Study Collection

The unveiled history of governmental message security (1945 - 1960)

By M.R. Oberman MSc

This article is motivated by the appearance of a book describing post-war developments in cryptography[1] and the recent acquisition of a rare Ecolex IV cryptographic machine by the Historic Collection of EEMCS in Delft. This "story" is about the security of electronic messaging communication. It started right after World War II when the telex network was the only carrier for electronic message traffic from desk to desk. The telex of that time was the precursor of our electronic mail and the follow-up of telegrams transmitted by Morse codes at the post office in the 1930s.

Telex is an abbreviation for teleprinter exchange. In a telex network, two tele printers send each other messages through a circuit-switched network. A teleprinter (Figure 1) can be directly operated by a person or can read character-based information from a paper tape reader. A printing mechanism prints the text on the receiving end, and a tape punch may be used to produce a paper tape. In order to reduce connection time, messages were often pre-punched so that they could be transferred at the highest speed possible. The transmission protocol is the Baudot code where each character is encoded in 5 bits. These 5 bits are used to read/punch so-called 5-hole paper tape [1]. The code transmitted, sent via fixed or wireless networks at that time, was easily intercepted by eavesdroppers. This created a need for encryption.

As with many projects, there is a multitude of people involved. Of these, a few people stand out. One of those people was prof. dr. ir. R.M.M. Oberman, the father of the author of this paper. He worked as a research engineer at the Dutch PTT from 1936-1957. Later he became affiliated with Delft University of Technology (1947-1980). He was appointed as an Honorary Member of the ETV later on. Prof. Oberman was the driving force behind the development of the first post-war cryptographic equipment for the Dutch government. The funding for research on electronic messages security after WWII was supplied by the Ministry of Foreign Affairs in The Hague, needing secret communications between the ministry and some of the most important Dutch embassies. Similar crypto-equipment was also used at that time (1946-1957) on all Dutch Royal Navy ships.

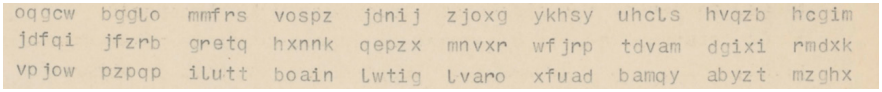

Figure 2. The formatting of a cipher text.

Oberman was well known for his developments in public switching technology. The same technique led to cryptography implementations, which immediately became a classified issue because of its governmental applications. This is the reason why nothing was ever written about it until I got my hands on his personal- and classified archive!

During WWII, every nation put emphasis on trying to read and decode messages from armies and diplomatic services from other countries, even from their allies. It became apparent that cryptographic equipment as used by several embassies was rather vulnerable to code-cracking. Crypto equipment was seen after WWII as the only mechanism to ensure fully secure electronic messages. Besides the added security it can be seen as the first step in administrative automation. An electronic cryptosystem replaced several people in a code room where coding and decoding messages was the main task. Through this development, fewer people had knowledge of classified information.

Figure 1. The Siemens Telex machine.

OTP

All crypto equipment immediately after WWII was based on the one-time pad system (OTP) [2, 3] which was the only system of that time that was proven to be unbreakable. Even in the age of quantum computing, this is to be expected. OTP stands for One Time Pad and is based on the use of a one-time, randomly composed key. In essence, a structured message (i.e. plain text) is drowned in real noise. The mixed sum of plain text and the random key is called the cypher text. Since the plain text is drowned in the noise, it is invisible and therefore unreadable. When

[1] www.oberman.nl/boek

Figure 3. The technician M. Koppenberg in front of "his" Colex.

the same noise is removed exactly from the received text, position by position with the same value (key-value) as on the sending side, the plain text reappears. The key generator was basically a perfect white noise generator. White noise as a technical item was well known to PTT being related to the simulation of telephone traffic to test switches.

One problem with OTP is the distribution of the key. The key must be available on both the sending and receiving sides before communications can be started. How do you ensure that the key text is available on both sides? A white noise OTP key generator cannot generate the same key text again. To overcome this problem, the white noise was recorded as a sequence of truly random numbers and punched on a paper tape (the key tape). The exact copy was made by a tape duplicator. The Ministry of Foreign Affairs in The Hague used its well-organized diplomatic postal system for the key distribution. For the Royal Dutch Navy, tapes were supplied during the ship visits to the home port. Proper key management was the crux behind the strict OTP security requirements.
OTP systems are symmetrical cryptosystems. They have identical keys on both sides, sending and receiving. OTP was the standard until 1975 when asymmetrical systems were invented. The sender and receiver have a different but mathematically related connection in asymmetric systems. This also laid the foundation for Bitcoin and other cryptocurrencies.

Colex

The Colex (Code-telex) system, like any OTP system, consists of two parts: the key generator and the mixer.
The key text must be at least as long as the message it protects and must comply with the white noise properties, i.e. be completely structureless and not be reproducible with the key generator. At that time it was a technical miracle. An example: a rotating drum suddenly stopped will give data with white noise properties. In the Ecolex systems, an advanced control mechanism was used to check the white noise statistics to be sure the key is fully random.
The mixer combines the key text with the message (plain text) producing the cypher text to be sent via the network. Such a mixer is network-dependent. When the network uses in-band signalling, the cypher text must not contain any control characters. At that time, the cypher text message format had a universal character: It consisted of a number of lines; each line is composed of 10 groups of 5 characters followed by two spaces (Figure 2).

A working system

Oberman had studied electrical engineering, as well as mechanical engineering at the then TH-Delft. This was special and practical for the development of the encryption system in those days, because in addition to the knowledge of switching properties and the needed electronic components, he also had knowledge of and insight into the mechanical properties of the system. E.g., the system must be able to work without maintenance or be locally repairable. After all, the systems could be located everywhere in the world in environments where people had little knowledge of this technology. It was almost impossible to service a defective system at remote locations such as embassies worldwide.

It takes more than just telex knowledge to make a good encryption device. In addition, there are several very different elements that make a system good. For example it had to be well

Û

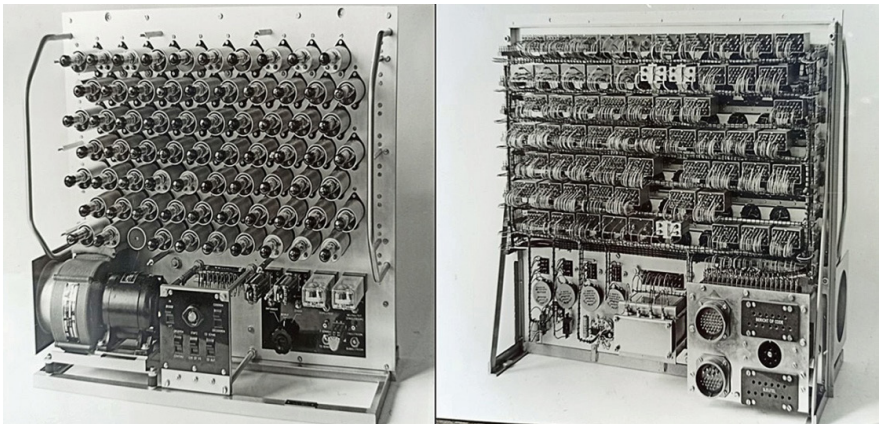

Figure 4. The Ecolex using radio tubes (front view and back view).

known within PTT in the same way as telex because of a diversity of subjects like functional standards to follow, tariffing, physical connection, network signalling and management issues. Encryption had to fit seamlessly into the worldwide telex network. Other important design questions were:

- What is a strong cryptosystem and why?
- How do we build a robust 24/7 running system?
- How to build a low-(non?) maintenance system? PTT had no service organization outside the national country's borders.
- How to build a system where mistakes do not lead to the release of the key text or the plain text?

Prof. Oberman first constructed a version of the Colex using relays (Figure 3). Other components were simply not available during the first post-war years. This relay-driven Colex encrypted 3 to 6 characters per second. In 1950 a radio tube follow-up was made – a functional 1-to-1 replacement - encrypting 40 characters per second, called the Ecolex (Figure 4).
The Colex was used from mid-1948 and officially put into service on April 5th 1949 by prime minister W. Drees in The Hague. At that time, it connected the embassies of Paris, London, Washington and Jakarta with the Foreign Affairs Office in The Hague. Six systems were made, each with about 98 identical relays. The switch to radio tubes made the relays intended for the Colex not usable anymore. However, the Colex relays had been purchased for twelve systems. The result: about six hundred relays had become redundant.

Transistors

Through visits to the USA in the course of 1952, including IBM and Westinghouse, Oberman had concluded that radio tubes were past their prime time. The transistor was, in his opinion, the better technical invention to replace radio tubes as the basic switching component. In his opinion, the transistor was the component that would take a fundamental step towards the realization of automation systems, computer systems, and also the construction of cryptosystems. Now we do know that the transistor became a future-proof solution, but in those days the considerations were:

- The basic switchgear unit was orders of magnitude smaller; the result: less extensive systems.
- Lower energy consumption, resulting in less heat generation.
- Faster switching capabilities.
- More robust than radio tubes, which means less maintenance.
- Non-hazardous low voltage and therefore more maintenance-safe.

Philips

In 1956 Oberman made the migration with his cryptosystems from the radio tube-based Ecolex to a system based on transistors as the core switching component. This was only 10 years after the first relay system was made by him and his team. Unfortunately, PTT wanted to eliminate everything related to the topic of cryptography. That change in policy was made a few years before 1957 when Oberman and his coworker Snijders [2] left PTT. Cryptography and everything related to it was passed on from PTT to Philips USFA in Eindhoven. In this way, USFA could make a quick start in the crypto field. Philips USFA produced the Ecolex IV of which a specimen was recently added to the Historic Collection in Delft (Figure 5). In 2003, the successor to Philips USFA stopped making crypto equipment in the Netherlands. A successful story came to an end.
The Colex and the Ecolex were simplex OTP systems. During WWII the theory behind the operation of OTP systems was already more than 35 years old and therefore widely known. The mathematical proof however was not given until WWII by Shannon [4]. There is no patent on OTP as a system since it is a well-known principle. A

What happened to the six hundred redundant Colex relays?
These relays were given by L. Kosten, who was head of the mathematical department at PTT in 1950, to the recently graduated Ir. W. L. van der Poel. Van der Poel joined PTT in 1950 immediately after graduating. His assignment was to build a computer. These redundant relays were the basis for the ARCO computer system which can still be seen in the Historic Collection.

Figure 5 . The Ecolex-IV, as recently acquired by the Historic Collection.

Figure 7. Prof. Oberman cycling at his department at the EWI-10th floor after his restart as extraordinary professor.

[2] A. Snijders cooperated closely with Oberman and also became a professor at TU Delft. He was the inventor of the state lottery system in 1970, which uses an OTP key generator.

patent could be obtained for a specific implementation thereof.
At that time, technology was very important to arrive at an effective solution. Additionally to technology, there must be a fit with the organizational environment. In short, this concerns the following points:

- The cryptographic work by prof. Oberman was quickly declared to be Top Secret classified information due to the sensitive type of application for the government. This sometimes led to less support or a lack of understanding of his work outside his immediate organizational environment.
- These struggles became the basis for his departure from PTT to the TU-Delft in January 1958.
- Prof. Oberman studied both mechanical and electrical engineering at the TU. This knowledge was crucial in order to make a good operational system in addition to a functional system.
- As a manager, little is known about Oberman historically. It was striking that when he left PTT for the TU, 10 out of the 13 people from his department at PTT followed him to the TU, to the switching department at the Electrical Engineering department at the TU-Delft within 2 years!

Besides these points the career of prof. Oberman has a few more remarkable aspects:
He holds more than 90 patents and he was the ultimate responsible person on behalf of the TU for the construction of the tall blue/orange EWI building, which was opened in 1969 and is still in use 52 years later.

Ê

Figure 8. M.R. Oberman, author.

[1] https://en.wikipedia.org/wiki/Baudot_code
[2] https://nl.wikipedia.org/wiki/One-time_pad
[3] www.cryptomuseum.com
[4] C. E. Shannon: Communication Theory of Secrecy Systems. Bell System Technical Journal, October 1949