Telephone Secrecy

Melville Klein

Abstract

This article presents a history of significant milestones in the development and deployment of high-level telephone security for the *National Security Establishment*. As a backdrop it briefly covers the methods to provide telephone privacy from shortly after the telephone was invented continuing through the introduction of the radiotelephone. Using these as precursors, what follows are the measures the U.S. government has taken to assure telephone secrecy since before World War II leading to today's ubiquitous availability of enciphered telephony (*ciphony*). The challenges ciphony has placed on science and engineering are emphasized over operational history, which are better dealt with by others referenced herein.

Tactical ciphony for military operations is not covered.

> ***James Harris Rodgers received a patent in 1881 on a circuit-hopping system, which under control of relays, transmitted over two or more circuits in rapid succession. –*** **The Codebreakers*, David Kahn, 1967***

Prologue

When telecommunications came on the scene in the 1840s, the "dots" and "dashes" of Morse messages, though readily adaptable to confidentiality, were mainly coded for brevity. Before filing at the telegraph office, commercial users coded their messages privately, not much different than for sensitive mail. During the Civil War both the Union and Confederate armies used *telegraphy* as the prime source of command and control. Nomenclator tables, a combination of *codes* and *ciphers*, were the dominant method to provide message confidentiality.

Operational U. S. telephone privacy, with the exception of jargon codes, had to wait over fifty years after Alexander Graham Bell first transmitted speech electrically (1876). Unlike the telegraph, which could be encrypted offline by either manual or mechanical methods, *telephone scrambling* had to be done electronically in real time. Therefore, in its early days the telephone operating company had no other technical option but to transmit in the clear. Customers accepted the minimal risks from wiretappers or operator monitoring. However, to thwart eavesdropping on their overseas radiotelephone circuits, AT&T introduced telephone privacy in the nineteen twenties by frequency *transposition*. Operationally effective in its time, it offered only technical challenges to all but the most concerted interloper, a far cry from the online cryptographic security available for telegraphy circa 1920. At the onset of World War II, telephone secrecy became a high priority "cost be damned program" drawing attention at the presidential level. (It remained, however, beyond the realm of economic reality until the Internet.)

This article spans the major milestones of strategic telephone secrecy from its World War II genesis at the Bell Telephone Laboratories (BTL) to the Cuban Missile Crisis. For italicized words the reader is referred to Appendix A, Glossary. See Appendix B for Acronyms; Appendix C for Figures; and Appendix D for "Telephone Secrecy Firsts."

Bell Telephone Labs: The Crucible of Telephone Security

Communication security has been a major concern of governments since time immemorial. The advent of telecommunications raised the specter within both government and the private sector of how to protect signals outside the control of the parties involved. The Bell Telephone Laboratories pioneered research in U.S. communication innovation. Telephony security could vary from jargon codes, physical security of the medium (e.g., *protected distribution systems*), to *noise masking* or *cryptography* (transposition or *substitution* under the control of a *code* or a *key*). Except for jargon codes, Bell Lab engineers filed for patents on the others starting before 1920.

Choctaw Indians speaking in their native language on radiotelephone during World War I completely surprised the Germans; in the WWII Pacific campaign Marines used four hundred Navajos as codetalkers – neither was ever broken.

A patent for noise masking was filed in 1919 by R. D. Parker, which claimed that "superimposing...a current of continuously varying frequency" derived from a phonograph record on the speech was a means of insuring secrecy. The recipient subtracted a synchronized replica of the masking noise thereby recovering the speech. This was a novel idea, but uncorrectable distortion over wireline or radio media made it operationally impractical at that time. BTL engineers continued to experiment with scrambling analog speech in the frequency and/or in the time domain to provide radiotelephone privacy. In the 1920s AT&T introduced the A-3 system to deny the casual listener intelligible speech. The A-3 "diced" the speech spectrum into five bands transposing and inverting them (of the 3,600 possible combinations, only six were operationally usable).

The German Postal Authority prior to WWII had become very adept at breaking the A-3, President Franklin Roosevelt and Prime Minister Winston Churchill's favorite means of radiotelephony.

Telephone Secrecy Breakthrough

Shortly before the Japanese attack on Pearl Harbor, President Roosevelt established the National Defense Research Committee (NDRC). Chaired by Vannevar Bush of Massachusetts Institute of Technology (MIT), it was premised on civilian control of military research. Bush brought together 6,000 of America's brightest academics and private sector engineers and scientists to promote and organize military research. One group in the NDRC, recognizing the importance and urgency of planning for a worldwide communications network, enlisted BTL to assist the Army Signal Corps with its systems engineering tasks including *communications security*. Message traffic was readily securable, but voice transmissions were not, especially radiotelephone where interception was easy and privacy methods primitive.

Dr. O. E. Buckley, who became president of BTL in 1940, was charged with contacting the military and others concerned with speech security, *ciphony*. In his study of military communications, R. K. Potter, Buckley's alternate representative, identified two distinct areas of need: 1) short-term mobile privacy and 2) long-term, high-echelon secrecy, both suitable for telephone circuits. Buckley, a strong ciphony advocate, undertook this work at the Bell Labs without a written contract under the auspices of the Chief Signal Officer (the NDRC eventually accepted BTL's proposal).

Development

A very tightly held program, designated Project X (aka SIGSALY) for the high-echelon strategic system, was initiated in October 1940.

BTL's task was to expeditiously develop, produce, and deploy fixed-plant highly secure telephone terminals to be operated and maintained by Signal Corps personnel. A small group of Bell Lab researchers under A. B. Clark, notably R. K. Potter, Harry Nyquist, and D. K. Gannett, investigated a suitable speech processor for SIGSALY. The team expanded to conduct research on encryption algorithms and modems for transmitting the signal over voice frequency channels.

The speech processor design capitalized on Homer Dudley's work circa 1935 on a voice coder (*vocoder*) for commercial privacy and *channel derivation* (i.e., deriving several channels in place of one) applications. The underlying principle of a vocoder was one of analysis and synthesis. The analyzer measures the voice energy from multiple filters across the audio frequency spectrum and also measures the fundamental *pitch* of the speaker. Variations in a speaker's delivery are nominally limited to 25Hz. The synthesizer creates harmonics of the speaker's pitch, which are modulated by the slowly varying spectrum energies. In the case of unvoiced sounds (i.e., "s" or "sh"), noise serves as the "carrier" (Figure 1). The resulting output is synthetic speech, which, though intelligible, leaves much to be desired for speaker recognition (positive identification). Research on the cryptographic component proved to be a more daunting challenge.

Potter's survey of eighty speech "secrecy" patents found a common fault in all. Like the A-3 they provided only technological surprise not cryptographic security – a determined and resourceful interloper could undo them. Rejecting these approaches, Potter pursued a different course in early 1941: noise masking the analyzer output. The results were similar to those of R. D. Parker. Next, Potter proposed digital substitution, using the method patented in 1919 by G. S. *Vernam* of AT&T for encrypting Teletype on-line: modulo2 addition of a five-level plain text tape with a random five-level key tape. (Table 1) Potter's experiments of *quantizing* vocoder channels to on-off signals added modulo2 to binary keys, though secure, produced badly mutilated synthesized speech, unacceptable to the listener.

		S	
		0	1
K	0	0	1
	1	1	0

Table 1
VERNAM Encryption Modulo2
C = (S+K) modulo 2
C(0) = [K(0) + S(0)] or [K(1) + S(1)]
C(1) = [K(1) + S(0)] or [K(0) + S(1)]
Given that K (key) is flat & non-predictable, cipher is flat independent of S (plaintext)

Subsequently M. E. Mohr constructed a quantizer for up to ten levels. After experimenting with it, the team decided to encode the vocoder channels into six nonlinear amplitude steps (*senary*). The adoption of senary steps at the syllabic rate (25Hz) was a compromise between received voice quality and expected radiotelephone transmission margins, i.e., fading, noise and linear distortion.

In May 1941 Potter and Nyquist concluded that, mathematically, modulo6 addition of a nonpredictable senary key (where all six levels were equally probable) to senary plaintext would produce a cryptographically secure senary cipher (Table 2). R. C. Mathes invented an electronic "re-entry" circuit for modulo6. (Though not told it was for SIGSALY, Claude Shannon, the father of Information Theory, was consulted early on about the modulo6 encryption.) The remaining elements of the system were the *modem* and source(s) of key.

The modem team, having had considerable experience with Teletype transmission over radio, was faced with the problem of designing a modem for a six-level signal vice the customary binary FSK. Amplitude modulation was discarded since selective fades could be as high as 20db on transatlantic radio. They adopted a scheme of frequency shift keying six frequencies in each channel every 20ms (The equivalent of 129bits/sec per channel for a 600 baud *senary* signal). The transmit modem consisted of a twelve senary FM signals (170 Hertz spacing) covering the audio spectrum. which could be transmitted over ordinary voice frequency telephone lines to an *independent sideband HF* radio transmitter.

		S					
		0	1	2	3	4	5
	0	0	1	2	3	4	5
	1	1	2	3	4	5	0
K	2	2	3	4	5	0	1
	3	3	4	5	0	1	2
	4	4	5	0	1	2	3
	5	5	0	1	2	3	4

Table 2
Potter-Nyquist Modulo6 Encryption
C= (S + K) modulo6
C(0) = C(1) = C(2) = C(5) = 1/6
Given that K (key) is flat and non-predictable, cipher is flat independent of S (plaintext)

The receive terminal separates the twelve enciphered channels, demodulates each channel and synchronously decrypts with matching keys. The decrypted *spectrum channels* drives the vocoder synthesizer as shown in Figure 1.

To take maximum advantage of off-the-shelf Teletype components, the engineering design was based on a parallel architecture throughout. Figure 2 shows the transmitter, composed of twelve separately filtered channels from the speech processor (*codec*) through the encryptor to the modem. The codec analyzer measured the energy in ten channels across the audio spectrum (150 to 2,950Hz); two channels (a main and vernier) measured the fundamental pitch or no pitch of the speaker. The analyzer outputs were quantized to six discrete levels via "*steppers*," RCA 2051 gas thyratrons (See photo on p. 87), one stepper for each level, firing at twenty millisecond intervals; the pitch frequency (main and venier) was similarly quantized.

A sixteen-inch record stored prerecorded one-time encryption key (SIGGRUV) which when added modulo6 to each of the codec steppers produced twelve cipher streams. Three additional tones, the first for turntable changeover and the other two for synchronization, were also recorded.

As an alternate senary key source, BTL developed the "thrashing machine" (SIGBUSE). It consisted of an array of clattering relays and telephone selector switches controlled by pseudo- random key from M-228 rotor machines (SIGCUM). The M-228 machines were developed by the Signal Corps for on-line Teletype encryption. A *full duplex* SIGBUSE system, housed in five bays, produced senary key on-line at 600 baud (See photo on p. 87). Though not as secure or reliable as the SIGGRUV, SIGBUSE did not pose the physical security concerns of distributing twelve minutes of key per one sixteen-inch record. SIGBUSE handled operational traffic up to SECRET, whereas the one-time key was used for TOP SECRET voice conferences.

Development of One-time Key System

Digitizing Gaussian noise produced the one-time key records described above. Noise outputs of twelve RCA 2051 thyratrons each sampled fifty times per second were quantized to six uniformly distributed levels via steppers similar to those used in the codec. The stepper outputs amplitude modulated twelve 170Hz spaced tones from 595 to 2,295Hz, which were combined and recorded on vinyl phonograph records at 33 1/3 rpm (Figure 3). Key production initially done in New York City by Bell Lab personnel was eventually taken over by ten officers and twenty-five enlisted members of the 805th Signal Service Company at the Pentagon in December 1944. By incorporating the BTL modifications (SIGSOBS), the Signal Corps was able to manufacture two acetate recordings (SIGJING) at once, lowering the cost. Two playback terminals were associated with every SIGSALY terminal, each providing of unique key for a *full duplex* TOP SECRET conference.

In March 1942 one channel of the system was tested on an HF simulator to determine its performance under artificial fading conditions. It passed. The completed experimental model was quickly tested for operation and stability, and was continually being used as a test bed for design refinements and for training Signal Corps personnel. By April 1942 a complete set of drawings was ready to be turned over to Western Electric.

“But that was before I was introduced to... the vast complex of top-secret global communications....the magic of unbreakable codes....” Excerpted from the Preface to “A World War II Wac’s Memoir: My Journey to the Pentagon’s Top Secret Command Center,” Dorothy Madsen (Lt. Col. USAR Ret), to be published.

Deployment

In early 1943 Alan Turing, the UK’s premier cryptologist, visited Bell Labs to accredit the system for the British government. The assistant chief signal officer had bestowed jurisdiction for ciphony to the Signal Intelligence Service (SIS) in February 1942 (However, this author could not find correspondence from NARA files where a S.I.S. or an A.C.S. official had accredited SIGSALY).

On 25 April 1945 Prime Minister Churchill had a long dialog with President Truman over SIGSALY on Heinrich Himmler’s offer to make a separate peace with British and American forces. Captain Madsen assisted Truman on its use for this historic telephone conversation.

Bell Lab members commented “on the terrible conversion ratio – 30kw of power for 30milliwatts of poor quality speech”!

During the first official SIGSALY conference, inaugurated on July 15, 1943, between Washington and London, Dr. Buckley said, “...it must be counted among the major advances in the art of telephony.”

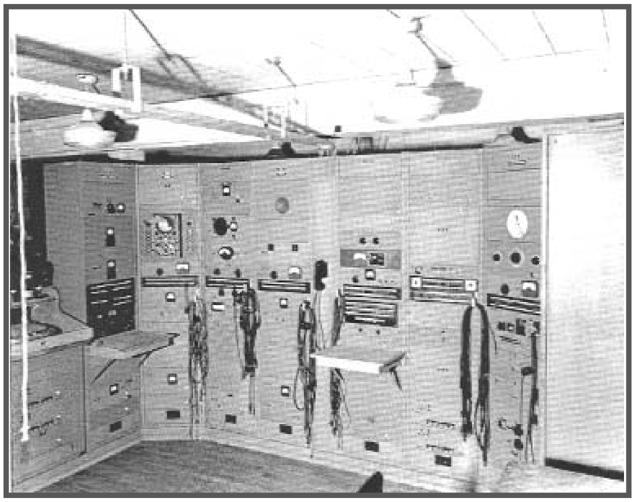
From 1943 to 1946, twelve SIGSALY terminals provided secure teleconferencing intra-theater, for the White House staff and the General Staff in Washington to Theater Commanders and our British allies. In the case of the Pacific Theater, the Pentagon terminal was connected to an HF radio terminal in Oakland, California, by full-period AT&T telephone lines.

SIGSALY was initially operated and administered by the Signal Corps. The General Staff assumed the responsibilities starting in March 1944 by the order of the secretary of war. Colonel Humelsine’s Staff Communications Branch at the Pentagon handled the classification, priority, reproduction and distribution of SIGSALY and secure (SIGTOT) message traffic. Captain Dorothy Madsen wrote a General Staff Circular for eligible users, set up the administrative procedures, and personally edited all transcripts.

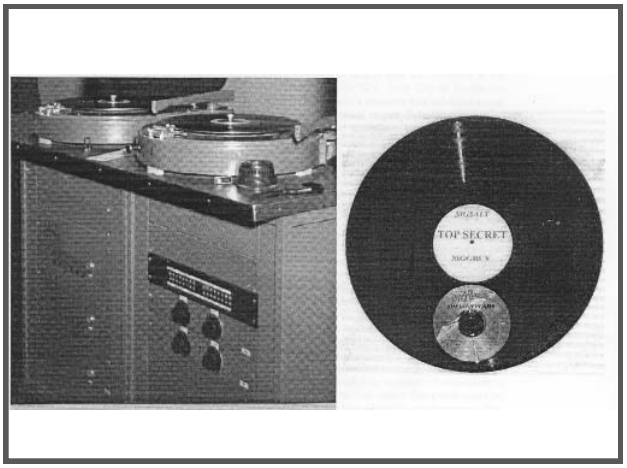
The 805th Signal Service Company was in charge of the overseas terminals, and to the extent possible followed the above procedures. The Signal Corps retained technical responsibility for transmission and encryption.

The Army Communication Service couriers distributed SIGSALY key records worldwide and in conjunction with AT&T Long Lines supported the 805th with radiotelephone and Teletype transmission facilities. One SIGSALY terminal occupied thirty seven-foot relay racks and required over 30kw of power.

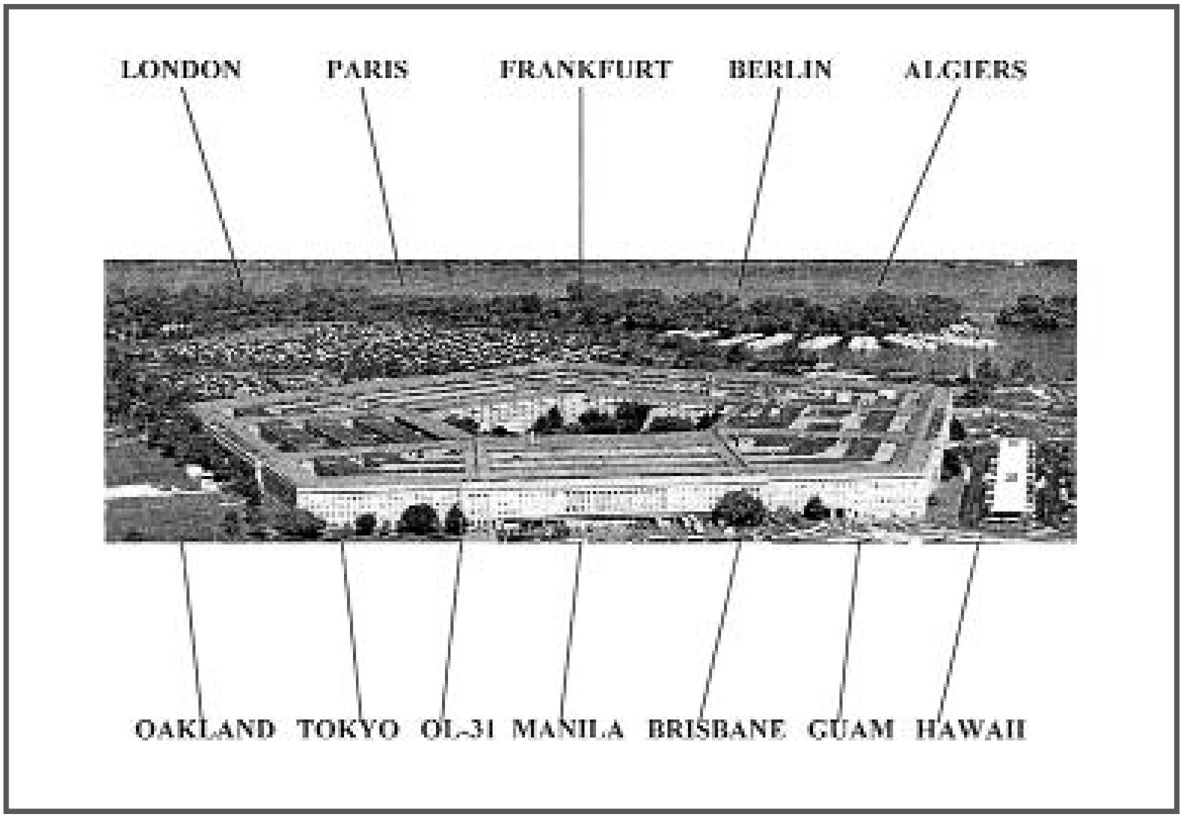
Until SIGSALY was decommissioned, the terminals



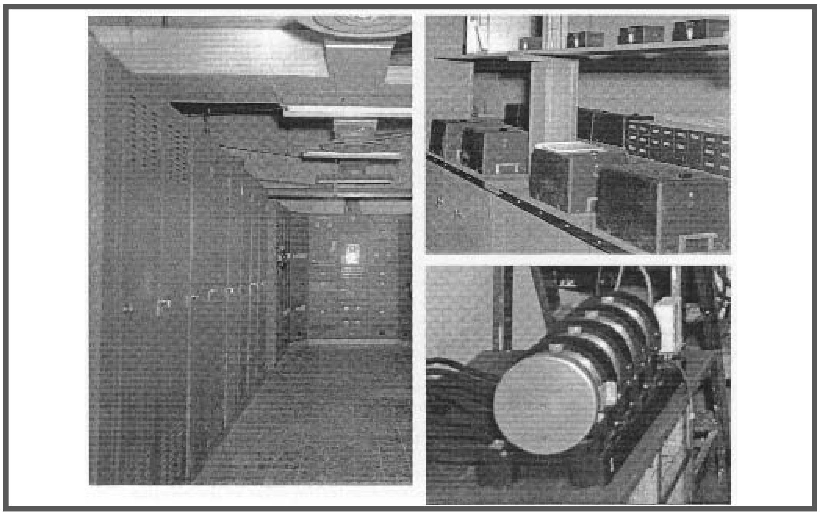
SIGSALY
(Photo from The Green Hornet, Donald Mehl)



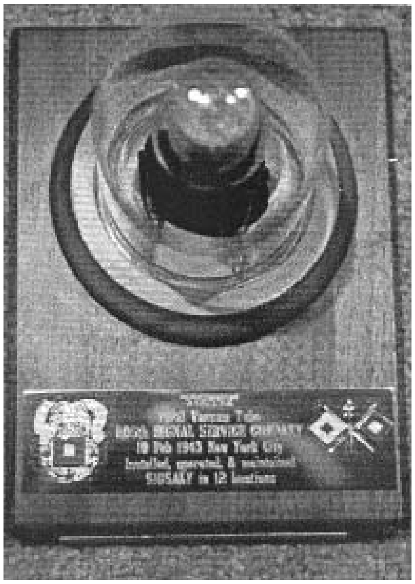
SIGGRUV turntable and disks
(Photo from The Green Hornet, Donald Mehl)



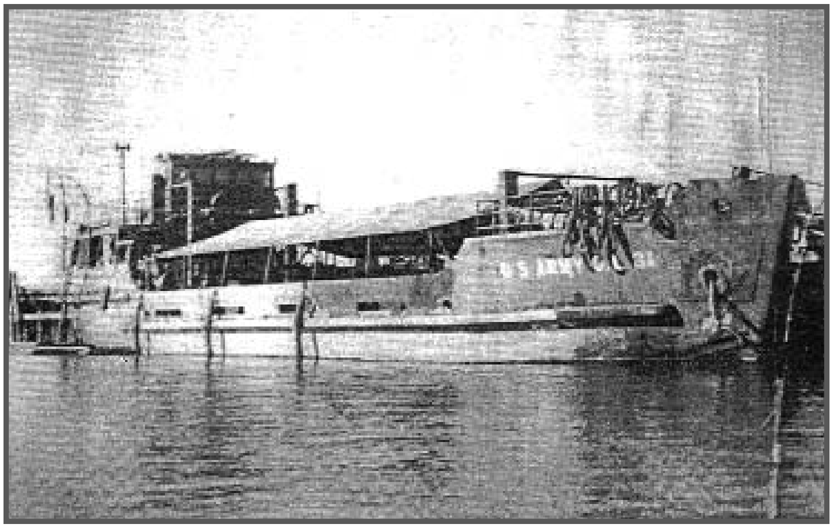
SIGSALY network
(Photo from The Green Hornet, Donald Mehl)



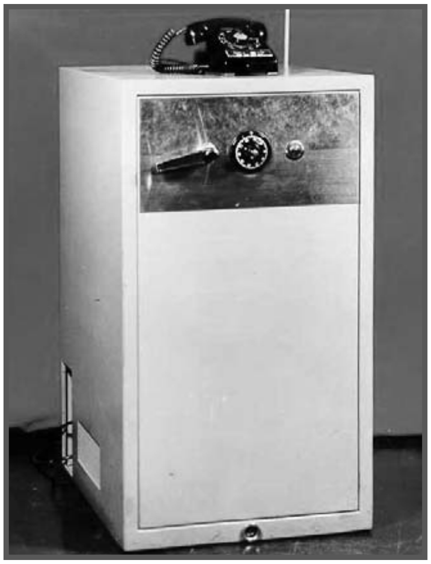
SIGBUSE
(Photo from The Green Hornet, Donald Mehl)


2051 Vacuum Tube
805th SIGNAL SERVICE COMPANY
10 Feb 1943 New York City
Installed, operated, & maintained
SIGSALY in 12 locations

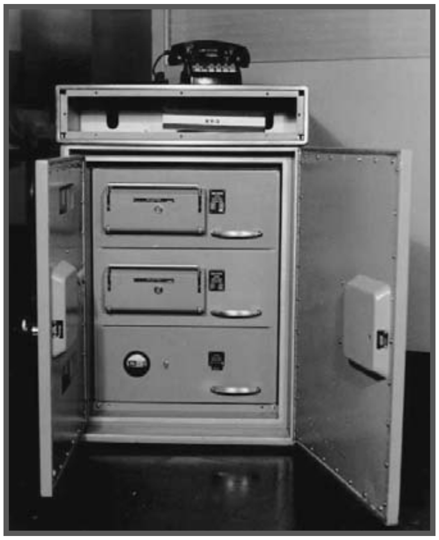
2051 Stepper
(Photo from The Green Hornet, Donald Mehl)



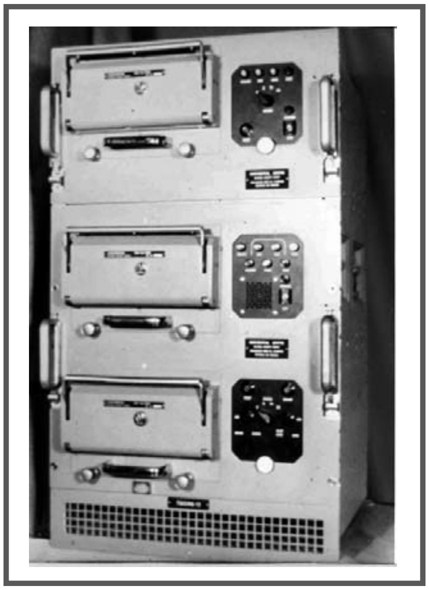
OL-31 barge (Photo from The Green Hornet, Donald Mehl)



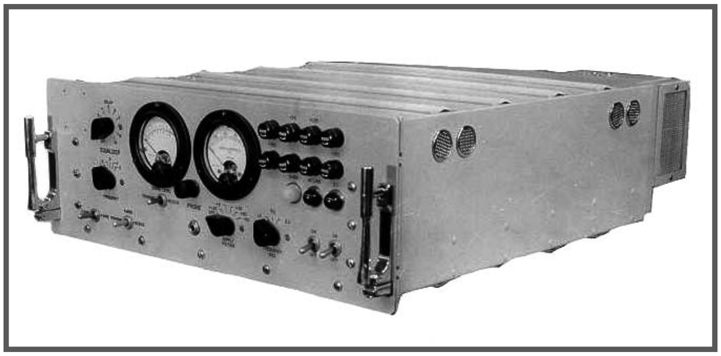
KY-9
(Photo courtesy of National Security Agency)



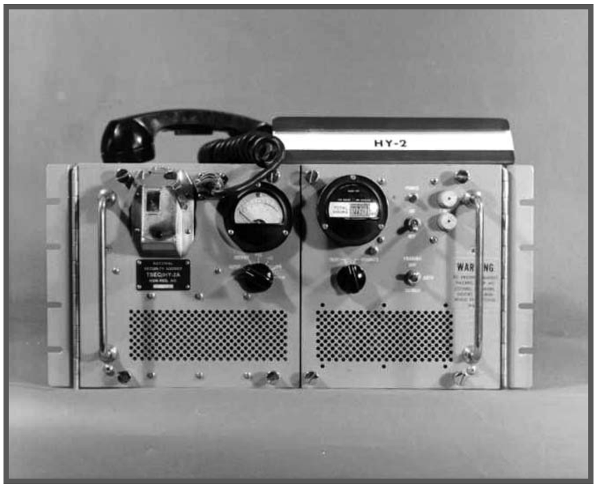
KY-3
(Photo courtesy of National Security Agency)



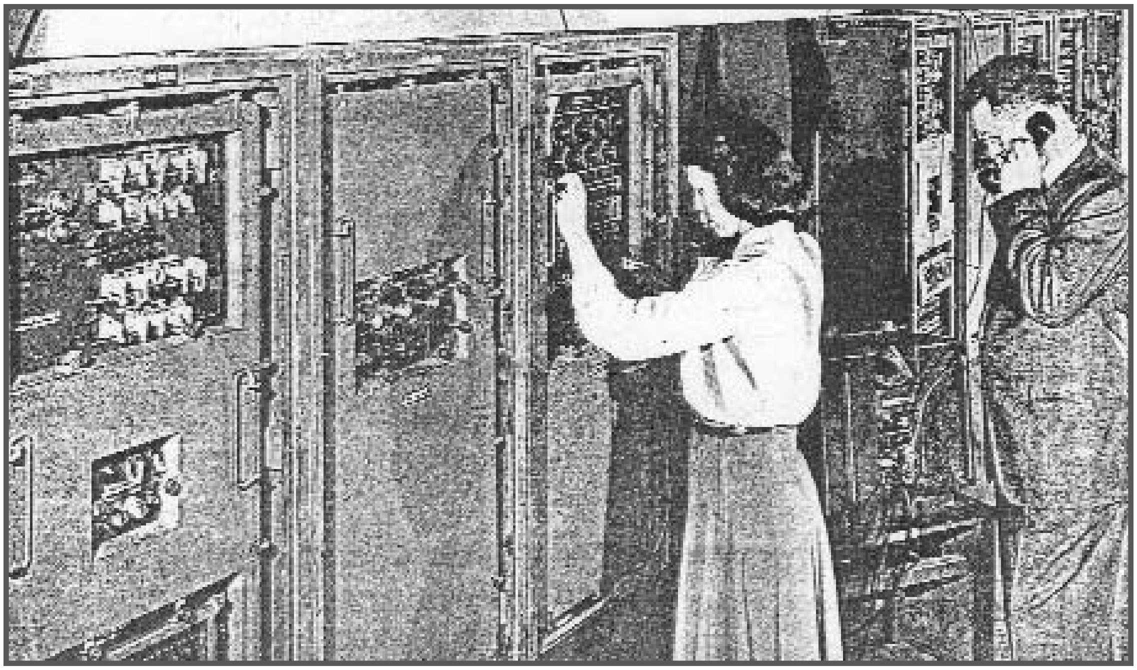
KG-13 (Photo courtesy of National Security Agency)



HN-6
(Photo courtesy of National Security Agency)

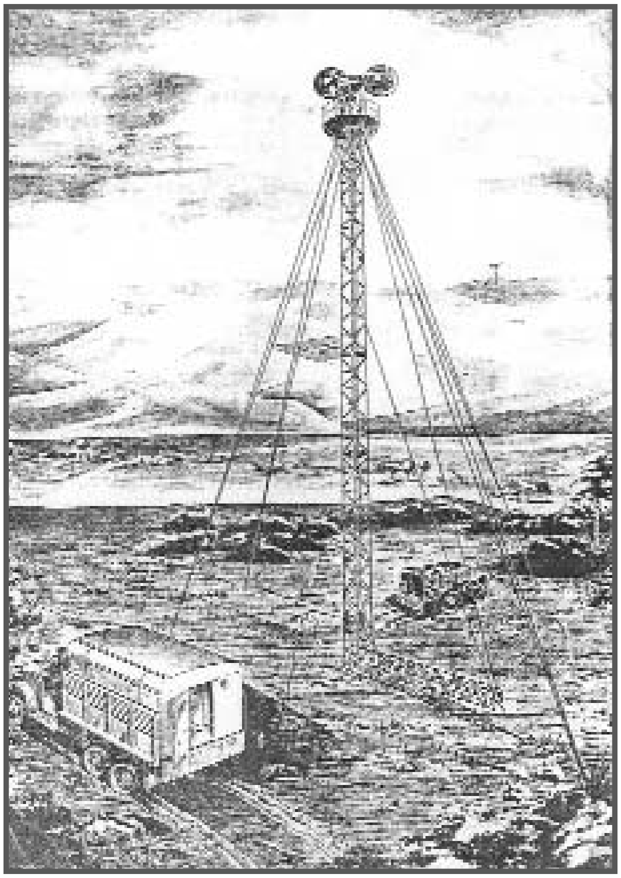


HY-2
(Photo courtesy of National Security Agency)



AN/TRC-6 (Photo courtesy of Bell Lab Record)

AN/TRC-6 (Drawing courtesy of Bell Lab Record)



and key production facilities were operated and maintained by the 81 officers and 275 enlisted men of 805th Signal Service Company with a small complement of Bell Labs personnel. The dedication and know-how of the 805th Signal Service Company kept SIGSALY availability extremely high under difficult wartime conditions. In his book *The Green Hornet*, Donald Mehl describes travails of SIGSALY on the OL-31 barge that followed General MacArthur on his island-hopping campaign from Australia to Manila to the Japanese surrender on Tokyo Bay (See photo on p. 87). The total program cost over its service life – R/D, procurement, training and Operation/ Maintenance (O/M) – was estimated to be $28M.

SIGSALY Decommissioning/Disposition

In February 1946 Major Luichinger submitted the results of his study and recommendations concerning the discontinuance of Overseas Secure Telephone Service to his boss, General Stoner, chief of Army Communication Service. In it he reported that in the last three months of 1945 operational SIGSALY traffic showed a continuing downward trend – Frankfurt averaging less than one call per day, which represented about 50 percent of the total. He recommended that all ETO terminals except Frankfurt and Berlin be terminated; only the Tokyo terminal on OL-31 barge was to remain operational.

Contrary to other claims made for it, SIGSALY did not use Pulse Code Modulation (PCM) or Spread Spectrum modulation as they are currently defined. (See Appendix D.)

On 13 August 1946 General Stoner, now the Assistant Chief Signal officer, in a memorandum to the Director of Intelligence, addressed Major Luichinger's report regarding the storage and destruction of SIGSALY and associated equipment. In summary it directed that

a) All equipment be returned to the ZI
b) Six overseas terminals, one key production facility (SIGSOBS), be destroyed
c) Six be stored as war reserves in the ZI with two SIGSOBS and Off Premises Systems

The report stated that "Upon their return in the fall 1946 SIGSALY terminals were to be transferred to the Army Security Agency until the state of the art permitted a replacement system."

Other World War II Ciphony Systems

As the first SIGSALY equipments were rolling off the Western Electric production line in 1943, the Bell Lab researchers were redesigning it. They subsequently developed "Junior X" (AN/GSQ-2,3), which occupied six five-foot bays. It used miniature vacuum tubes, serial vice a parallel architecture, and a key generator in lieu of a one-time key. In the fall of 1944, the Signal Corps contracted for GSQ-2,3 production with delivery set for March of 1946, too late for WWII service. (Figure 5)

Also during the later stages of the war, BTL built and tested a multichannel Line-of-Sight (LOS) radiotelephone system (AN/TRC-6) for the Signal Corps. It saw only limited service in Europe as the first binary coded speech transmission system (analog *Pulse Position Modulation (PPM)*).

As an engineering accomplishment, SIGSALY was in a class by itself, especially if one considers the sheer magnitude of BTL/Western Electric starting from scratch to deliver the first operational terminals in thirty months. From a technology standpoint, SIGSALY had many operational "firsts":

- The first to use digital *speech compression*
- The first modem to use digital FM rather than binary (FSK)

- The first to extract and record digital (senary) key from a noise source
- The first to use a nonbinary Vernam encryption algorithm
- The first to store and distribute digital key on phonograph records
- The first to use *Protected Wireline Distribution* (*OPEPS*)

A few days after the war ended, the War Department renamed the Signals Security Agency (nee Signal Security Service nee Signal Intelligence Service) the Army Security Agency, placing it under Army Intelligence Staff (G-2) instead of being subordinate to the Office of the Chief Signal Officer (OCSIGO).

Passing the Gauntlet

Army Security Agency's mission remained the same as the S. I. S.: codebreaking and codemaking, COMINT and *COMSEC*. Under the latter a small contingent was established to conduct R/D on future voice and data systems while an operational group continued to produce and distribute keying material, certify system security, issue operating doctrine, and handle equipment procurement.

Future strategic ciphony R/D followed two distinct paths: *wideband* for local nets and narrowband for transit over voice grade channels and fixed plant military networks. Clarence Wright, a Signal Corps veteran, headed ciphony R/D until leaving for industry in 1949. Mitford M. Matthews, Jr. led Secure Telecommunications Equipment Development (STED) from 1949 until 1962 when he was named director of the NSA R/D. During his tenure in STED, he was instrumental in shaping the direction of the ciphony development. Working on ciphony under him was William Erskine and later Mahlon Doyle on cryptography; Fred Buck, narrowband systems; Harvey Solee, strategic wideband systems; William King on wideband tactical systems; and Edward Enriquez on transmission engineering.

The challenges confronting this fledgling group in furthering ciphony engineering and science from its SIGSALY crucible at Bell Labs were

a) **Authentication**: Improve digital narrowband speech processing performance to achieve positive speaker recognition.

b) **Ubiquity**: Lead industrial base and academe in digital telephony and modem standards such that wherever the PSTN could go ciphony could go.

c) **Architecture**: Improve crypto-algorithms, key management/distribution methodologies and promote user-friendly security doctrine for civil and military applications.

d) **Network architecture**: Develop methods needed for various operational venues and performance margins.

e) **Affordability**: Develop the technologies and designs that keep acquisition and O&M costs low and system availability high.

f) **Staffing**: Supplementing WWII Signal Corps veterans with fresh college graduates.

Less than one percent of the phones in the national sector were secure by 1974 – "Major COMSEC Challenge: Secure Voice" Cryptologic Systems, Fall 1973, Carl Brown.

Commercial interest in ciphony, with its prohibitive comparative cost and the threat of DoD patent secrecy orders, discouraged competitors. Much like AT&T with telephony, NSA had a virtual monopoly on strategic ciphony. It developed and procured the equipment; issued operating doctrine and keying material; and trained operational personnel from the national security community. Policy guidance, derived from the National Security Council (NSC) and the U. S. Communication Security Board (USCSB), was carried out by NSA under the secretary of defense, U. S. COMSEC executive agent. While USCSB clearly directed that classified telephone conversations be secure, user budget priorities precluded all but top-level civilian and military users access to secure telephones. NSA was instrumental in defining the course of postwar communication architecture from the predominately analog networks to ones that could more readily support digital transmission.

The first postwar strategic operational ciphony system was the AFSAY-816, based on the AN/TRC-6 radio. NSA modified the WWII security modulator (AN/TRA-16) to provide link encryption for eight channels of virtually toll-quality digital speech between two secure enclaves (*SCIF*) in the Washington area. Each speech channel in the AFSAY-816 was converted to five-bit (32-level) PCM, time-division multiplexed before being bulk encrypted at 320 kbits/sec (Figure 6).

In the Washington area, wideband ciphony became the system of choice for high-level DoD, intelligence community, and National Command Authority (NCA) users. Both from within or between physically secure enclaves, individual users wanted toll-quality end-to-end speech encryption, i.e., ciphony at their desks. That amounted to "ciphony in a safe" vice SIGSALY where the user went to the "tank" (SCIF) to participate in a telephone conference.

Herbert Hoover was the first U.S. president to have a telephone installed at his White House desk. – "A Major COMSEC Challenge: Secure Voice," Carl Brown, 1974

STED engineers developed on-line toll-quality codecs and streaming key generators for wideband ciphony. But the very high reoccurring operating expense limited it to short-range applications. The STED transmission engineering branch in conjunction with engineers from C&P, the local "Baby Bell," tested C&P's cable plant for short-haul digital performance. They found that unloaded 19 AWG cable would support 50kb/s binary data for up to twenty-six miles. (A forerunner of sorts of the current *DSL*). NSA arranged for a special tariff for these lines from C&P in the mid-1950s, thus launching a common holder ciphony service in Washington, D.C., and nearby Virginia.

The initial network served the White House, State Department, the Pentagon, and CIA Langley, and residences of senior government officials. The terminal, TSEC/KY-1, was "push-to-talk," not universally accepted by civilian subscribers. Housed in a three-combination safe cabinet (though not desktop – it was desk-side), the KY-1 converted the speech to a one-bit binary code (DSM) at a modulation rate of 50kb/s (Figure 7). Its modem converted the modulo2 encrypted speech directly to the line as "pluses" and "minuses," *diphase* modulation, a form of digital phase-shift modulation (one cycle of 50kHz for a "one" and negative cycle for a "zero").

The TSEC/KY-3, a more robust solid-state desk-side terminal, was developed as a replacement for the KY-1 in the late 1950s. The KY-3, a 6-bit PCM codec, was designed for transit over PSTN, replacing twelve analog voice channels. A milestone at that time was to design an integrated full-duplex network of KY-3 local area network (LAN) feeding narrowband secure long-haul trunks. Ciphony for the wide area network trunk (WAN) consisted of separately packaged components: codec (TSEC/HY-2), additive key stream generator (TSEC/KG-13) and voice frequency wireline modem (TSEC/HN-6), thus providing a more economical worldwide network. As seen in Figure 8, there were two drawbacks in this approach: the signal had to be in the clear at the LAN to WAN interface; therefore, the communication center had to be a SCIF. In addition, the output voice quality suffered, having been subjected to two cipher-to-plain conversions. *DCA* adapted this scheme for *AUTOSEVOCOM* architecture in the mid-sixties.

The KY-9 narrowband equivalent, the KY-3, was specified to be a transistorized desk-side terminal fully compatible with the PSTN. Bell Labs was awarded a contract for its development in the mid-1950s. Its design consisted of an eight-channel vocoder at 1,667 bit/sec, and it used a vestigal sideband modem (VSB) patterned after the BTL Air Force SAGE modem. The daily key was changed by a punched card. Calls were placed in the clear and switched by the users to activate the encryption in a push-to-talk mode. The modem worked reasonably well over the PSTN and the Autosevocom (Figure 8).

President Kennedy used the KY-9 in a conversation with General Norstad in Paris on October 26, 1962. Notes from that conversation are as follows:

> **....if the Russians will halt missile activity in Cuba we would be prepared to discuss NATO problems with the Russians. He felt that we would not be in a position to offer any trade for several days. He did feel that if we could succeed in freezing the situation in Cuba and rendering the strategic missiles inoperable, then we would be in a position to negotiate with the Russians....**

At $40,000 a copy, fewer than 300 KY-9s were produced to provide end-to-end speech secrecy for high-level users in common holder networks.

In the 1960s the Bell System “went” digital with the introduction of the T Carrier, which offered twenty-four-channel intra-city PCM voice at 1.544 megabits per second. NSA saw this as an opportunity to enhance the ubiquity and to reduce tariffs for multichannel ciphony on high-capacity trunks in the Washington metropolitan area. The TSEC/KY-11 provided bulk encryption for those applications. T-1 terminals, *Tempest* modified, were competitively bid, thus negating STED’s need to develop codecs and modems for intra-city toll-quality telephone secrecy. The was the beginning of government-industry “marriages” between COTS digital voice architecture and government encryption.

Thus, in twenty years, the cost, weight, power, and footprint of a single channel narrowband ciphony terminal were reduced by factors of about 25, 13, 190, and 20, respectively (Figure 10). Considerable strides were also made in both voice frequency and wideband ciphony systems performance and in their procurement and O/M costs.

Epilogue

A future article will cover the transitional milestones in science and technology affecting U.S. strategic ciphony development, policy, and operating doctrine:

- narrowband codecs (channel vocoders to LPC)
- modems (static to dynamic)
- cryptography from symmetric to asymmetric
- key distribution (courier to electronic)
- crypto-architecture (common user to end-to-end session keys)
- design philosophy (breadboard hardware to software simulation)
- components (custom SSI to COTS LSI)
- standards (proprietary to shared)
- accessibility (high status to common user)
- policy (from classified national security to government unclassified but sensitive to commercial applications)
- other players in government ciphony, e.g., Dept. of Commerce and NATO

Salient disclosures of crypto-science and mathematics that preceded the Internet telecommunication wave:

- *New York Times* July 3, 1976, headline “Green Hornet Patent Awarded” – a disclosure of BTL patents of the WWII undecipherable speech system (FOIA). “...a precursor to digital speech encoding and a forerunner of present day pulse code modulation.”
- Cryptography in the public domain: Data Encryption Standard (DES), Diffe-Hellman and Rivest Shamir Adelman (RSA) re public key.
- Equities: DIRNSA’s concern on open-source publication of crypto-algorithm research, in American Council on Education (ACE) Report.

Pre-1962 NSA Ciphony Pioneers

Cryptographers: Mahlon Doyle and others

Narrowband CODECS: Fred Buck, Mitchell Brown, and others

System Architecture: Fred Buck, C.R. "Dick" Chiles, Mitford "Mit" Mathews, David Wolfand

Transmission Engineering: Edward Enriquez, Robert "Pete" Peterson, Wallace Bailey, David Bitzer

Wideband CODECS: Bob Manry, Harvey Solee, Bill Ike, Milan Pavich, Bill Brandenstein

Acknowledgments:

A tip of the hat to Robert Price for the deft and responsive e-mail dialogues on SIGSALY, in particular on Appendix D. Mahlon Doyle, Donald Mehl, David Kemper and David Kahn and Dorothy Madsen, (Lt. Col. USAR Ret), for their review. Many, many thanks to Lula Greenwood and Stephanie Shea for composing, to Barry Carleen for editing, to Bob Morelli for patent searches, to Danny Wilson and Rowena Clough for their reference searches. Also to David Hatch and Robert Hanyok for guiding me through the NSA and NARA archives and to Colonel William Williams, for his assistance on the Mandatory Declassification Review (MDR) reports on ciphony incorporated in this monograph.

Appendix A
Glossary

AUTOMATIC SECURE VOICE COMMUNICATIONS NETWORK (AUTOSEVOCOM): A worldwide, switched, secure voice network developed to fulfill DoD long-haul, secure voice requirements.

BASEBAND: The original band of frequencies produced by a transducer, such as a microphone, telegraph key, or other signal-initiating device, prior to initial modulation. In transmission systems, the baseband signal is usually used to modulate a carrier.

BIT: Abbreviation for binary digit. 1) A character used to represent one of the two digits in the numeration system with a base of two, and only two, possible states of a physical entity or system. 2) A unit of information equal to one binary decision or the designation of one of two possible and equally likely states of anything used to store or convey information.

BAUD: 1) A unit of modulation rate. Note: One baud corresponds to a rate of one unit interval per second, where the modulation rate is expressed as the reciprocal of the duration in seconds of the shortest unit interval. 2) A unit of signaling speed equal to the number of discrete signal conditions, variations, or events per second. Note 1: If the duration of the unit interval is 20 milliseconds, the signaling speed is 50 bauds. If the signal transmitted during each unit interval can take on any one of n discrete states, the bit rate is equal to the rate in baud times log 2 n. The technique used to encode the allowable signal states may be any combination of amplitude, frequency, or phase modulation, but it cannot use a further time-division multiplexing technique to subdivide the unit intervals into multiple subintervals. In some signaling systems, non-information-carrying signals may be inserted to facilitate synchronization, e.g., in certain forms of binary modulation coding, there is a forced inversion of the signal state at the center of the bit interval. In these cases, the synchronization signals are included in the calculation of the rate in bauds but not in the computation of bit rate. Note 2: Baud is sometimes used as a synonym for bit-per-second. This usage is deprecated.

CHANNEL DERIVATION: A technique whereby many channels may be derived from a single channel by compression, e.g., through bandwidth or time sharing.

CIPHER: Any cryptographic system in which arbitrary symbols, or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both.

CIPHONY: Process of enciphering audio information, resulting in encrypted speech.

CODE: System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. NOTE: Codes may or may not provide security. Common uses include (a) converting information into a form suitable for communications or encryption, (b) reducing the length of time required to transmit information, c) describing the instructions which control the operation of a computer, and (d) converting plain text to meaningless combinations of letters or numbers and vice versa.

CODEC: Acronym for coder-decoder. A circuit that converts analog signals to digital code and vice versa.

COMMON HOLDER NET: All subscribers have the same crypto-variable.

COMMUNICATIONS SECURITY (COMSEC): Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. NOTE: Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

C&P: Chesapeake and Potomac, a former "Baby Bell."

CRYPTOGRAPHY: Principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

DIPHASE: Digital modulation scheme where "ones" are one phase of the modulation rate and "zeros" the opposite phase.

DSL: Digital Subscriber Line

ENCIPHER: Convert plain text to equivalent cipher text by means of a cipher.

FULL-DUPLEX (FDX) CIRCUIT: A circuit that permits simultaneous transmission in both directions.

HIGH FREQUENCY (HF): Frequencies from 3 MHz to 30 MHz

INDEPENDENT-SIDEBAND ISB TRANSMISSION: Double-sideband transmission in which the information carried by each sideband is different. Note: The carrier may be suppressed.

JARGON CODES: A hybrid language used to code speech.

KEY: Information (usually a sequence of random or pseudo-random binary digits) used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter-countermeasures patterns (e.g., frequency hopping or *spread spectrum*), or for producing other key. NOTE: "Key" has replaced the terms "variable," "key(ing) variable," and "cryptovariable."

MODULATION INDEX: In frequency modulation approximately the ratio of the frequency deviation to the modulating frequency.

NATIONAL SECURITY ESTABLISHMENT: National Security Council, Intelligence Community and DoD civilian and military officials.

NOISE MASKING: A technique where a high-level noise is added to the speech signal. The technical difficulties in removing the noise become too great to make it operationally practical over radio channels.

NOMENCLATOR: An encryption system that relies on a combination ciphers alphabet and codes to use.

PITCH: The fundamental frequency of the speaker.

PROTECTED DISTRIBUTION SYSTEM: Wireline or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

PULSE-AMPLITUDE MODULATION (PAM): Modulation in which the amplitude of individual, regularly spaced pulses in a pulse train is varied in accordance with some characteristic of the modulating signal. Note: The amplitude of the amplitude-modulated pulses conveys the information.

PULSE POSITION (PPM): Modulation in which the temporal positions of the pulses are varied in accordance with some characteristic of the modulating signal.

QUANTIZATION LEVEL: In the quantization process, the discrete value assigned to a particular subrange of the analog signal being quantized.

SCIF: Sensitive Compartmented Information Facility

SENARY: Having six things or parts.

SPECTRUM CHANNELS: Band of frequencies to be analyzed or synthesized.

SPEECH COMPRESSION: A technique of coding speech where its output bandwidth is less than its input bandwidth.

SPREAD SPECTRUM: A form of modulation where the carrier is unpredictable, the bandwidth of the carrier is much wider than the bandwidth of the information, and detection is accomplished by cross-correlation with a replica of the carrier.

STEPPER: In SIGSALY, a circuit which converts an analog signal into six discrete levels.

SUBSTITUTION: A substitution cipher is one in which each code group is substituted for another code group.

TELEGRAPHY: A form of telecommunication for the transmission of written matter by the use of a signal code.

TELEPHONE SCRAMBLING: A noncryptographic method of making speech unintelligible to an eavesdropper.

TELEPHONE SECURITY: See Communication Security

TEMPEST: An unclassified short name for investigations and studies of compromising emanations.

TRANSPOSITION: A cipher where the plain text code groups remain the same, but their order is scrambled.

VERNAM: Inventor of modulo2 encryption algorithm.

VOCODER: Voice coder for speech compression

WIDEBAND: In telephony, the property of a circuit that has a bandwidth greater than 4 kHz

Appendix B

ACRONYMS and ABBREVIATIONS

ACE: American Council on Education

ACS: Army Communication Service

AUTOSEVOCOM: Automatic Secure Voice Communications Network

COMSEC: Communications security

COTS: Commercial Off-the-Shelf

DCA: Defense Communication Agency

DCM: Delta Code Modulation

ISM: Independent Sideband Modulation

LAN: Local Area Network

LPC: Linear Predicative Code

LSI: Large-Scale Integration

NARA: National Archives and Records Addministration

NSC: National Security Council

NSDM: National Security Decision Memorandum

OPEPS: Off Premise Extension Privacy System

POTS: Plain Old Telephone System

PPM: Pulse Position Modulation

PSTN: Public Switched Telephone Network

SAGE: Semi-automatic Ground Environment

SCIF: Sensitive Compartmented Information Facility

SIGINT: Signals intelligence

SIS: Signals Intelligence Service

SSI: Small-Scale Integration

USCSB: U.S. Communications Security Board

VSB: Vestigial Side Band

WAN: Wide Area Network

Appendix C

Figures

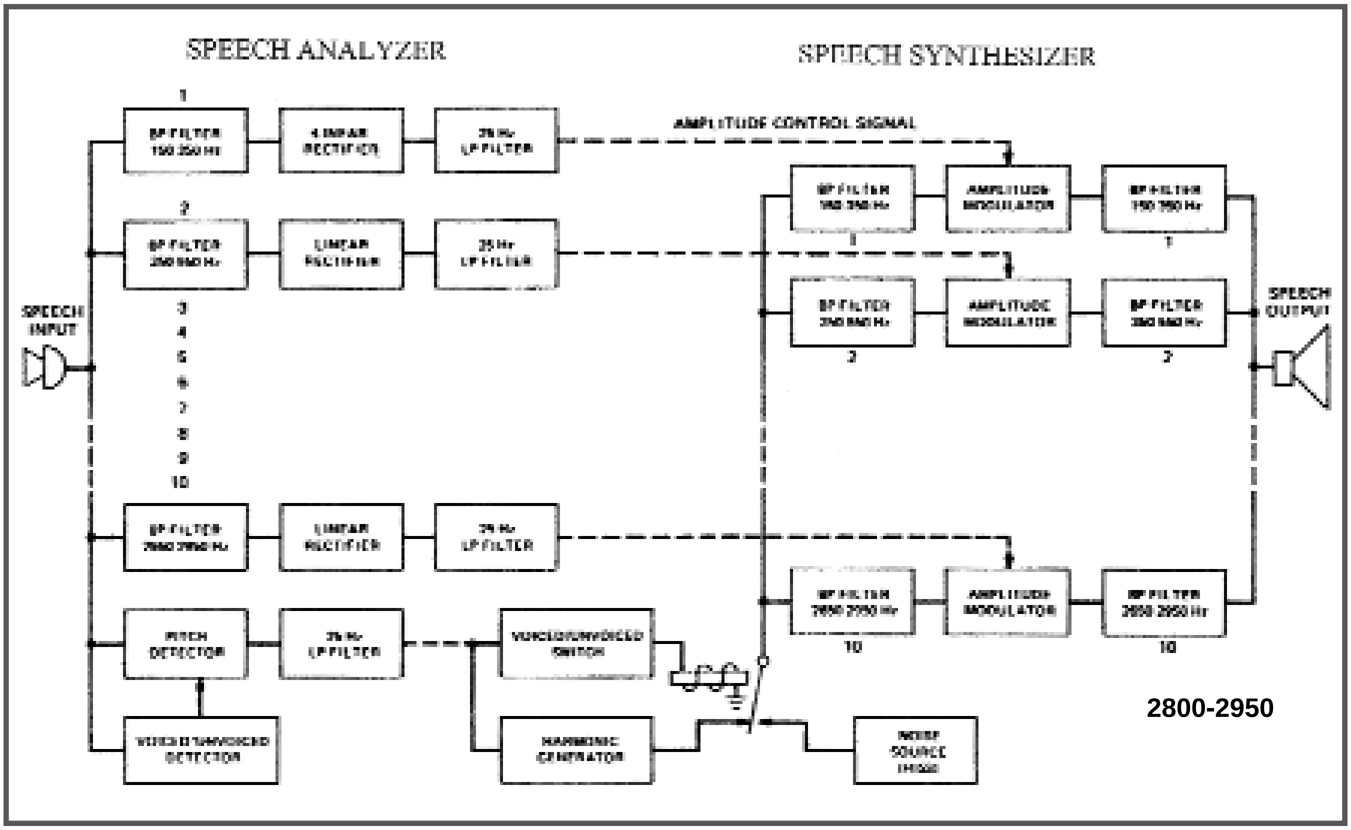


Fig. 1. Vocoder block diagram
(From A History of Engineering and Science in the Bell System 1925-1975,
M. D. Fagen Editor, 1978)

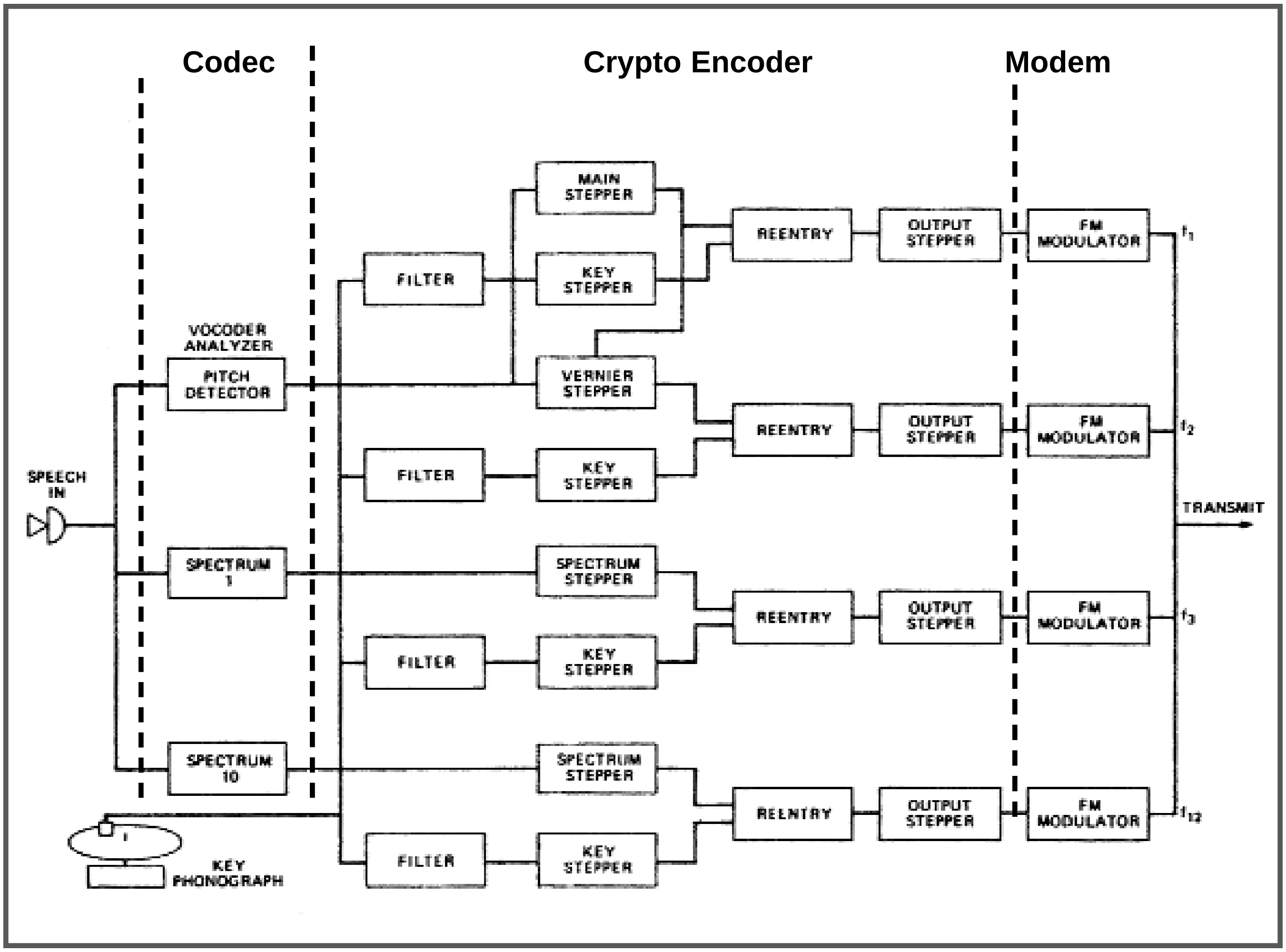


Fig. 2. X System Transmitter
(From A History of Engineering and Science in the Bell System 1925-1975,
M. D. Fagen, Editor, 1978)

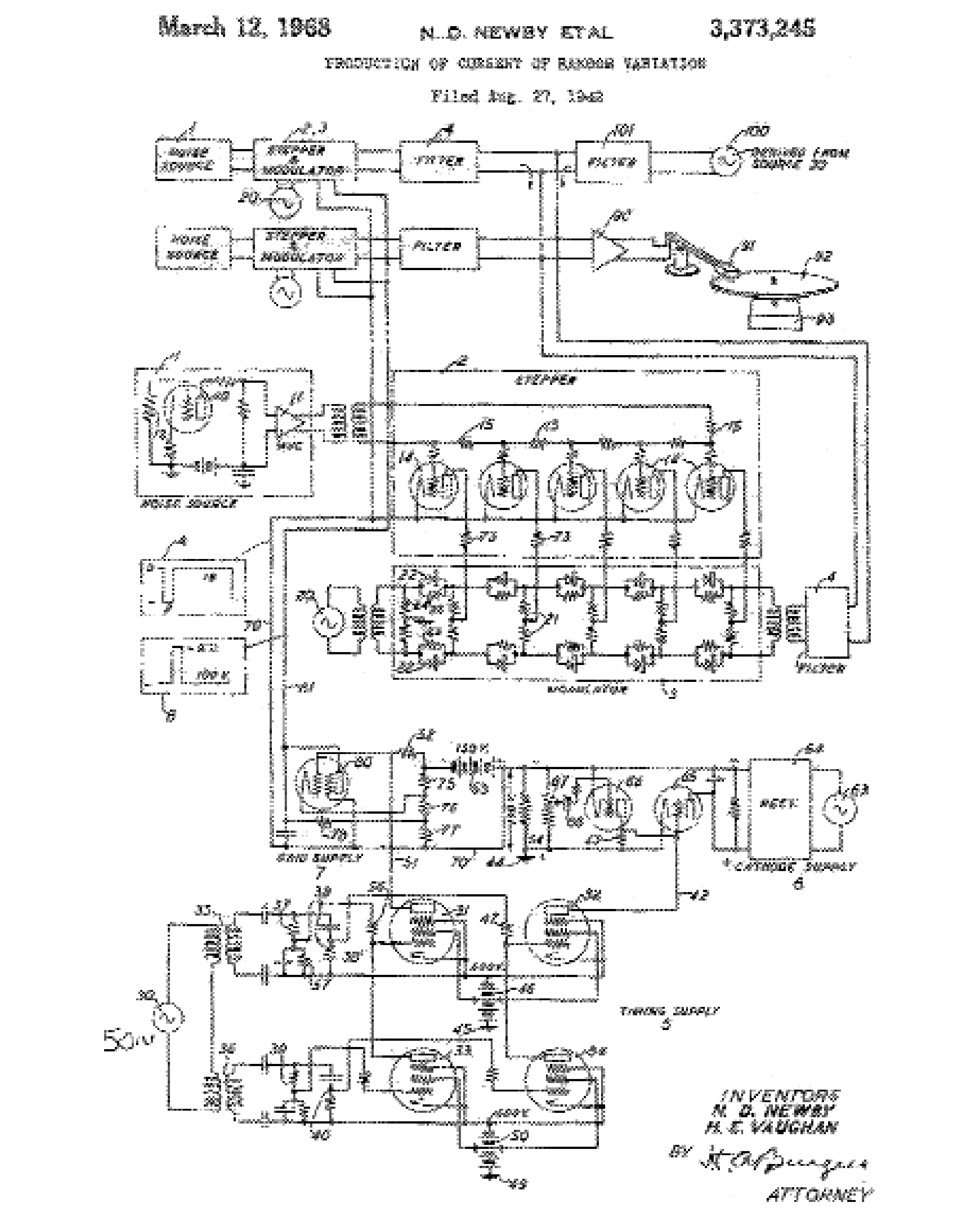


Fig. 3. The basis of SIGGRUV

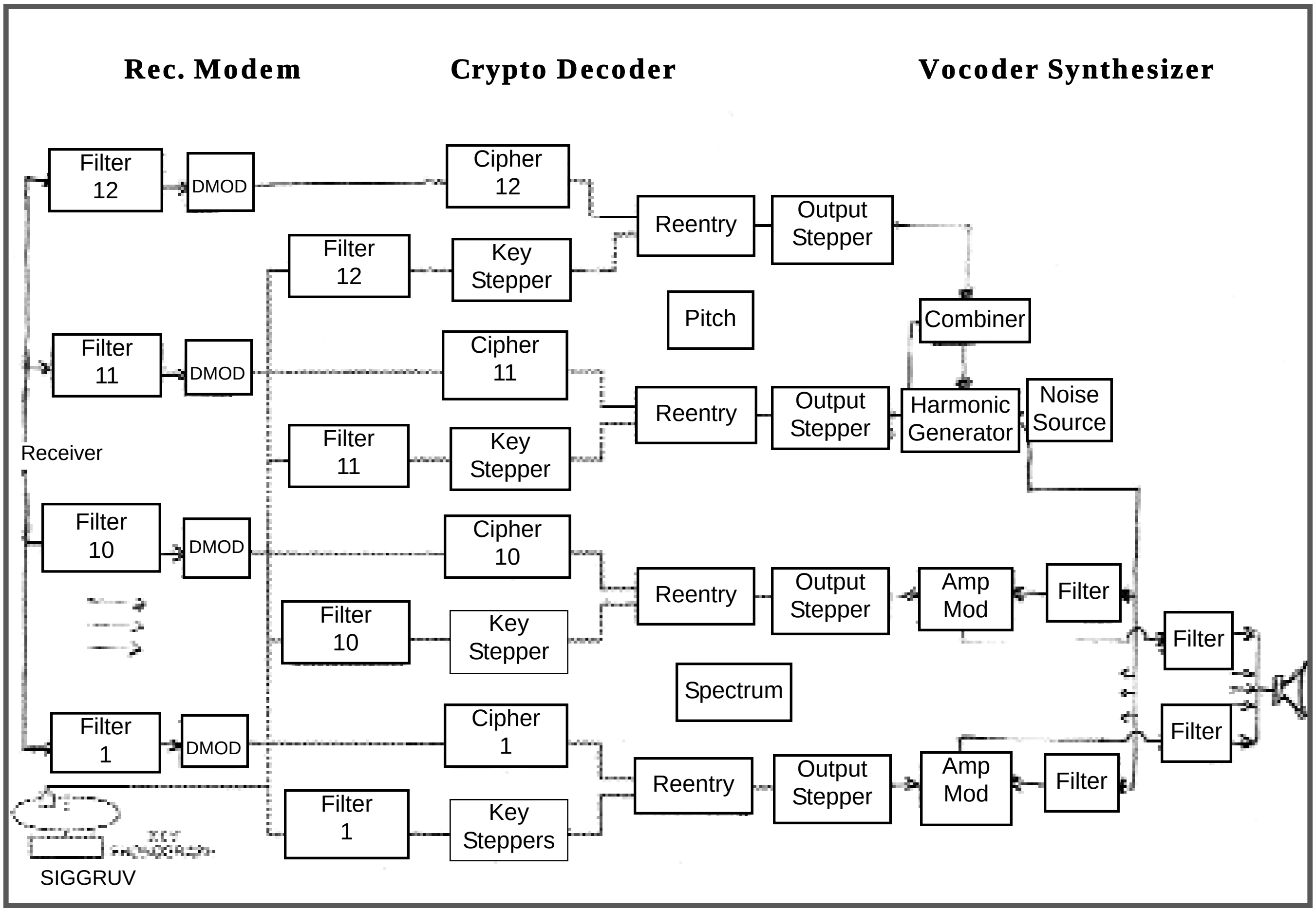


Fig. 4. X System receiver
(From A History of Engineering and Science in the Bell System 1925-1975,
M. D. Fagen Editor, 1978)

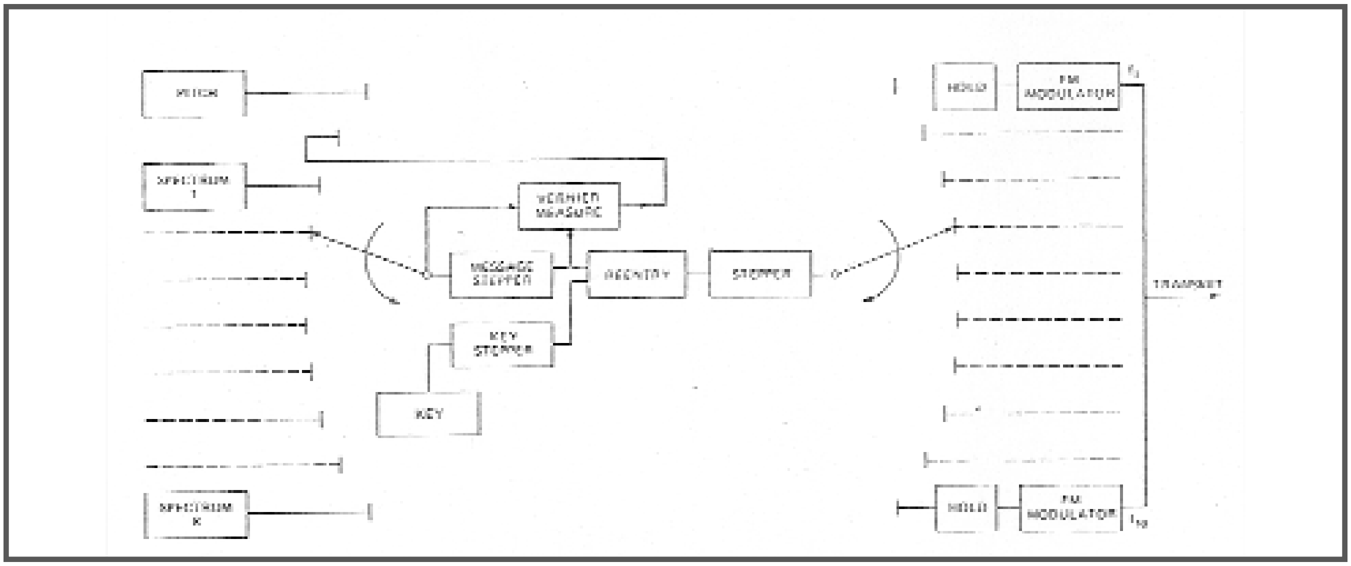


Fig. 5. AN/GSQ-2, 3
(From A History of Engineering and Science in the Bell System 1925-1975,
M. D. Fagen Editor, 1978)

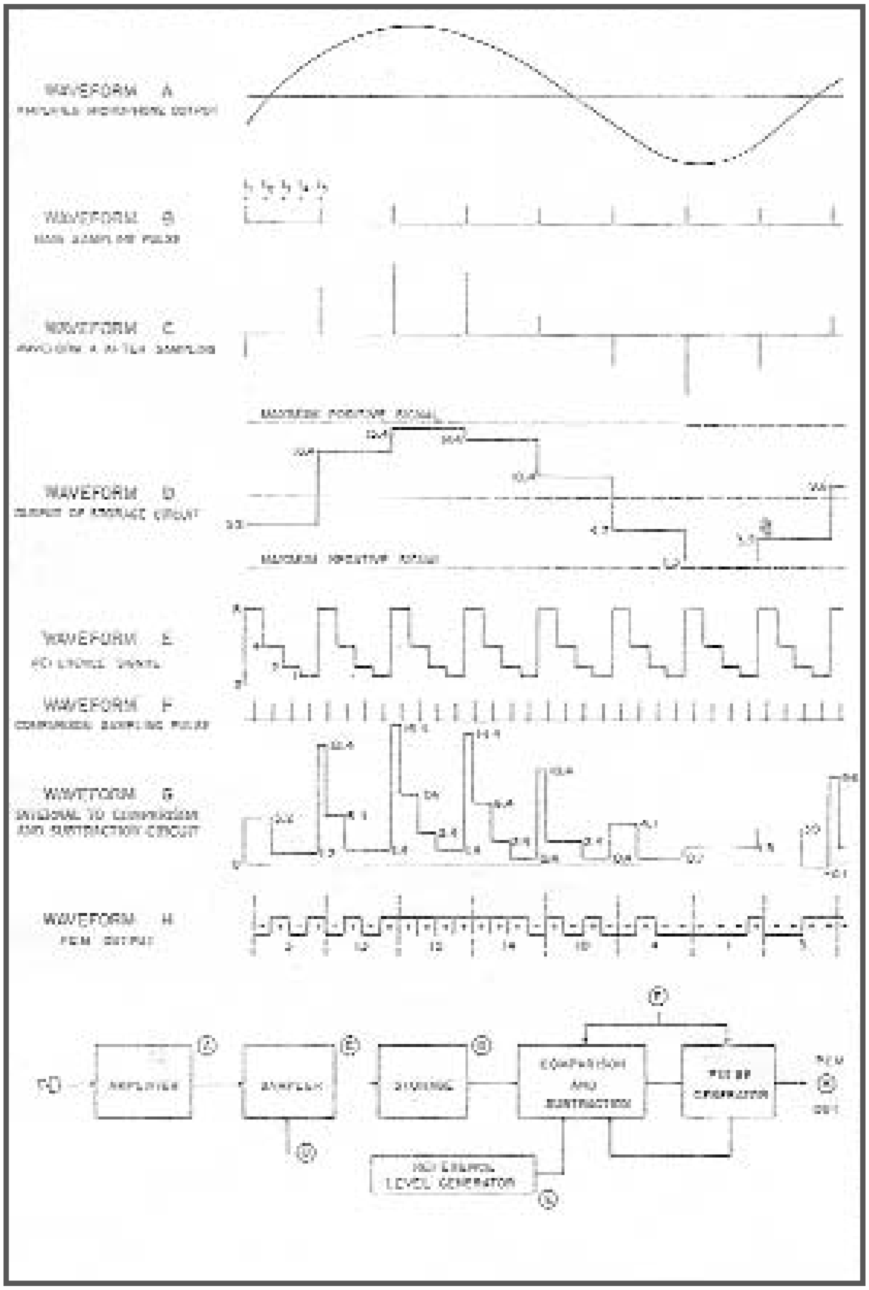


Fig. 6. PCM Decoder
(From “The ABC of Ciphony,” Fred E. Buck, NSA Technical Journal, July 1956)

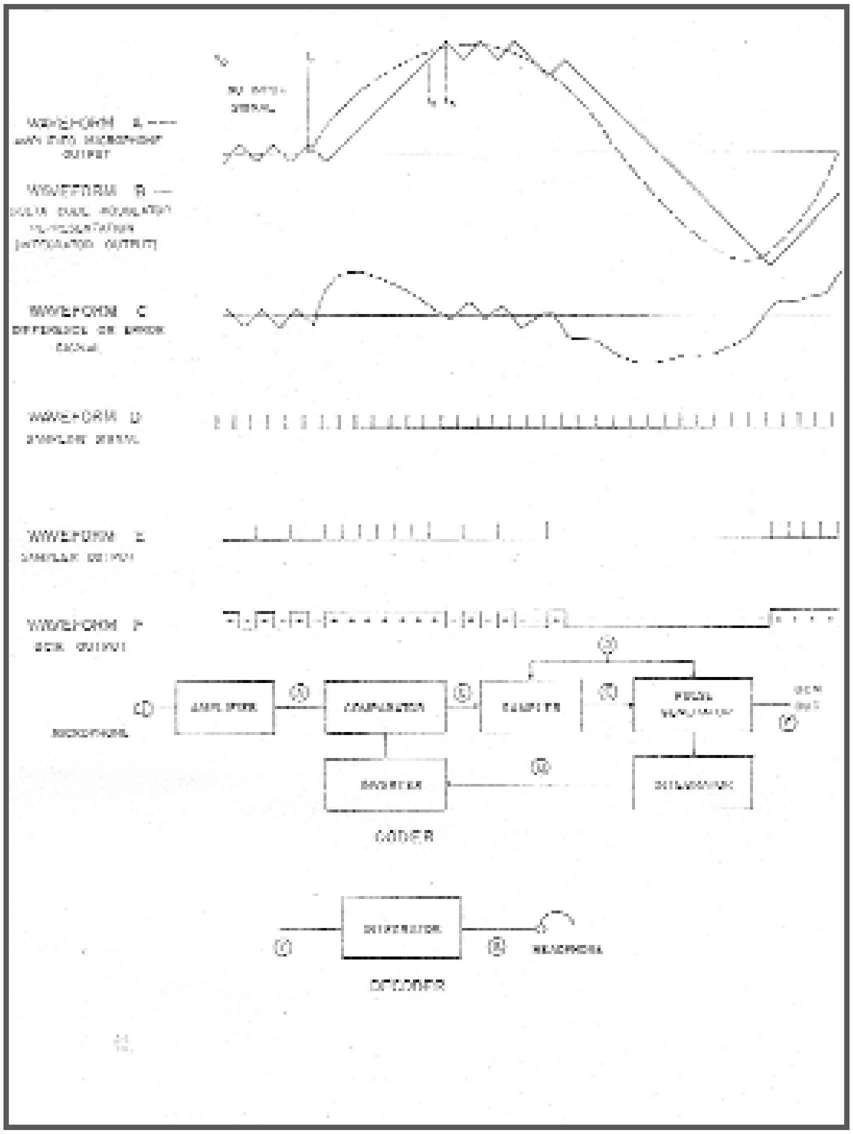


Fig. 7. DCM
(From "The ABC of Ciphony," Fred E. Buck, NSA Technical Journal, July 1956)

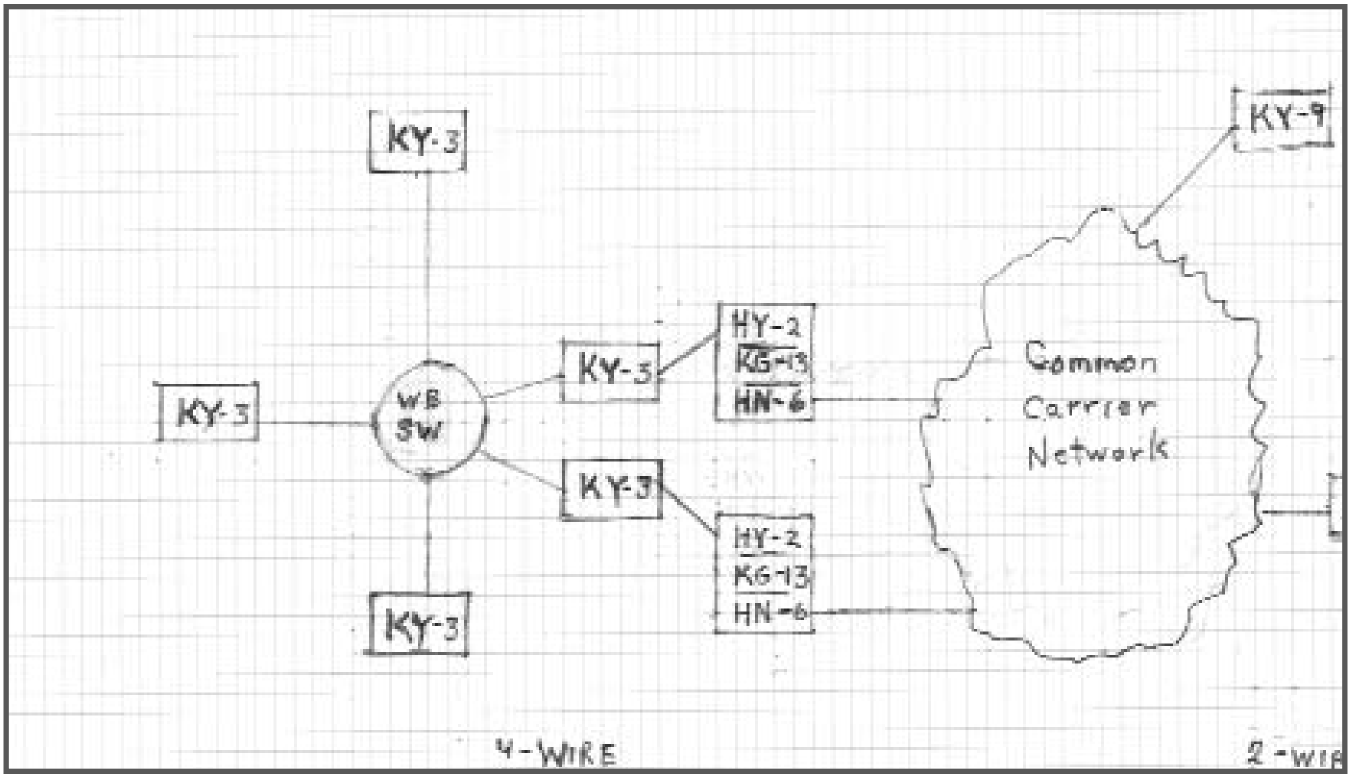


Fig. 8. Hybrid Architecture

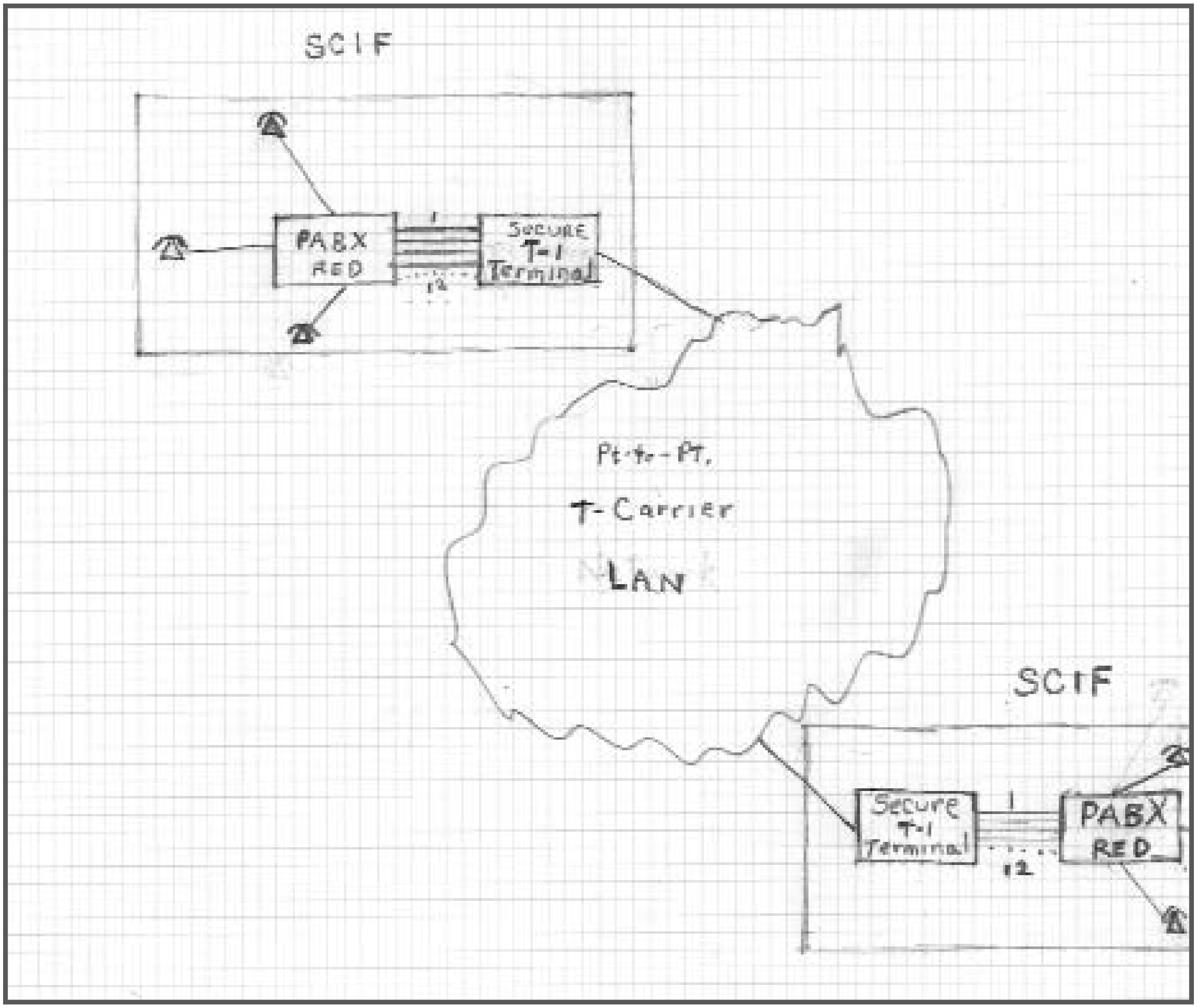
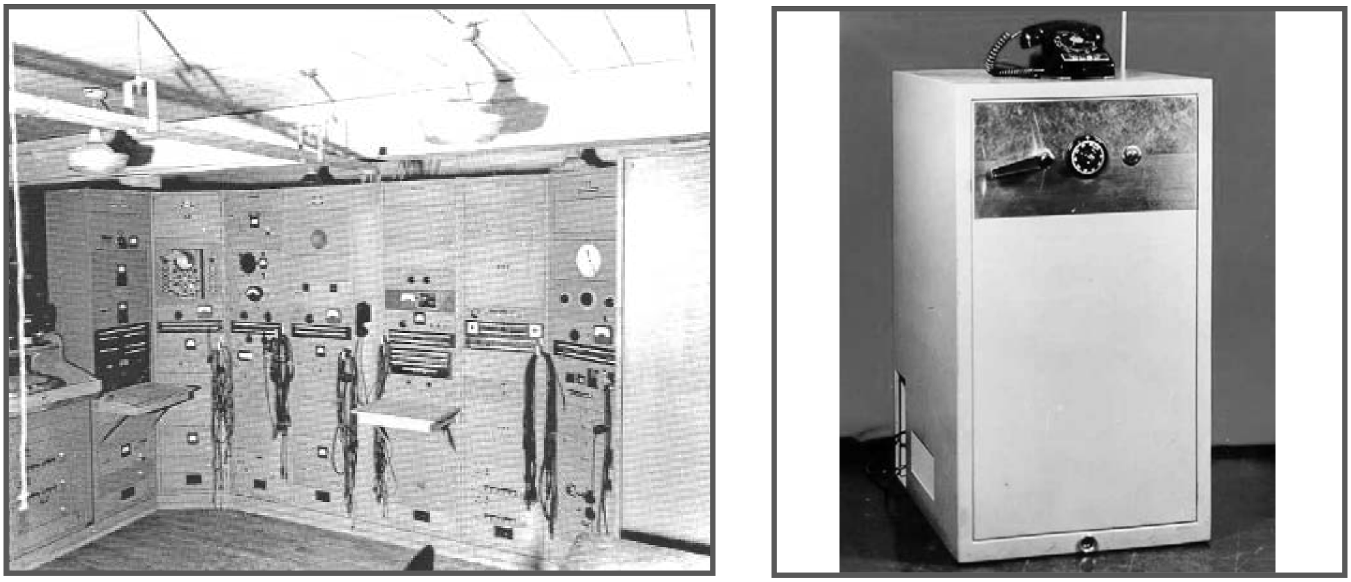


Fig. 9. Secure T-Carrier



SIGSALY

TSEC KY-9

Fig. 10. Narrowband ciphony – twenty-year comparison (SIGSALY vs. KY-9)
(Courtesy of National Security Agency)

World War II - 1943		**Cuban Missile Crisis – 1962**
22H x 19W x 25D x 30	Footprint	42 7/8H x 23 1/4W x 30 3/4D
37 tons (uncrated)	Weight	565 pounds (uncrated)
30kw	Power	160 watts
$1 million	Cost	$40,000

Appendix D
SIGSALY "Firsts"

Following the July 3, 1976, *New York Times* disclosure of the X-System's (aka SIGSALY) existence, brought about by a FOIA which lifted the secrecy orders on BTL wartime patents, a concatenation of articles began appearing in the technical literature on its attributes. First and foremost, in 1983 was "Secret Telephony as a Historical Example of Spread–Spectrum Communication" by W.R. Bennett.

In it he referred to two seminal papers: "A History of Engineering and Science in the Bell System..." and R. A. Scholtz's 1982 IEEE paper on spread spectrum communications. After comparing the technical features of the X-System with concepts of spread spectrum from Scholtz, W.R. Bennett states:

> **If we consider Scholtz's three basic signal characteristics ...1) random or pseudorandom wide-band carrier, 2) carrier bandwidth wider than data bandwidth, 3) detection by cross correlation, the X-System is not included. However, if we take the broader definition of spread spectrum as any transmission method where utilizing a wider band than is occupied by the signal itself the X-System belongs and is, in fact, one of the earliest successful applications.**

By Scholtz's criteria SIGSALY, admittedly, is not spread spectrum; by the same token neither does it qualify by Bennett's definition. Achieving a wider band than that of the signal itself does not of itself satisfy the performance attributes of a spread spectrum communication system. Furthermore, SIGSALY incorporates an unusual but a rather conventional FDM/mFSK modem consisting of subcarriers spaced on 170Hz centers. At its 50 baud per channel, the deviation rate or *modulation index* is less than two, hardly enough to satisfy Bennett's own criteria for spread spectrum.

Broadcast FM (multiplicity factor > 20) is vulnerable to jamming principally because it does not embody correlation detection, as is the case with SIGSALY, whereas the Army's F9C, which conformed to Scholtz's three fundamental principles, provided over 20 db of protection against deliberate interference. The fact that the vocoder compressed the speech by a factor of 10, the transmitted signal is expanded to the equivalent modulation rate of 1,548 b/s. (# channels x # samples/sec per channels x log 2 (#amplitude per channel) due to digitization. The line signal provides less protection against a jammer than a binary multichannel FSK.

Bennett characterizes the SIGSALY speech coding as requiring

> **...sampling, quantizing and coding, a combination which was later called pulse code modulation (PCM). Since PCM expands bandwidth the telephone channel could not carry the resulting enciphered signal. The availability of the vocoder..... enabled the problem to be solved. PCM could be applied to the vocoder channels without increasing their total bandwidth...**

In the Bell System history, the SIGSALY (Appendix E) notes that vocoder channels were sampled at twenty millisecond intervals and were quantized to six levels (senary). The Bell Lab researchers described it as a form of PCM, not PCM per se as it is currently defined.

PCM is a digital scheme for transmitting analog data. The signals in PCM are binary; that is, there are only two possible states, represented by logic 1 (high) and logic 0 (low). This is true no matter how complex the analog waveform happens to be. Using PCM, it is possible to digitize all forms of analog data, including full-motion video, voices, music....

Sources

Bell Telephone Publications

"A Mathematical Theory of Communication," C. E. Shannon, *The Bell System Technical Journal*, July 1948

"Another Long Distance "First" *Long Lines*, Vol. 25 #8, 1946

"AN/TRC-6 – A Microwave Relay System," H. S. Black, *Bell Laboratories Record*, Dec. 1945

"Communication Theory of Secrecy Systems," C. E. Shannon, *The Bell System Technical Journal*, October 1949

"Spectra of Quantized Signals," W. R. Bennett, *The Bell System Technical Journal*, July 1974

Books

A Brief History of Cryptology, J. V. Boone, 2005

A History of Engineering and Science in the Bell System 1925-1975, M. D. Fagen, Editor, 1978

Alan Turing, The Enigma, Andrew Hodges, Simon & Schuster, 1983

A World War II WAC's Memoir: My Journey to the Pentagon's Top Secret Command Center, Dorothy Madsen (Lt. Col., USAR, Ret) to be published

Frequency Analysis Modulation and Noise, Goldman, 1948

Information and Secrecy, Colin Burke, 1994

The Codebreakers, David Kahn, 1967

The Green Hornet, Donald Mehl, 1997

IEEE, AIEE, I.R.E.

"Certain Topics in Telegraph Transmission Theory," H. Nyquist, *Transactions* , AIEE, 1927

"Cryptology and the Origins of Spread Spectrum," David Kahn, *Spectrum*, 1984

"Further Notes and Anecdotes on Spread Spectrum Origins," Robert Price, *IEEE Transactions on Communications*, Vol. COM-31, No. 1, January 1983

"Secret Telephony as a Historical Example of Spread-Spectrum Communication," William R. Bennett. *IEEE Transactions on Communications*, Vol. COM-30, No. 1, January 1983

"The Origins of Spread Spectrum Communications," Robert A. Scholtz, *IEEE Transactions on Communications*, Vol. COM-30, No. 5, May 1982

"The Philosophy of PCM," B.M. Oliver, J.R. Pierce, C.E. Shannon. *IRE,* November 1948.

"The 25th Anniversary of Pulse Code Modulation," Deloraine and Reeves, *Spectrum*, May 1965

National Archives and Records Administration

NSC Executive Committee Meeting No. 8, October 27, 1962

RG 111, Office of the Chief Signal Officer

RG 227, National Security Agency

RG 457, National Defense Research Committee

SIGSALY Speech Encipherment System RC-220-T1 Technical Manual Vol. A. Bell Telephone Laboratories School for War Training, NARA DECLASSIFIED 5/11/96

National Security Agency

"A History of Secure Voice Coding: Insights Drawn from the Career of One of the Earliest Practitioners of the Art of Speech Coding," Joseph Campbell and Richard Dean, 1993

"A Major COMSEC Challenge: Secure Voice," Carl Brown, *Cryptologic Systems*, 1974

"Data Transmission over Telephone Circuits," Melville H. Klein, *NSA Technical Journal*, 1958

"Narrow-Band Speech Security," Mitford M. Matthews, *NSA Technical Journal*, December 1958

Seventh Lecture: Ciphony Equipment and other Specialized Systems, David Boak, 1973

"Speech and Facsimile Scrambling and Decoding," Monograph No. 17, 1969

"The ABC of Ciphony," Fred E. Buck, *NSA Technical Journal*, July 1956

"The SIGSALY Story," Patrick Weadon, NSA, 2000

The Start of the Digital Revolution, R.R. Peterson & J. V. Boone, NSA, 2000

The Quest for Cryptologic Centralization and the Establishment of NSA, 1940-1952, NSA, Thomas L. Burns, 2005

National Security Council (NSC)

"NSDM 266 Improved Security of Telecommunications," August 15, 1974

Unpublished Notes

"History of SIGGRUV – The SIGSALY Recording Project," David Kemper, Sept. 1995

(This article was published in 2005.)