army Group (NORTHAG), we were committed to NATO and our job was as a mobile communications centre for NATO. In that capacity, we had no connections with the British Army or with BAOR (British Army of the Rhine). I was of course "NATO Cosmic Cleared" due to the danger of my seeing "secrets".

We spent a lot of time in German forests, our equipment being housed in elderly Bedford box body wagons, which were dressed overall in camouflage nets. We suffered from blackout conditions, all the lights automatically being extinguished whenever a door was opened, to great shouts of "Shutdadoor" so all work stopped until it was closed again. However, we were using very noisy 27.5 kV/A Meadows generators that could be heard for miles in the quieter periods of night time.

The German Radio Relay wagons that we were connected to had generators that were inaudible even close up, but they did not bother with either camouflage or blackouts. The Dutch Army in their turn ran bundles of cables in plain sight down the sides of the roads to connect to the nearby telephone exchanges. Ask any child within a ten-mile radius, and they could tell you where “the Army” was!

We used the Norwegian ETCRRM and German Lorenz 554 Mixers, both being “Vernam” cypher machines. The ETCRRM and Lorenz mixers were theoretically compatible, so long as one remembered that one of them did a “read and then feed” and the other did a “feed and then read”, so the Lorenz mixer had to be offset by one character from the index marks on the one-time tapes.

When using Mixers, the sender encrypted his message by mixing the plaintext message in real-time with a truly random one-time tape (OTT). Only the receiver had an exact copy of that one-time tape, mixed in real-time with the arriving encrypted message, thus retrieving the original message. Usually, both sides used the same roll of OTT to send and receive messages and agreed upon a starting position on the OTT punched tape for each message, and later destroy (burned) the used sections of the tapes. This system was in theory unbreakable.

The Lorenz Mixers, when used in a vehicle, caused the wagon to jump up and down in time with the operators’ feet whilst setting the Mixers up, as in order to transmit without encryption, the operators had to keep pressing and releasing a foot-switch, and they always developed a rhythm and stayed “in step” with each other. At this time, the Washington-Moscow Hotline, an encrypted teletypewriter link between the United States and Russia, also used the ETCRRM machines.

However, one day, a bright Spark (i.e. signals operator) connected a recording oscilloscope to the output of an ETCRRM, and by using this modern technique, he discovered that the plain language message could be read as five-bit spikes that sat on top of the encrypted message.

After some considerable panic, the machines were modified to use “Dry keying” where the teleprinter merely switched its contact open and closed to operate an electronic relay, rather than switching a higher voltage mechanical relay. Unfortunately, our telegraph equipment consisted of a few Lorenz Lo15 teleprinters and a large number of Lorenz tape readers and tape perforators, all declared obsolete by RAF Germany, due to their age and unreliability, and scheduled for scrapping, which our Technical Officer had scrounged from them for our use. This equipment was not compatible with “Dry Keying”, as they had several irremovable filters on their transmit contacts.

This problem was only resolved when NATO finally found the funds to buy us Siemens T100 teleprinters, along with a few Siemens tape readers and printing reperforators, which we had to modify by removing the transmit contact filters as soon as we received them. Thus, we were able to begin operations again. This also made our job easier, as we did not have to queue up, to read the tapes on the only available printer in each complex, to find out what the other end was telling us. We tended to use a set of standard test tapes when setting up, and could usually recognise them by looking at the tapes. For instance, the pattern punched by RYRYRY was fairly distinctive.

One of our engineers once accidentally (?) transmitted, instead of a test tape, the first half of a set of Smutty Limericks from a copy of Playboy, which had been banned in the UK. His request "INT QRK" (Q-Code for "what is the intelligibility of my signal?") resulted in a non-standard response, which he had to read on the Lo15 teleprinter, "I will tell you after you send the rest of this tape". I still remember a few of these limericks today, 60 years later.

We were told that any messages that we transmitted online, we could expect to be common knowledge in the USSR 48 hours later. Only the volume of traffic served as protection as it took so long to go through all our transmissions. I do know that 19th Signal Regiment did the same to East German traffic, and the East German Fernmeldebataillon wished the Regiment "seasons greetings" around Christmas every year. These messages were apparently always decrypted within a few days.

After two years of this fun, which did not involve much bathing for several weeks, I was posted to the NATO Joint Headquarters (JHQ) at Rheindahlen, as one of five technicians working in the HQ Northern Army Group, 2nd Allied Tactical Air Force Communications Centre. Try saying that mouth-full when answering a phone.

At Rheindahlen, we employed ECOLEX online cypher machines, again using one-time tapes, which in one of their two modes were compatible with ETCRRM and Lorenz Mixers. These were operated 24/7 by a group of around 50 WRAC girls (Women's Royal Army Corps) on a four-way shift system. We Technicians also worked a four-way shift, covering the ComCen 24/7 with myself, as the Corporal in charge, working an 08:00 to 18:00 five-day week, and covering the shifts of any Technician who was on leave or off work sick. I was the only married Technician and commuted every day from Roermond in the Netherlands to Rheindahlen, some 35 kilometers by road.

Our Cypher Room was manned by a mix of Luftwaffe, Dutch and Belgian Army personnel, and a single British Soldier, all of whom were Senior NCO's, who encrypted higher classifications of message offline. I never did work out their shift system, as it differed from ours. We joked that they encrypted their shift roster to prevent us working it out.

The offline encrypted KL-7 messages came out of the Cypher Room in five-letter groups, printed by the KL-7 on long paper strips and then stuck onto A4 pages, which had to be transcribed into punched teleprinter tapes (Murray Coded) for onward transmission. The messages were then sent online double-encrypted (i.e. superenciphered) using the ECOLEX machine. Occasionally, the KL-7 messages arrived already transcribed into punched tapes.

One operator would read out the five-letter groups to another who typed them on a teleprinter to produce the Murray Code tape. The hardcopy and message printed tape then had to be compared by the same method, one reading out loud, the other comparing what they heard with what was in front of them. No wonder messages were sometimes delayed in transmission.

I found that the only "tools" that we technicians needed to keep the KL-7 running, was an India rubber (i.e. natural rubber or latex) and a set of half clothes-pegs. The India rubber was used to clean the contacts on the rotors, keyboards and rotor basket, the clothes-pegs were used as wedges to keep the Rotor Basket positioned firmly against the contacts in the body of the machine.

The Cypher Operators themselves periodically changed a set of four valves always as a set. They had maintenance kits, which they jealously guarded from us. Most traffic was produced on a trio of KL-7's, but a separate one with different settings was specifically used to sent traffic to the US ARTY (United States Artillery). Several spare rotor sets were used for these machines, and several days settings left on them, as sometimes receipt of messages could be delayed beyond their dates of encryption.

We were not permitted to meter out the rotors. In case of doubt, we placed the rotor onto a conductive copper board to check if each pin had continuity through to the other side, and then check for shorts between pins on a wooden tabletop. I never found any problem with the rotor wiring. However, operator errors (finger trouble) could occasionally cause a message to be unreadable. The operators would set their machines, type the message to be encrypted, and then type the encrypted message from the resulting tapes back onto the KL-7, to check that the message came out "en Claire" again, before issuing the encrypted message to be sent, superenciphered over the ECOLEX machines.

Unfortunately, our efforts were in part negated by several venal Americans who on different occasions sold KL-7 manuals, settings, rotor sets and even complete machines to the USSR. How many others were not caught, I do not know, but at least the U.S. Army Signals Warrant Officer Joseph Helmich and U.S. Navy communications specialist John Walker were detected in their treachery.

When the USSR invaded Czechoslovakia on 21 August 1968 to halt the Prague Spring uprising and suppress the reforms, senior NATO officers borrowed our illegal Broadcast receiver, so NATO strategy was ordered by what they could glean from the BBC Monitoring Service, who had reporters in Prague. It took several days before an increase in traffic through our ComCen showed that they were able to read military information instead of the civilian transmissions, and yes, we were given our "banned" radio set back shortly after this. A blind eye was turned to our use of radio receiving equipment inside a secure ComCen, which was inside a secure building, which was inside an often secure car park.

I left Germany in 1969, going to Singapore in charge of an electronic test instrument calibration workshop, then back to the UK as a Trade Instructor at the Army Apprentices College, so I had no further contact with Cypher Equipment. I ended my military service in 1975 whilst still teaching at the College.

An ex Electronics Technician once told me that in the 1970's, during his debrief after repairing a faulty Teletype 33 for them, he upset the American Security Officer at the then USAF Menwith Hill in Yorkshire, when he expressed his surprise that the KL-7 was still in use there. The Electronics Technician had recognised the distinctive noise the KL-7 made, despite being screened off from the machines as he walked past them. I believe that after that event, the faulty equipment was relocated to a separate office for visiting service engineers, although only a few security-cleared people would have recognised the machines and their function, especially sight unseen.

© 2024 Mo Davies, Sergeant Class1 Technician, UK, Ret.

Version 1.2 written for [Cipher Machines and Cryptology](#).

More information on the KL-7 is available at the [TSEC/KL-7 ADONIS & POLLUX webpage](#).