# THE KL-7 ON MERCHANT SHIPS DURING THE 1982 FALKLANDS WAR

**Operation Corporate and the TSEC/KL-7 Cipher Machine on the Eburna Tanker**

**Bernard Kates**

I was a civilian Radio Officer, employed by Shell which is how I came to be on the Eburna when it was chartered by the Ministry of Defence for the Falklands Task Force. The term they used was STUFT (Ship Taken Up From Trade). When I joined the ship she was just finishing a refit in dry dock and we only had one short trip across the North Sea to Petit Couronne and Hamburg before we got STUFT.

The Eburna was a product carrier, which is a tanker that can carry several different types of oil cargo without cross-contaminating them. We carried a cargo of fuel oil, diesel and aviation fuel which we transferred by RAS (replenishment at sea) to other ships. While we were doing that, we discovered that naval vessels did not at that time have the ability to make their own fresh water, and so we started making it for them and transferring that at the same time as oil.

Replenishment at sea or RAS involves two ships steaming alongside each other at a distance of 25 metres, maintaining a steady speed and keeping exact station on each other throughout complex anti-submarine manoeuvres. A RAS may take anything up to 12 hours to complete and requires outstanding seamanship by both crews. Let me assure you, it is not for the faint-hearted!

The KL7 was used by the British merchant ships that were sent to the Falkland Islands as part of the Task Force back in 1982. I had a very steep learning curve as radio officer, getting used to cryptography and using the KL7. In that event, encrypted traffic was sent to us by teleprinter broadcast in FEC mode (Forward Error Control) via Portishead Radio and we transmitted our encrypted replies using ARQ (Automatic Repeat Query) with SITOR. There was a large volume of traffic so I was very grateful that I didn't have to receive and send using manual Morse!

I did not keep any examples of the traffic we sent or received. However, I found this message, sent in clear by Portishead Radio/GKA to collective callsign MBMS (All British Merchant Ships) on 30th March 1982.

```
PORTISHEADRADIO TELEX NR604/30 CK68/66 30/1512 =

MBMS PORTISHEADRADIO =

REPORTS HAVE BEEN RECEIVED THAT ARGENTINA HAS ESTABLISHED A MILITARY
ZONE AROUND ITS MAINLAND TERRITORY AND THE FALKLAND ISLANDS AND HAS
SAID THAT ANY BRITISH SHIPS OR AIRCRAFT FOUND THEREIN WOULD BE
REGARDED AS HOSTILE AND THAT ARGENTINA WOULD ACT ACCORDINGLY AGAINST
ANY BRITISH SHIP OR AIRCRAFT FOUND WITHIN 200 MILES OF THE MAINLAND
FALKLAND ISLANDS SOUTH GEORGIA OR SANDWICH ISLANDS =

MODUK NAVY ++
```

Following this broadcast, all merchant ships involved with the Task Force were instructed to use encrypted callsigns and all radio traffic was encrypted.

I had no experience at all with naval communications nor crypto systems, apart from BRIMER which was the very basic Vigenère system carried by all British merchant ships, and probably easy to break. I did get an assistant, a Radio Officer from the Royal Fleet Auxiliary who had spent about 35 years in the navy and who knew the KL-7 extremely well. So between the two of us, we managed to keep the radio room going including dealing with encrypted traffic, and we also maintained a 24 hour watch on the UHF tactical net. We were very busy!

For the KL-7 we had a tape perforator which we used to prepare messages for sending. It could also read punched tape and we attempted to receive traffic that way by setting the teleprinter to copy to both tape and paper, but there was too much traffic. Our traffic would be mixed in with traffic for many other ships, so if we left the tape running all the time we would find the radio room full of it and we didn't know where on the tape our traffic began and ended.

So we let the teleprinter print it and then we typed the ciphertext into the KL-7. Then we stuck the gummed paper tape onto a message form and delivered it to the Captain. Sometimes, if we were feeling generous, we would also translate the "navy-speak" into English so that the Captain could understand what they were saying. The system indicator "FDDND" was always the first group of ciphertext. We would set up the KL-7 following the key setting instructions for the day, then switch it to "P" and type in that group, then switch to "E" and do the encryption.

Our KL-7 was supplied with one rotor cage and one set of rotors, which caused us problems because the settings always changed at 00:00 UTC but it often happened that a message encrypted with the previous day's settings would arrive up to two hours later. The instructions were that once the machine had been set, the key sheet for that day was to be destroyed, so in theory there would be no way for us to go back. In practice we kept the key sheet for an additional 24 hours so that we could go back if we had to. If we'd had a second cage and rotor set we would have kept one set for "yesterday" and the other for "today" so swapping between them would have been easy.

Daily machine settings were printed in a booklet which had the edges of all its pages stuck together, one page per day and one month per booklet. To set up the machine you would peel yesterday's sheet off, revealing today's settings on the sheet underneath. Used sheets would be torn out and incinerated.

The KL-7, rotor set and setting instructions were supposed to be kept in the safe. However, as we didn't have a safe (we were a Merchant ship) we kept them in a cupboard. There were very few spies running around in the middle of the South Atlantic so we figured that was probably secure enough.

I remember rewiring at least one of the rotors every month, and that it was quite a fiddly task involving many small parts. It was best to do it under strong light, and not a good idea to try it in rough weather when the ship was rolling and pitching so that parts could easily fall to the floor and disappear under the furniture!

I have downloaded the KL7 simulator and am having fun with it reliving old memories. The only thing the simulator doesn't do that the real machine did is to fail occasionally (actually quite often!) due to dirt under the keyboard. In accordance with Murphy's Law it would always do that when urgent traffic was on hand. Then there was nothing for it but to take the machine apart and clean it out.

Regarding communications capabilities, most marine transmitters were crystal controlled in the early days but from the 1970s on they were synthesised, although the first generation of Marconi synth gear was a bit unstable, so for SITOR use they had to be replaced with a high stability version. It was all very primitive.

When I was at sea between 1977 and 1984 most of my amateur gear was more sophisticated than the maritime gear. The Eburna was a rare exception. It had a fully synthesised transmitter that could go anywhere between 1.6 and 30MHz with 1.2kW. Maritime transmitters generally were marine bands only, so this was a bit of a luxury.

A standard ship installation had MF and HF capability, CW and USB, on the Maritime bands only. Ships and coast stations operated on separate frequencies to avoid QRM. On SSB the frequency spacing was large enough that full duplex operation was possible, particularly on larger ships where we could get some distance between the transmitting and receiving antennas. Ships also had maritime VHF in the 156 to 174MHz band, FM.

Many of the STUFT merchant ships were not originally fitted with radio telex installations and so would have had to rely on manual CW to receive the encrypted traffic broadcast from Portishead. When the Ministry of Defence discovered that, they insisted that all ships must have telex gear, and they supplied it before the ships sailed to join the task force.

There must have been much frantic scrambling around to find space in what was often a cramped radio room, then install the telex gear. I was fortunate in that the Eburna was very well equipped, with three main receivers (one dedicated to telex) and a high stability 1.2kW transmitter so we had no messing about with that.

Also, some of the STUFT ships were ferries taken from the cross-channel and North Sea routes and would not have had HF radio at all, so they would have needed quite a serious upgrade to their radio rooms.

For the UHF tactical net in the Naval Task Force they supplied us with a Clansman manpack portable radio, with two batteries but with only its attached blade antenna. That wasn't going to work well inside the wheelhouse, a nice steel box that may as well have been a Faraday cage! The only way we could have used that radio would have been to take it outside and operate from the bridge wing, but we were not about to do that when the temperature was below freezing most of the time.

So I cut up a coat-hanger and made a dipole cut for 300MHz, found a well-placed feed-through pipe above the chart table and duct taped it up there. Fortunately I found a length of discarded RG-58 coaxial cable with a BNC plug on it which proved to be exactly the right length to connect the dipole to the Clansman. So then we could sit in relative comfort in the chartroom and operate the radio from there.

It was immediately obvious to us that the Navy had absolutely no idea how merchant ships operated or how they were equipped. They never realised that for us to keep a 24 hour radio watch would require both radio officers to work 6 hours on, 6 hours off for the duration of the entire campaign.

Also, they seemed to expect us to know how to handle a tactical net, including encrypting and decrypting figures and phrases using the NATO code book. At first, I had no idea what was going on and it took me several days to work it out. Eventually I did, but I observed that a tactical net in a war zone is not the best place to learn military radio procedure!

There is quite a lot of information in the public domain about the armed forces involvement with the Falklands campaign but very little about the Merchant Navy during operation Corporate. You will find some information on the high-profile merchant ships that were involved, including the Queen Elizabeth 2 and the Canberra, but not much else.



Written for Cipher Machines and Cryptology.

More information about the KL-7 is available at the webpage TSEC/KL-7 ADONIS & POLLUX.

Ed. 3