History of the TSEC/KL-7 ADONIS & POLLUX

The first standard U.S. Armed Forces Tactical Lightweight Rotor Cipher Machine Using Electronics

Dirk Rijmenants

ABSTRACT

The TSEC/KL-7 is the first crypto machine to use electronics, developed as standard crypto device for the U.S. Armed Forces, the CIA, the FBI, NATO, and three Asian countries. This article presents the history of development, production, procurement, and use of the KL-7, based on declassified reports, records, minutes and technical publications from the cryptologic services, intelligence agencies and departments of defense of the countries involved.

KEYWORDS

TSEC/KL-7, AFSAM-7, ADONIS, POLLUX, ASA, AFSA, NSA, CIA, FBI, NATO

ARTICLE

Published 17 May 2022. Latest update 25 August 2025 - Version 5.2

CONTACT

Dirk Rijmenants
Cipher Machines and Cryptology
https://www.ciphermachinesandcryptology.com
E-mail: dr.defcom@telenet.be

INTRODUCTION

The TSEC/KL-7 is an American off-line crypto machine, developed by the Army Security Agency (ASA) and the Armed Forces Security Agency (AFSA) under the name AFSAM-7. The machine was introduced by the National Security Agency (NSA) in 1953 and renamed TSEC/KL-7 in 1955. The KL-7 was the first tactical, lightweight, rotor-based machine that used electronics and had excellent cryptographic properties. During the Cold War, the KL-7 was used extensively by the U.S. military, the CIA, the FBI and NATO, becoming the first-ever multinational crypto machine. The KL-7 was designed to resist any cryptanalytic attack, even when its technical details were disclosed. Two major security breaches occurred in the 1960s, when two U.S. warrant officers independently sold both the KL-7 design and operational key lists to the Soviets.

COPYRIGHTS

BRIEF DESCRIPTION OF THE KL-7

The TSEC/KL-7 is an off-line non-reciprocal rotor cipher machine with electro-mechanical and electronic components, including four electron tubes. The machine measures 12 x 12 x 3.37 inches (30,5 x 30,5 x 16,2 cm) and weighs 20.5 lbs (9,3 kg), which was quite compact for such a complex machine in the 1950s. The main components are:

- TSEC/KL-7 (AFSAM-7) is the complete machine.
- KLB-7/TSEC Base is the base of the machine and supports all other components. Its contact panel assembly has spring-loaded contacts across its surface that mate with the various other parts of the machine, making exchange of defective parts quite easy.
- KLA-7/TSEC (AFSAM-107) Rotor Stepping Unit is located on top of the base and contains the stepping mechanism and the actuator switches to manually advance the rotors if required. The Rotor Stepping Unit also carries the Cipher Unit.
- KLK-7/TSEC (AFSAM-207) Cipher Unit, also referred to as rotor cage, holds eight rotors that perform the actual encryption. One of the rotors is stationary.

The KL-7 is powered by 24 V DC, supplied either by the Power Converter that transforms 110 or 220 V AC into 24 V DC, or directly from a 24 V battery (e.g., vehicle battery). The 24 V DC powers a DC motor, which mechanically drives a 150 V AC generator inside the same housing, the stepping mechanism, the printer drum, and the pulse generator. The 24 V DC also powers the vacuum tube filaments and the stepping electromagnets. The 150 V AC is rectified to provide +220, +200 and -70 V DC to the electronics.

The keyboard contains 26 letters, 10 figures, the Letters and Figures keys, the space bar and repeat key. Underneath the keyboard is the Sliding Contact Board, operated by the Selector handle to switch between Plain, Encipher, and Decipher modes. When a key is depressed, the signal travels through the eight rotors to the printer. Which character is printed depends on the signal direction through the rotors, as chosen with the Selector handle, the selection of the eight 36-pin rotors from a set of 12, their internal wiring, the selected notch ring for each rotor, the order of those rotors in the Cipher Unit and their position at the start of the message.

The printer has a clockwise rotating print drum. At the same axle is a pulse generator with a rotating magnetic armature and fixed double stator with 37 pulse coils in a 360-degree pattern. When a pulse coil circuit is activated, its pulse is amplified by the electronics to energize the print hammer at the exact moment when the character passes the hammer.

When a character is printed, this also activates a clutch, connecting the printer axle through reduction gears with a second axle to provide both timing signals through its camshaft and mechanical power for the Rotor Stepping Unit. The rotors can step individually after each keystroke. This requires the activation of electromagnets that either allow or prevent the mechanical power from the DC motor to move a particular rotor (the electromagnets themselves do not move the rotors). Which rotors advance is determined by the notch rings on seven rotors (one rotor remains fixed). The notch rings control seven switches, connected to a logic maze circuitry that activates the stepping magnets to advance one single or multiple rotors, depending on the circuit's logic. [1 2 3]

Full technical description at https://www.ciphermachinesandcryptology.com/en/kl-7.htm

DEVELOPMENT OF THE AFSAM-7 AND TSEC/KL-7

The development of the KL-7 involved several agencies. The Signal Intelligence Service (SIS), established in 1929 as part of the Army Signal Corps, was responsible for cryptanalysis under the direction of renowned cryptologist William F. Friedman. In March 1943, the SIS was renamed the Signal Security Service (SSS), and by July of the same year it was again renamed the Signal Security Agency (SSA). Its successor, the Army Security Agency (ASA), was established in September 1945 and remained active until late 1976.[4]

In 1949, the Armed Forces Security Agency (AFSA) was established to merge all Communications Security (COMSEC) and Communications Intelligence (COMINT) efforts. William Friedman led AFSA's cryptologic division, and the agency gave the machine its initial designation AFSAM-7. However, the AFSA's means and responsibilities were scattered across numerous civilian and military services. To improve coordination, the National Security Agency (NSA) was established in 1952, with Friedman as chief cryptologist. The development of the KL-7 therefore involved the ASA, AFSA, and NSA.[5] [6] [7] [8]

The roots of the KL-7 go back to the Second World War, when the U.S. Army SIGABA rotor cipher machine, called ECM (Electric Cipher Machine) by the Navy, and the SIGABA CCM (Combined Cipher Machine) had set a new standard for secure, high-level Allied communications. At the tactical level, the lightweight mechanical M-209 was widely used. By the end of the war, the M-209 was no longer considered secure, and the U.S. Army expressed the need for a lightweight, secure crypto machine that could replace the M-209, yet offered a cryptographic strength comparable to the SIGABA.

The U.S. Navy was also seeking a compact cipher machine with the qualities of the ECM, with a focus on saving weight. In March 1945, the Army headquarters tasked the Signal Security Agency (SSA), soon after renamed Army Security Agency (ASA), to develop a machine that meet their requirements. Meanwhile, the CCM, based on the AJAX crypto principle and used by both the U.S. and United Kingdom, had become outdated and required replacement..

The project was designated MX-507, and the ASA saw it as a long-term research project. The researchers quickly decided to opt for a rotor-based machine. They also had to design a completely new lightweight printing system, as the machine was required to operate off-line and print out the messages on a paper strip. They eventually succeeded in reducing the printer system to one-quarter of its original size and weight.[9]

The ASA applied a new cryptographic principle, called re-entry or re-flexing, which required 36-pin rotors. The idea was to take parts of the cipher output, re-enter the output back into the enciphering process and re-encipher it again. Cryptanalyst Albert W. Small conceived this method in 1940 and filed a patent in 1944. However, his patent was placed under Patent Office Secrecy Order and would cause a patent conflict in 1957.[10]

The rotors were a further development of the early World War II types. The so-called Blue Rotor, used until the late 1950s, was a fairly large Hebern-type 26-pin rotor, simple and rugged. The regular rewiring of those rotors, required for security reasons, was quite complicated. A modified version of the Blue Rotor, called White Rotor, carried an alphabet ring and notch ring.

The U.S. Navy also developed a smaller Hebern-type 26-pin rotor called the Yellow Rotor, for its successor to the CCM. There was also a study on the use of printed rotors, with the circuits etched onto the rotor body. That project ended in 1953 and was ultimately abandoned.

The Armed Forces Security Agency (AFSA) was created in 1949 as the first American central cryptologic organization. One of its primary goals was to provide standardization of secure communications devices and determine a general policy for crypto equipment. The research conducted by the ASA was transferred to the AFSA in December 1949. The MX-507 was renamed AFSAM-7, which stands for Armed Forces Security Agency Machine No 7.

After a series of cryptologic studies, already initiated in 1946, AFSA decided to use the 36-pin Red Rotor with a rotatable alphabet ring and notch ring, for both the off-line AFSAM-7 and the AFSAM-9 teletype encryption. However, the Red Rotor had two major problems: tolerance issues with the plastic molding process and contact problems. The rotor used beryllium copper contacts, from which particles wore off and turned into abrasive non-conductive copper oxide. This worsened the wear even more, and also caused contact problems.

From 1946 on, several external contractors studied the problems with the Red Rotors. Tests with 200 contact materials found none better than beryllium copper and the plastic compound remained the most suitable. After more modifications and improvements, the Red Rotor was accepted but contact problems persisted.

After ten years of research, costing $1,250,000 ($14,598,851 in 2025), the engineers arrived at the Orange Rotor. One of the improvements was a rotatable alphabet ring that could be set by depressing and rotating it, without removing the ring from the rotor. Production of the Orange Rotor started in 1956. This rotor became the standard 36-pin rotor, later also for the KL-47B and KW-9. The development and production of the rotors involved Molded Insulation Co, Minneapolis-Honeywell Regulator Co. and American Phenolic Corp. (Amphenol).[11]

In April 1949, the United States and its allies had formed the North Atlantic Treaty Organization (NATO) and deteriorating relations with the Soviet Union resulted in a grim Cold War. Secure communications between the NATO members were an important part of making a front against the USSR. An additional challenge, faced by the AFSA, was to design for themselves a machine they could also distribute among their NATO allies without disclosing vital secret crypto technology that might end up in Soviet hands.

Given the size of NATO, it was more than likely that this machine or its specifications would eventually reach Russian soil. The design had to withstand any possible cryptanalytic attack by Soviet codebreakers, even when the technical details of the machine were disclosed. The security of the machine had to depend solely on the secrecy of the key settings, in keeping with Kerckhoffs' well-known principle of cryptography.

In September 1950, the AFSA demonstrated an engineering model. The final design used eight 36-pin rotors, a re-entry of ten rotor signals, and a most complex irregular stepping of the rotors, electrically controlled by notch rings on the rotors. Problems with the printer timing and the letter/figures shift system were solved by a clever design with electron tubes, making the AFSAM-7 the first tactical cipher machine ever to use electronics.[12]

During an ad hoc committee session of the BRUSA COMSEC conference, William Friedman, Albert Small, and Abraham Sinkov discussed the AFSAM-7. Friedman explained that the purpose of the conference was to discuss a limited exchange of cryptographic principles. When asked about the implications of an AFSAM-7 being captured, Small replied that it would not affect the security of U.S. communications for some time.[13]

The AFSAM-7 was approved, and the Army was asked to build prototype models. By December 1950, the Army declared the AFSAM-7 ready for mass production, being the first standard crypto machine in the U.S. Armed Forces. The cryptosystem was designated POLLUX, contractors were selected, and operational and maintenance manuals were prepared.

In February 1951, contracts were signed to produce 25,000 AFSAM-7s at a rate of 5,000 per year. The first repair and maintenance course for Army and Air Force personnel was scheduled in September 1951. However, due to tooling problems and material shortages, delivery of the AFSAM-7 was first delayed to June 1952, and then delayed again to January 1953. [14] [15]

In 1951, the BRUTUS crypto principle was proposed as a replacement for the CCM's outdated AJAX principle. The BRUTUS rotor stepping maze controlled the irregular movement of the rotors, with rotors 2 and 6 rotating in opposite direction, differing from the POLLUX stepping logic. BRUTUS used seven 26-pin rotors from a set of ten, with removable cams and alphabet rings. The number of notches on the notch pattern had to be 7, 9, 11, 15, 17 or 19 (co-primes numbers). Meanwhile, the Navy had been developing its own machine, initially named the Portable Cipher Machine (PCM) and later renamed AFSAM-47. They had already adopted the BRUTUS crypto principle for their AFSAM-47, but production, planned for late 1950, was already delayed.

The uppercase system on the British TYPEX cipher machine was non-standard, making a combined U.S./U.K. system impossible until the TYPEX was replaced. The CCM Replacement's Working Party suggested a system for combined use, to achieve compatibility between the AFSAM-7, AFSAM-47, the British SINGLET, and other U.K and U.S. machines. This comprised the Space key to piggyback on letter Z, switching to figures on J, and switching to letters on V.

However, the design of the AFSAM-47 used eight uppercase characters and was only compatible with the British SINGLET machine. Neither the limited nor extended uppercase system could be introduced until the British stopped using the TYPEX with BRUTUS adaptor. The limited upper-case system, which included numerals and space, was eventually adopted for all combined cipher machines. Until a combined policy was agreed, all cipher machines designed for U.S./U.K. were required to include at least the limited uppercase system.[16]

In October 1951, AFSA announced two types of operation: AFSAM-7 traffic for high-level communications was designated ADONIS, while traffic for the Army and Air Force was designated POLLUX. The differences between the two cryptosystems were the rotor sets and the Message Rotor Alignment procedure at the start of each individual message.

In 1952, the British services wanted to use the BRUTUS crypto principle to replace the CCM, as agreed in 1951. However, analysis showed that initial and long-term costs for meeting NATO requirements, including parts and rotors, were lower for ADONIS with its 36-pin rotors than for BRUTUS.

Plans were made for the phased introduction of the ADONIS principle in combined machines by January 1955. ADONIS equipment would be provided to the U.K. until they could produce their own crypto machine called SINGLET, incorporating the ADONIS principle. The final production contract for the AFSAM-7 was signed on February 9, 1952.[17]

The U.S. urged to standardize ADONIS with 36-pin Red Rotors, as these supported the re-entry principle, which was impossible with 26-pin rotors. ADONIS also avoided the use of rotor cage adaptors, ensuring compatibility with other combined cipher machines. AFSA's successor, the newly formed National Security Agency (NSA), also preferred ADONIS because the AFSAM-9 teletype encryption machine with nine 36-pin rotors, later renamed TSEC/KW-9, was also in development. As it turned out, the TSEC/KW-9 pushed the speed of electromechanical encryption to its limit and suffered from frequent synchronization loss.[18]

In December 1952, the U.S. Office of Communications Security Conference discussed the replacement of the CCM. Participants included the U.S. Army, Navy, Air Force, and cryptologists William Friedman and Albert Small. By then, the British were using the early POLLUX principle. Although technically identical, ADONIS conveyed the Message Indicator (i.e., rotor start positions) in encrypted form to the receiver, whereas the earlier POLLUX used a less secure method in clear. Friedman raised the question whether they should refrain from telling the British that POLLUX was inadequate and ADONIS more secure.

Meanwhile, production of the Navy AFSAM-47 continued to be delayed and the security of BRUTUS was questioned. One proposal was to improve the security of the BRUTUS with its 26-pin rotors by adding a plugboard. Although this could make it more secure than ADONIS, the AFSAM-7 had already been developed and was in production by the Burroughs corporation. The BRUTUS-based Navy AFSAM-47, manufactured by Teletype Corporation and subcontractors, was two years behind. The U.S. Army and Air Force preferred the AFSAM-7, and it could be made available for combined and NATO use by early 1955. The use of a plugboard for the AFSAM-7 was also briefly discussed, but Friedman argued that operators strongly opposed the idea because setting a plugboard was error-prone and also created problems when a message from the previous day would arrive.

In the long term, the AFSAM-7 with 36-pin rotors was more secure than the Navy AFSAM-47 with 26-pin rotors, as the AFSAM-7 could resist cryptanalysis longer. According to Friedman, cryptologists from both the U.S. and the U.K agreed against using BRUTUS for the AFSAM-47. Albert Small also preferred the ADONIS principle, but the U.S. Navy insisted on continuing production of the AFSAM-47 using the BRUTUS principle. Although the British also preferred BRUTUS, it was practicality, production costs, and the need for rapid replacement that prevailed.[19]

It was officially agreed that the SIGABA CCM machine, which used the less secure AJAX principle, urgently required replacement, as all cryptanalytic attacks effective against AJAX also worked on the CSP 2200, a modified SIGABA ECM Mark II. Friedman made it clear that ADONIS and AFSAM-7 were the solution to the CCM problem. Meanwhile, Navy tests on the AFSAM-47B, a modified AFSAM-47 with 36-pin rotors, compatible with ADONIS, were underway and had already completed 100 hours on the KL-47 printer without error. However, any production of the AFSAM-47B was at least two years behind that of the AFSAM-47.[20]

The Joint Chiefs of Staff believed that replacing the CCM by a machine using the BRUTUS principle should be postponed until service tests of the AFSAM-7 were completed. However, the Navy insisted on retaining the AFSAM-47 with BRUTUS and wait to see whether the AFSAM-7 ADONIS tests and production would succeed or fail, before redesigning their own AFSAM-47 with 26-pin rotors into the AFSAM-47B with ADONIS and 36-pin rotors.[21]

By November 1953, the delegation of the COMSEC Conference, which assessed the security of cryptographic equipment, did not favor POLLUX, because using the Message Indicators in clear posed risks of in-depth messages, and recovery of the key settings, certainly with high traffic volumes. In contrast, ADONIS was considered secure at all classification levels for at least ten years, when proper operating standards were maintained. U.S. cryptologists even considered the machine secure for the next twenty years. However, the British considered the AFSAM-47 with BRUTUS principle only secure for the next five years and recommended replacing the British CCM as soon as possible since it was expected to become insecure within three years. The TYPEX II and Typex Mk 22 remained secure for the next five years.[22] [23] [24] [25] [26]

The AFSAM-7, favored by the NSA, eventually proved successful, and the ADONIS principle was also chosen for the Navy AFSAM-47B. The NSA introduced the AFSAM-7 into the U.S. Armed Forces, and a smaller number of AFSAM-7s were also purchased by the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA).

In March 1954, the U.S. Joint Chiefs of Staffs approved the introduction of the ADONIS crypto-principle, now used in both the AFSAM-7 and AFSAM-47B, into the medium and high levels of NATO by mid-1956.[27] The AFSAM-7 was cryptographically more than capable of resisting any attack at the moment of its release. In 1955, the AFSAM-7 was renamed TSEC/KL-7, according to the new crypto equipment nomenclature, determined by the NSC in 1954, where TSEC = Telecommunications Security, K = Cryptographic, L = Literal (ciphertext in letters).[28]

The AFSAM-47B was renamed TSEC/KL-47. Individual components of the KL-7 and KL-47 were manufactured by several different U.S. government contractors. After final assembly at various locations, the machines became the property of the NSA and were distributed within the U.S. Although cryptographically compatible with the KL-7, the KL-47 retained an extended uppercase system with punctuation, while the KL-7 had a limited uppercase system with numerals only. Therefore, sending messages from a KL-47 to a KL-7 required spelling out the punctuation marks, or omitting them, to avoid decryption errors.

An ancillary Baudot paper tape reader called TSEC/HL-1 was developed for the KL-7 to enable direct reading and processing of five-bit punched tape, as produced by standard teleprinters. This required the removal of the KL-7 keyboard and installation of the KLX-7/TSEC keyboard adapter between keyboard and chassis.

In 1957, Boris Hagelin, engineer and founder of the Swiss company Crypto AG, told NSA cryptologist William Friedman that he had filed a patent application for the re-entry principle in 1953. Hagelin's U.S. patent No. 2,802,047 was issued in 1957 and conflicted with that of Albert Small, who had already filed the patent application in 1944, at the insistence of none other than William Friedman. In addition, in 1956, Small requested declassification of his still-pending patent, which remained under Secrecy Order.[29] [30]

The issue of conflicting patents had to be resolved. The NSA feared that sensitive information might be disclosed and preferred that Albert Small's pending application remained classified if he would not acquire legal claims for compensation. Another option was to release only unclassified portions of the patents. The conflict was ultimately resolved, and Albert Small's Patent 2,984,700 was issued in 1961. Crypto AG later incorporated the re-entry principle in its HX-63, twelve years after the introduction of the AFSAM-7.[31] [32]

TEMPEST ISSUES

TEMPEST, the set procedures and techniques to shield devices from eavesdropping on unintentionally emitted signals, was in its early research stages when the KL-7 was being developed. Although Bell engineers recognized the risk of unwanted stray signals as early as 1943, initial attempts to reduce those signals were limited to power supply filters and shielding as much as possible. The first breakthrough came in 1956 with the introduction of low voltage circuits with transistors. However, this occurred four years after the introduction of the KL-7, and the first comprehensive TEMPEST regulations were only drafted in 1958.[33] [34]

The KL-7 was fitted with a radio interference filter between the external power supply and the internal electronics, but some electrical contacts and coils could still be a sources of unwanted signals. In 1955, the NSA conducted a study to determine whether the printer-magnet coil, which triggers the print hammer, emitted signals that could be exploited. These print coil signals were detectable up to 25 feet from the machine.

Analysis of recorded signals during decipherment of a KL-7 message showed that by measuring the interval between intercepted pulses of the print coil, and knowing the order of the letters on the print drum, enabled the recovery of the plain text. Variations in the KL-7 motor speed between pulses could complicate measurement of the intervals, but other signals, radiated at the same distance, could determine the change of motor speed, making recovery of the plain text much easier. The researchers also found a correlation between the number of rotors that stepped and print drum speed deviations.

The KL-7 remained in use without additional technical changes to reduce unwanted signals, but the 1958 TEMPEST regulations undoubtedly recommended operating the machine only at fixed or tactical locations where close-range eavesdropping was unlikely. Nevertheless, even in secure locations, stray signals could unexpectedly piggyback on other equipment and enable eavesdropping from far greater distances.[35]

THE KL-7 IN SERVICE

The KL-7 was initially intended solely for use by the U.S. Army, Air Force, Navy, the CIA and FBI. At the 1953 Communications Security Conference in London, the NSA proposed sharing the ADONIS crypto principle with NATO allies. The goal was to improve communications security and interoperability, and replace the less secure Combined Cipher Machine (CCM) with the more advanced AFSAM-7.

Between 1951 and 1954, the Army Security Agency (ASA) procured 6,547 units, intended to replace the less secure M-209. The FBI ordered 120 AFSAM-7s, 120 office cases at $100 each, 120 additional AFSAM-207 cipher units (i.e., KLK-7/TSEC) at $50 each, 250 sets of rotors (two per machine to enable a swift daily key change), five spare AFSAM-107 stepping units (i.e., KLA-7/TSEC), five spare AC power converters at $25 each, paper tape and ink ribbons. The order totaled $258,900. However, by 1953, the cost of the FBI order had risen to $299,232 (equivalent to $3,560,199 in 2025) due to rising production costs.[36]

ASA initially received 650 AFSAM-7s, including 120 for the FBI. These were gradually issued, two per FBI office. Meanwhile, the twenty FBI offices with the highest message volumes already received AFSAM-7s on loan from the NSA, which also train FBI personnel in operating the machine. The CIA received its first four AFSAM-7s for local testing in 1954, but field use only started the following year.[37] [38]

By 1954, all FBI offices, Quantico, the White House Signal Detachment (WHSD), the Seat of Government, and President Dwight D. Eisenhower's Air Force One were equipped with the AFSAM-7. However, many AFSAM-7s from the early production runs suffered from technical deficiencies. In April 1954, the NSA director received a list of deficiencies, noted by the Chief of Army Field Forces during testing.

To meet performance standards, the ASA requested modifications to 2,339 AFSAM-7s from the 1st, 2nd, and 3rd production run, at the time in storage facilities. These units were returned the following month to the Burroughs Corporation. Upon arrival of the second shipment at the ASA, it was discovered that 615 from the 1400 already delivered AFSAM-7s also required modifications. As a result, machines already deployed to the White House, ASA Europe, and ASA Pacific had to be replaced by modified versions.[39] [40]

The U.S. Joint Chiefs of Staff approved the use of the AFSAM-7 by NATO in 1954. The plan called for its introduction at medium and high NATO levels by mid-1956. The NSA recognized that the AFSAM-7, or reproductions using the same cryptographic principle, might eventually enter non-military use in NATO countries, or even fall into Soviet hands. Nevertheless, the NSA remained confident that the AFSAM-7 was secure against Soviet attempts to decrypt the messages, even if its cryptographic principles and specifications were compromised. The machine was therefore certified for handling Top Secret messages.

Meanwhile, the new British BID/60 SINGLET crypto machine was developed with the same crypto principle as the AFSAM-7, intended to replace the aging CCM (LUCIFER), the British CCM-Typex interoperable with the American CCM/SIGABA. The British SINGLET closely resembled the AFSAM-7 and used identical rotors, but was not expected to enter production before 1960. In 1954, the U.S. decided to allocate 3,500 AFSAM-7 units to the United Kingdom and 3,000 units to other NATO countries. These machines were loaned and remained the property of the NSA.[41]

In early 1955, the Standing Group of the North Atlantic Military Committee (NAMC), which provides policy guidance, decided to supply the AFSAM-7 to the Supreme Allied Commander Europe (SACEUR) for distribution to all NATO members.[42] Target date to replace the CCM with the AFSAM-7 was set for 1 July 1956. In the meantime, the AFSAM-7 was renamed TSEC/KL-7.

In 1955, the U.S. Army Security Agency Europe assigned two military instructors to NATO, to assisted in training personnel designated to repair and maintain the TSEC/KL-7. Candidates for the maintenance school had to be qualified as teletypewriter mechanics and have the appropriate security clearances. Basic knowledge of electronics was also desirable.[43] [44]

In September 1955, the NAMC issued an allocation list for KL-7s. The then-current quantities were: Belgium 156, Denmark (including Greenland and the Faeroes) 158, France 711 (including the Commander Biscay Atlantic sub-area and the Commander Moroccan Atlantic sub-area), Greece 200, Italy 603, Luxembourg 15, Netherlands 239, Norway 169, Portugal (including the Commander Continental Portugal and the Island Commanders of the Azores and Madeira) 168. Each country's Ministry of Defense Army, Navy and Air departments received four KL-7s each, and the Supreme Commanders 12 KL-7s.

Within the Allied Headquarters, the HQ Commanders in Chief received 12 KL-7s. The Allied Land Commands, Allied Army Groups and Tactical Air Forces, and the Armies and Tactical Air Forces 8 KL-7s each. The Army Corps and Air Divisions received 6 KL-7s, The Army Division, Air Force Escadres, and Wing Groups 3 KL-7s. The independent brigades 2, National District Commands 2, major fleet Bases 4, Island Commands 3, Patrol Force Commanders and Flag Officers 2 each, Naval and Maritime Air Bases 3. Ocean-going aircraft carriers, battleships and cruisers 2 each, destroyers, destroyer escorts, submarines, and Patrol Coastal boats 1 each. Temporary or alternative Naval or Maritime Air bases received 2 KL-7s.[45]

Note that 3,500 units had already been assigned to the UK in 1954. In the following years, more KL-7s were allocated to additional countries and military echelons, with the 1965 allocations being the last known.[46]

In 1956, NATO decided to procure the HL-1 tape reader and KLX-7/TSEC keyboard adaptor to handle the growing volume of encrypted traffic.[47] The NATO members were required to determine their required stocks of KL-7 spare parts, and could also order a kit with basic spare parts at the price of $150 per machine. The kits and spare parts were gradually delivered between 1957 and 1960.[48] [49]

Also in 1956, the CIA's Operations and Training Division planned to employ the AFSAM-7 for mobile message centers. Noise issues were resolved with a soundproof container, and a keyboard adaptor became available in 1957. That same year, CIA O&T personnel visited the NSA to observe the HL-1 tape reader, which could process perforated tapes. The HL-1 was later installed on loan at the CIA Signal Center.[50] [51] [52]

In 1957, NATO agreed to adopt the KL-7 for second-level and first-level communications with ADONIS key lists, replacing Typex (SIMPLEX) traffic that used the Typex II with SIMPLEX pads. This agreement also comprised each NATO member's Ministries of Defense and Foreign Affairs, their embassies in Paris and Washington, and their National Military Representative in Washington.[53] In 1958, KL-7 deployment was further extended to minesweepers, fast patrol boats, and long-range maritime aircraft.[54]

The KL-7 was used by the U.S. and its NATO allies Australia, Belgium, Canada, Denmark, France, Federal Republic of Germany (i.e., former West Germany), Greece, Italy, Luxembourg, the Netherlands, Norway, New Zealand, Portugal, Turkey, and the United Kingdom. Outside of NATO, the KL-7 was also loaned to South Vietnam, South Korea and Nationalist China.[55]

Some geopolitical info on the Asian countries: South Vietnam, officially called Republic of Vietnam (RVN), existed from 1955 until the North Vietnamese victory in 1975 and formation of the current Socialist Republic of Vietnam (SRV). South Korea was formed in 1948, following the division of the Korean peninsula in two states along the 38th parallel, with the U.S.-backed South Korea, officially the Republic of Korea (ROK), and the Soviet-backed North Korea, officially the Democratic People's Republic of Korea (DPRK). The Republic of China, often called Nationalist China, was founded in 1912 by the Kuomintang. Following the communist victory in 1949, the Kuomintang fled to the island state of Taiwan, since then officially called Republic of China (ROC), to this day disputed by mainland People's Republic of China (PRC).

In 1958, the price per KL-7 totaled $1,458. The set comprised the KLB-7 base at $814, KLA-7 stepping unit $328, KLK-7 cipher unit $80, CE87054 Carrying Case $161, CE87066 AC Power Converter $75, and a set of rotors $100. A complete KL-7 would cost $16,025 when converted into present 2025.[56]

The extended use of the KL-7 was discussed, and NATO member Canada pointed out that the KL-7 had not yet reached full reliability due to problems with the pulse generator and proposed a book cipher as essential back-up. The KL-7 was also used aboard NATO submarines. In 1959, they approved the Basic Submarine Code as a backup system for the KL-7. The code, in itself not secure enough, was used in conjunction with one-time letter pads.[57] In December 1959, NATO also authorized the use of KL-7 ADONIS for first-level military and diplomatic traffic.[58] By 1966, approximately 25,000 KL-7 had been produced for the U.S. and its allies. [59]

When France left NATO's military structure in 1966, NATO required a separate cryptosystem to exclude France from its most sensitive communications. Initially, two new KL-7 ADONIS key lists and a new set of rotors with other internal wiring were introduced. NATO did continue to distribute COSMIC TOP SECRET key lists to France but introduced separate key lists for the other NATO members, from which the French were excluded. The KL-7 key lists for General Small Ships, the Maritime Patrol Aircraft, Atlantic Channel North Sea and Baltic Area remained available to France.[60]

Despite its extensive use, the KL-7 was not universally popular and became notorious for its keyboard and rotor contact problems. The operators often had to push firmly on the keys to keep the machine cycling, which reduced their typing speed, and increased the risk of typos. Dirty contacts and the beryllium copper issue could cause the machine to halt, the notorious so-called dead-rove. To mitigate these issues, the rotors and keyboard contacts required regularly and meticulous cleaning.

The contact problems with keyboard and rotors were inherent to the design with numerous moving electrical contacts. In Plain mode, the signal from key to printer pulse coil passed through only two contact points on the keyboard’s sliding contact board. In Cipher or Decipher mode, the route from key through all rotors to pulse coil passed at least 13 contact points.

However, due to the re-entry principle, the encrypted output could loop back to the input through one of the ten re-entry wires, and re-encrypted again by the eight stepping rotors, resulting in up to ten passes through all rotors and their numerous contacts. In such a case, up to 472 contact points had to function flawlessly. Dirt or copper oxide on a single contact point could interrupt the electrical signal and permanently halt the machine, requiring extensive cleaning of all rotors and the keyboard contacts.

During start-up, the electron tubes require 16 seconds to heat up before typing on the keyboard is possible, since the printer is controlled by the electron tubes. The KL-7 also produces a significant acoustic signature. When the KL-7 is powered, the motor slowly accelerates, and the reduction gears produce a characteristic high-pitched noise. The advancing rotors also produce a distinctive sound.

The KL-7 and KL-47 rotors were regularly rewired by personnel with appropriate security clearances. Some rotors were rewired annually at the national or NATO level, while some rotors, often referred to as the “NSA rotors”, were sent directly to the NSA for rewiring by NSA personnel only. It was strictly forbidden to operators, and even to maintenance technicians with crypto clearance for KL-7, to check out the internal wiring of the rotors.

Technicians were not permitted to test the rotors pin-to-pin. Instead, they were instructed to place a defective rotor on a large conductive plate that made contact with all rotor pins simultaneously, and check each pin at the other side with an Ohmmeter. This method allowed the technician to detect a broken wire without revealing its corresponding pin on the other side of the rotor.

There were incidents where a KL-7 or KL-47 was compromised. One well-known incident was the seizure of the USS Pueblo by North Korea in 1968. Officially, the ship was designate an AGER-2 (Auxiliary General Environmental Research). In reality, the ship was equipped with SIGINT (Signals Intelligence) and ELINT (Electronic Intelligence) systems to intercept North Korean and Soviet communications en technical signals. When the North Koreans forces attacked and boarded the ship, the U.S. Navy immediately ceased all communications with the KL-47 until the NSA had distributed new key lists. The machine itself was designed to resist cryptanalysis, even if the technical specifications were known to the adversary. However, what they didn’t know was that some KL-47 key lists had already been compromised.[61]

During the Vietnam War, KL-7s were loaned to the Army of the Republic of Vietnam (ARVN). COMSEC support for the KL-7 was organized by the ASA, located at Tan Son Nhut Air Base in Saigon (today Ho Chi Minh City). The Special COMSEC Support Unit at the Air Base provided crypto maintenance down to component level. Its mission included supporting the ARVN’s crypto unit and training personnel to perform basic maintenance and operate the KL-7. Australian and New Zealand forces also used the KL-7 in Vietnam.[62]

In 1965, the 101st U.S. ASA Security Detachment, operating under cover designator 7th Radio Research Unit, was based in Saigon. The 7th RRU conducted Signal Security analysis (SIGSEC) and performed cryptographic security assessments of the ARVN's use of the KL-7 to ensure the machines were operated as prescribed. The 7th RRU concluded that the ARVN became highly proficient in using the KL-7.[63]

The U.S. forces in Vietnam used the KL-7 from division level down to company level. However, an analysis by the 101st ASA Detachment revealed that Communications Security (COMSEC) was often neglected in the heat of battle. Operation SILVER BAYONET, including the famous Battle of Ia Drang in 1965, showed that a combination of underestimated enemy strength and poor COMSEC could cause heavy losses. The KL-7 was not employed for intra-battalion communications or at lower echelons. Instead, manual systems were used, which were often less secure, or plain unencrypted messages were transmitted over radio.[64]

During the course of the Vietnam war, and after the withdrawal of most U.S. troops in 1973 and the subsequent defeat of the ARVN in 1975, various types of crypto equipment fell into the hands of the North Vietnamese Army (NVA), including some KL-7s. One of those machines, a KL-7 belonging to a U.S. Marine unit, was handed over to the Russians, who sent it to the Soviet Socialist Republic of Poland for analysis. After the dissolution of the Soviet Union, Polish officials handed that KL-7 over to the NSA, where it is now part of NSA's National Cryptologic Museum collection.

Advances in technology and the introduction of miniature electronic components greatly increased computational power available for cryptanalysis. As a result, the KL-7 was no longer considered secure enough by the mid-1960s. Vital message traffic, enciphered with the KL-7, was often superenciphered (i.e., double-enciphered) using other systems.

During the Cold War, signals units from several NATO member states provided secure communications to NATO in West Germany. From the early 1960s, NATO's Joint Headquarters in Rheindahlen was supported by British signal personnel, and communications were encrypted on-line in real-time with one-time tape mixers.

Although they also used the KL-7, the off-line encrypted KL-7 messages left the cipher room in five-letter groups, printed on paper strips and stuck onto A4 pages or message forms. These ciphertext groups were then transcribed onto punched teleprinter tapes for onward transmission and sent on-line, superenciphered using the ECOLEX one-time tape mixer.[65]

By the 1970s, the KL-7 was largely replaced by the long-established KW-37 JASON, KW-26 ROMULUS and KW-7 ORESTES on-line cipher equipment, while the fully electronic KL-51 RACE off-line cipher machine could be regarded as its successor. Some KL-7s remained in service, mostly as back-up, until they retired in the early 1980s.

Although the KL-7 was intended only for use by the U.S. military, its NATO allies and certain government departments, there were some instances in which civilians operated the machine. One example was the 1982 Falklands War. Within days, the British Navy had to deploy a large naval task force across the South Atlantic.

They chartered merchant ships to support the operation and one of these was the Eburna tanker, carrying fuel oil, diesel and aviation fuel, to transfer fuel at sea. The civil radio officers had no experience with naval communications or cryptosystems and had to quickly learn the basics of cryptography and how to operate the KL-7.[66]

MAJOR SECURITY BREACHES

In 1974, a highly sensitive, well-placed source told the FBI that the Soviet military intelligence directorate GRU had an agent codenamed "Greenwood", who was an American from the U.S. military, previously stationed in France and Vietnam. The FBI launched counterintelligence operation codenamed "Hookshot", and the Army Intelligence and Security Command (INSCOM) narrowed the search to former U.S. Army Signals Warrant Officer Joseph Helmich (1937-2002). From 1958, Helmich held a Top Secret security clearance. He served in 1963 as a crypto custodian in France, and from 1964 to 1965 in Vietnam with crypto clearance in a supply unit. In 1966 he was stationed at Fort Gordon, Georgia, but resigned from the Army after his security clearance was revoked. Since Helmich fit the profile perfectly, the FBI launched an intensive surveillance investigation.

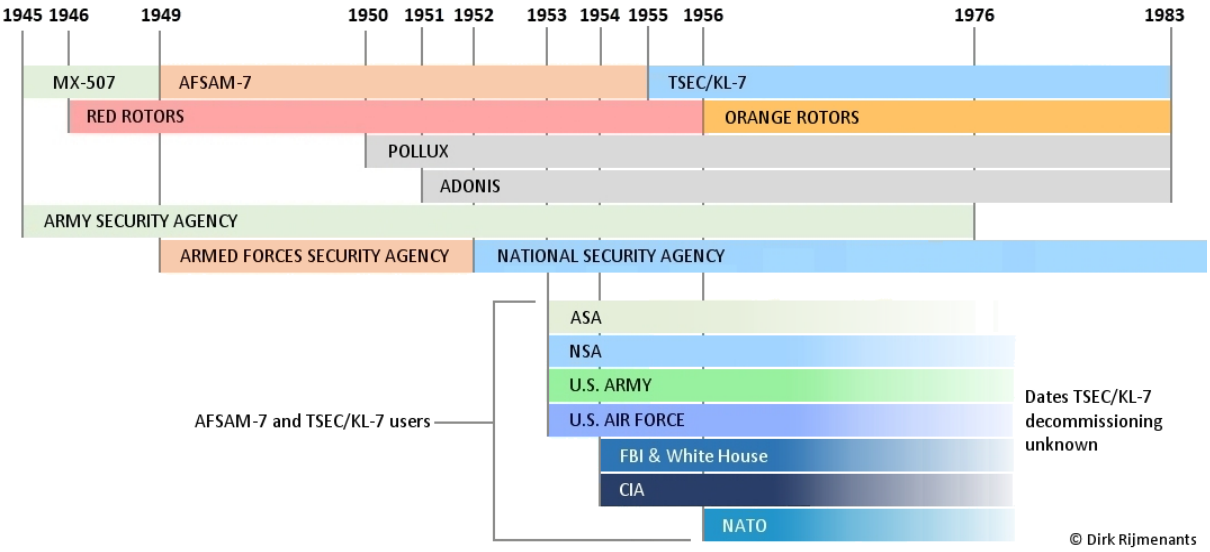
Facing financial problems, Helmich contacted the Soviet Embassy in Paris in 1963 and received $131,000 in exchange for technical information on the KL-7, which at the time was the most widely used cipher machine in the U.S. military. After returning to the United States, Helmich continued to provide KL-7 key lists to the Soviets until 1966, enabling them to decrypt KL-7 messages from U.S. troops and Military Intelligence units in Vietnam. Although suspicions arose as early as 1964, since his wealth did not match his pay grade, it was only during the FBI surveillance in early 1980 that they observed him visiting the Soviet Embassy in Canada to make contact with the KGB. After extensive interrogations, Helmich eventually confessed in 1981 and was sentenced to life imprisonment.[67] [68] [69] [70] [71] [72]

In 1985, the FBI received a tip from the ex-wife of John Anthony Walker (1937-2014), a retired U.S. Navy communications specialist with a Top Secret Crypto clearance. The FBI observed Walker dropping a grocery bag alongside a road north of Washington, D.C. The bag contained 129 copies of stolen secret U.S. Navy documents. At the same moment, a Soviet KGB agent left a grocery bag containing $200,000 a few miles away, a classic espionage tradecraft dead drop to covertly exchange documents and money without meeting face-to-face. John Walker was arrested the following night in a motel. The subsequent investigation sent shockwaves through the military intelligence community.

In 1967, Chief Warrant Officer John Walker simply walked into the Soviet Embassy in Washington, D.C. with a KL-47 key list, offering to sell secret U.S. Navy documents for cash. This marked the start of a spying career that lasted 18 years. In 1973, John Walker recruited his friend Jerry Whitworth, who was also a U.S. Navy communications specialist. Walker left the Navy in 1976 and recruited in 1984 his brother Arthur, a retired U.S. Navy officer who worked for a Department of Defense contractor. Walker also recruited his son Michael, who had enlisted in the Navy. They would later become known as the Walker spy ring.

During a search of Walker's home after his arrest, the FBI discovered a special device provided by the KGB and designed to read the internal wiring of the KL-47 rotors. During interrogations, Walker also admitted handing over complete technical maintenance manuals to the Soviets, allowing them to reconstruct a fully operational KL-47, cryptographically identical to the KL-7. Michael Walker was arrested in 1985. John Walker, Arthur Walker and Jerry Whitworth were sentenced to life imprisonment. Michael Walker was released in 2000.[73] [74] [75]

TSEC/KL-7 TIMELINE



The timeline above shows the development from the MX-507 project to the AFSAM-7 and TSEC/KL-7. The ASA developed, procured, and distributed the machines. From 1949 onward, the AFSA, and later its successor, the NSA, was responsible for communications security. Although the AFSAM-7 existed on paper in 1949, it took two years from the 1950 engineering model to the actual start of production in 1952, with deliveries to the Armed Forces only beginning in early 1953. The POLLUX procedure for low-level traffic was adopted in 1950, and the more secure ADONIS procedure for high-level message traffic was introduced in 1951. Owing to persistent problems, the Red Rotors were replaced by the Orange Rotors in 1956.

Although the NSA succeeded the AFSA in 1952, the machine's name did not change to TSEC/KL-7 until 1955. Machines produced from 1955 onward carried the name TSEC/KL-7, while earlier production runs were gradually retrofitted with the updated name labels. The exact dates of the KL-7’s final decommissioning of are unknown, as the machines were gradually recalled from multiple services and allied countries.

FINAL THOUGHTS

The KL-7 was a unique machine in several respects. It was the first machine developed under a centralized cryptologic organization and introduced as a standard crypto device in all parts of the U.S. armed forces and their allies. At that time, the KL-7 employed the latest cryptologic techniques and was the first cipher machine to incorporate electronics. However, its rotor-based design quickly became obsolete in the face of electronic miniaturization and growing computational power. The KL-7 was one of the last electromechanical rotor cipher machines.

The compromise of some key sheets and disclosure of technical details did not compromise all KL-7 communications. Different key settings, also known as crypto nets, were used for different services, military units, echelons, and separate geographical locations. This practice, known as compartmentalization, prevented the broad compromise of all communications if a single key setting is exposed.

The importance Soviet Intelligence placed on the KL-7 and KL-47 key lists, despite already possessing full technical details of these machines, suggests they were either unable to break the message traffic purely by cryptanalysis, or they lacked sufficient computing power to decipher and exploit the messages within a practical timeframe during the 1960s.

Many operators cursed the machine for its quirky keyboard and frequent contact problems, which demanded regular maintenance. They welcomed its fully electronic successors, yet today they speak with nostalgia about the machine and even vividly recall the distinctive sound of its stepping rotors.

Although less well-known to the general public than the WWII German Enigma machine, the more advanced KL-7 served for decades in many countries around the world, playing a part in Cold War intelligence, companionship, and even exciting stories about treason and espionage. The KL-7 is a true Cold War cryptologic icon.

BIOGRAPHICAL SKETCHES

Dirk Rijmenants has a passion for all things radio, electronics, programming, and cryptology. During his 39-year career, he worked with a wide range of COMSEC equipment, and on some of which as a technician. Since 2004 he runs the Cipher Machines and Cryptology website and the SIGINT Chatter blog, to share his interest in cryptography, military, and intelligence history.

REFERENCES

All of the following documents are declassified and publicly available. Some references include specific page numbers. However, as different versions of some documents exist, page numbers may vary, requiring the use of a search tool to find the relevant passages.

Certain organizations or authors impose conditions or limitations on public or commercial use of their documents. The NSA documents are released through their Declassification & Transparency Initiatives, Freedom of Information Act releases (FOIA), the William F. Friedman Collection, and NSA Historical Releases. Other sources include FOIA's and historical releases, preserved by the National Security Archive and governmentattic.org, the CIA Reading Room and the Internet Archive. Please consult their terms of use. All NATO documents are sourced from the NATO Archives Online. Please consult their guidelines for use, permission, and credits. All referenced documents are also available on the KL-7 webpage:

https://www.ciphermachinesandcryptology.com/en/kl-7.htm

[1] NSA - Repair and Maintenance Instructions for TSEC/KL-7 (AFSAM 7) Joint, 1955. Declassified 30 Mar 2009, FOIA Case #47709 by Bill Neill, and published by Nick England.

[2] NSA - Operating Instructions for TSEC/KL-7 ADONIS Operation, September 1966. Canadian CSEC information declassified and released 28 April 2001 CSEC ATIP Cace#A-2010-00015. NSA information declassified and released 21 April 2011, FOIA Case #64246.

[3] NSA - A History of U.S. Communications Security - David G. Boak Lectures, Volume I, original p33, July 1973. Released in 2015, ISCAP No. 2009-049.

[4] U.S. National Archives, Records of the National Security Agency/Central Security Service (NSA/CSS). Record Group 457, 1917-93. Timeline with dates establishment U.S. Army cryptologic services SIS, SSA and ASA.

[5] NSA - Post War Transition Period, the Army Security Agency 1945-1948, 7 April 1952. Declassified for release by NSA on 05-31-2016 pursuant to E.O. 13526, MDR Case 82626.

[6] NSA - The Early History of NSA by George F. Howe. Approved for release by NSA 18 Sep 2007. FOIA Case #7319.

[7] Joint Chiefs of Staff - Memorandum AFSA 1949, JCS memorandum to director of Armed Forces Security Agency on establishment of AFSA. ID A68965 Declassified for release by NSA on 12-04-2014 pursuant to E.O. 13526.

[8] AFSA Armed Forces Security Agency Council, establishment Armed Forces Security Agency, 1951. Doc ID A68919. Declassified for release by NSA on 1 March 2014 pursuant to E.O. 13526

[9] NSA - Cryptologic Almanac 50th Anniversary Series, AFSAM-7, p1-p3. Doc ID 3575720. Declassified and released by NSA 10 April 2007 pursuant to E.O 12958, as amended. MDR 51909.

[10] NSA - U.S. Signal Corps Patent Board, Meeting No 30, 1940. Friedman Collection, document ID A104884. The process of altering characteristics of Cryptographic Devices by Re-Cipherment or Re-Codement by Mr Albert W. Small, Junior Cryptanalyst.

[11] NSA - A History of U.S. Communications Security Post-World War II, Equipment - Part II, A.4, Rotors and Rotor Development, p80-84. Released 4 February 2011, pursuant to E.O. 13526. MDR59142, published by governmentattic.org

[12] NSA - Cryptologic Almanac 50th Anniversary Series, AFSAM-7, David A. Hatch, NSA doc ID 3575720. Declassified and released by NSA 10 April 2007 pursuant to E.O 12958, as amended. MDR 51909.

[13] NSA - Minutes of an ad hoc committee of the BRUSA COMSEC Conference, held on 30 September 1950. NSA Friedman Records, doc ID A67271.

[14] NSA - The National Communications Security Materiel Program, September 1954. Friedman collection, doc ID A61110. Declassified and released 30 January 2014 pursuant to O.E. 13526.

[15] NSA - Cryptologic Almanac 50th Anniversary Series, AFSAM-7, p5.

[16] NSA – Report of the U.K./U.S. Communications Security Conference Held in London In July 1951. Friedman records A67165. Released 20 May 2014.

[17] NSA - Memorandum for Members AFSAC, Replacement or the Combined Cipher Machine, 24 December 1952. Friedman Records, doc ID A59485.

[18] NSA - A History of U.S. Communications Security - David G. Boak Lectures, Volume I, original p33, July 1973. Released 14 October 2015, ISCAP No. 2009-049.

[19] NSA - Transcript of Office of Communications Security Conference, Replacement of the Combined Cipher Machine, 22 December 1952. Friedman Collection, document ID A59490. Released on 28 January 2014 pursuant to E.O. 13526.

[20] NSA – Letter AFSA Director Gen. Canine to Chief Division of Cryptography Department of State, Capt. Parke, Memo for Record, 24 June 1952. Attacks on AJAX, Hermes and CSP 2200 (HCM Mark 4). Released 19 Sept 2013. ID A272413,

[21] NSA - JCOS Staff Meeting, Replacement Combined Cipher Machine (CCM), 1953. Friedman collection, doc ID A59449. Released 27 January 2014 pursuant E.O. 13526.

[22] NSA - UK/US Communications Security Conference 1953 Report Sub-Committee to the Executive Committee - Security assessment of cryptographic equipment in use and under development, pdf p4-p5. NSA ID A522921. Released 27 May 2014 pursuant to E.O. 13526

[23] NSA - U.S. Communications Security Equipment, Part I, Literal Cipher Machines - AFSAM 7, AFSAM 47B, 1953. Friedman collection ID A522530, released 11 November 2014 pursuant to E.O. 13526.

[24] NSA - JCOS Staff Meeting, Replacement Combined Cipher Machine (CCM), 1953. Friedman collection, NSA doc ID A59449. Released 27 January 2014 pursuant E.O. 13526.

[25] NSA - Memorandum USCIB, Disclosure ADONIS Cryptoprinciple to NATO Countries, 30 September 1953. Friedman documents, NSA doc ID A61288.

[26] NSA - Program to Improve the Communications Security of NATO Countries, 21 September 1953. Memorandum for the Members of USCIB, Friedman documents, NSA doc ID A61293.

[27] NSA - Memorandum for the Members of USCIB, 3 May 1954. Release of AFSAM-7 to NATO Nations. Friedman documents, NSA doc ID A61057. Released 21 April 2014.

[28] NSA - Nomenclature For Communications Security Materials, 24 November 1954, doc ID A66119. Released in 2014 by NSA, pursuant to E.O. 13526.

[29] Patent nr 2,802,047 from August 6, 1957, B.C.W. Hagelin, Electric Switching Device For Ciphering Apparatus. Filed Oct. 16, 1953, ISCAP No. 2009-049

[30] NSA/CSS Archives, Memorandum For The Record, Hagelin Negotiations, 18 December 1957, report Friedman's visit Hagelin Laboratories, conflicting re-entry principle patents, NSA doc id A60669.

[31] NSA - Applications for Patent of Albert W. Small. NSA Chief Patents Branch, 27 February 1956. Request for declassification of re-entry principle, NSA doc ID A58689.

[32] A. W. Small, 1944 U.S. Patent 2.984.700, Method and Apparatus for Cryptography, re-entry principle filed Sept. 22, 1944. Issued May 16, 1961, after solving patent conflict.

[33] NSA - History of U.S. COMSEC, Vol I, 10th Lecture Tempest, original p89, and Vol II Tempest lecture (update) original p39. Release 14 October 2015.

[34] NSA - TEMPEST: A Signal Problem. Released by NSA on 27 September 2017, FOIA Case #51633.

[35] NSA - Plain Text Radiation Study of TSEC/KL-7 (AFSAM 7), Donald E. Schumacher, 2 August 1955.

[36] FBI - Automatic Ciphering Equipment, Note Mr. Harbo to D.J. Parsons. Purchase of 120 AFSAM-7, office cases, cipher units, rotor sets. FBI Record/Information Dissemination Section Records Management Division, FOIA Black Vault, pdf p46-47, 74-76,178 from 29 Sept 2015.

[37] FBI - Letters J.E. Hoover on FBI Bureau Codes, distribution TSEC/KL-7 (AFSAM-7), key lists FBI offices, training, 1960. SENSTUDY 75: FBI Files Shared with Church Committee (62-HQ-116395), p.3, p.5, p.17.

[38] CIA, Newsletter Sept. 9, 1953. Delivery AFSAM-7 in October 1953. Released 30 March 2001, FOIA CIA-RDP78S05452A000100030020-2.

[39] FBI - Memorandum of Conference AG's July 13, 1955, J.E. Hoover. AFSAM-7 procured for all field offices, Quantico and Govt. Government, pdf p257-262. FOIA No. 1145592- 00 governmentattic.org

[40] ASA, History of the Army Security Agency and Subordinate Units, Fiscal Year 1954, Volume I, Procurement of Cryptographic Equipment, p43-47. NSA Doc ID 6582943.

[41] NSA - Report of the U.K./U.S. Communication Security Conference 1953, sharing 3,500 AFSAM-7 to U.K. and 3,000 to other NATO countries. Friedman Documents, NSA Doc ID A523031.

[42] NATO – Memorandum SACEUR, proposed distribution of AFSAM 7 to NATO, target date 1 July 1956. NATO Doc Item SGM-179-55.

[43] NATO - Cryptographic Arrangements for NATO. KL-7, Typex SIMPLEX and Typex LUCIFER, NATO doc Item SGM-0287-56.

[44] NATO - Training of NATO Command and National Personnel in Operation, Maintenance and Repair of the TSEC/KL-7, 19 August 1955. NATO doc Item SGM-0586-55.

[45] NATO -Provision of an Off-Line Cipher Equipment for NATO use, 14 September 1956. NATO doc item SGM-687-55

[46] NATO - Allowance Table for ADONIS Equipment, 29 March 1965. list of countries and allotted KL-7 per department and military levels. NATO doc Item SGM-0115-65.

[47] NATO - Availability HL-1 and KLX-7, 23 March 1959. Request Federal Republic of Germany for 38 TSEC/HL-1 and KLX-7/TSEC. NATO doc Item SGM-0181-59.

[48] NATO - Automatic Use of the KL-7. TSEC/HL-1 tape reader and KLX-7 keyboard adaptor, 18 May 56. NATO doc Item SGM-0792-56.

[49] NATO - Policy Ordering and Maintaining Supply Spare Parts TSEC/KL-7, 21 December 1956. NATO doc Item SGM-0854-56.

[50] CIA - Monthly Report 1-30 Sept. 1956 Systems Engineering Branch - Engineering Division, AFSAM-7 for Mobile Message Center, noise issue, keyboard adaptor, pdf p4, p7. Released 17 July 2001, FOIA CIA-RDP78-02820A000100080017-4.

[51] CIA - Trip to NSA by O&T and Security Divisions, 9 August 1957. Released 13 November 2002, FOIA CIA-RDP78-02820A000300010030-4.

[52] CIA - operation 1951-66, AFSAM-7/KL-7 use at CIA Headquarters Signal Center, p82-87. Released 28 October 2004, FOIA CIA-RDP84-00499R000400080001-4.

[53] NATO - Replacement First Level Typex-Simplex Channels, 9 September 1957, including list of Ministries of Defense, Ministries Foreign Affairs, Secretary of State for External Affairs. NATO doc Item SGM-0588-57.

[54] NATO - Extension Use TSEC/KL-7 for General NATO Communications, 10 September 1958. NATO doc Item MCM-0115-58.

[55] NSA - Records related to the charter and meetings of the USCSB from 1940-1980. United States Communications Security Board (USCSB). Minutes of the Thirteenth Meeting 23 November 1970, governmentattic.org pdf p43.

[56] NATO - TSEC/KL-7 Meteorologic Use. Minesweeper, Patrol Boat, Maritime Aircraft, including price KL-7 and parts, 9 April 1958. NATO doc Item SGWM-208-58.

[57] NATO - Submarine Code in Conjunction with One-time Pad as Backup for KL-7, 24 February 1959. Use for command to all subs, and subs only to command. NATO doc Item SGM-0116-59.

[58] NATO - TSEC/KL-7 ADONIS Systems for National Traffic, 4 December 1959. Authorization for national military and diplomatic traffic. NATO doc Item SGM-0688-59.

[59] NSA - A History of U.S. Communications Security - David G. Boak Lectures, Volume I, original p37, July 1973. Released in 2015, ISCAP No. 2009-049.

[60] NATO - Distribution Cryptomaterial, 1 May 1967. After France leaving NATO, separate KL-7 key lists issued to France. NATO doc Item IMSWM-059-67.

[61] NSA - Cryptographic Damage Assessment, USS Pueblo, AGER-2, 23 January - 23 December 1968. NSA Doc ID 3075790. Released 2012 FOIA Case #40722.

[62] The KL-7 in Vietnam. COMSEC Support for the TSEC/KL-7 at Air Base Saigon, D. Maring, 2024.

[63] NSA - National Security Archive Electronic, Briefing Book No. 90, Dubious Secrets, Document 13A, Annual Historical Summary U.S. Army Security Agency, FY 1965. U.S. 101st USASA Security Detachment 7th RRU, Saigon, Vietnam.

[64] NSA - Working Against the Tide (COMSEC Monitoring and Analysis) Part Two, Chapter III - COMSEC Surveillance. June 1970. Viet Nam War era. Battle of Ia Drang 1965. Use of KL-7 at division down to company level, p90-95. Released 2004, FOIA #41608.

[65] The KL-7 at NATO in West Germany. ET's Story on OTT Mixers and the TSEC/KL-7, M. Davies, 2024.

[66] The KL-7 on Merchant Ships During the 1982 Falklands War, Operation Corporate and the KL-7 Cipher Machine on the Eburna Tanker, B. Kates, merchant ships civil radio officer, 2017-2022.

[67] FBI - Operation Hookshot, counterintelligence operation and identification Joseph George Helmich. NSIA-FBI files, National Security Archive, archive.org

[68] DNI - Office Director of National Intelligence, Counterintelligence - CI References, CI Reader Volume III. p265, Joseph George Helmich.

[69] NATO - Annual Review of Terrorist, Espionage, Subversive and Other Activities (November 1984 - November 1985), p26-27 Walker Spy-Ring. NATO doc Item C-M(85)75

[70] CIA - Generals Testify in Espionage Case. General Westmoreland and General Rienzi in Helmich case, sanitized copy New York Times, released by CIA on 22 July 2010, CIA-RDP90-00552R000302610012-8

[71] CIA - Prosecution in Ex-GI's Spy Trial Paris Saga Joseph Helmich, declassified CIA sanitized copy Washington Post. Released by CIA on 22 July 2010, CIA-RDP90-00552R000302610009-2

[72] CIA - Ex-Army Cryptographer Indicted on Spy Charges, Joseph Helmich, declassified CIA sanitized copy Washington Post. Released by CIA on 6 January 2012, CIA-RDP90-00965R000100270071-7.

[73] DNI - Office Director of National Intelligence, Counterintelligence - CI References, CI Reader Volume III. p233, John Anthony Walker.

[74] NATO - Annual Review of Terrorist, Espionage, Subversive and Other Activities (November 1984 - November 1985), p26-27 Walker Spy-Ring. NATO doc Item C-M(85)75

[75] U.S. Army Command and General Staff College - Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System, 1967-1974, as Exploited by CWO John Walker. Major Laura Heath thesis.