Telephone Security

This article presents a history of significant milestones in the development and deployment of high-level telephone security for the US and its UK allies during World War II. 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 US government took to assure telephone secrecy. The challenges enciphered telephony (ciphony) has placed on science and engineering are emphasized over operational history, which is better dealt with by others referenced herein.

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 US 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 scram-

bling had to be done 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 covers the major milestones of strategic telephone secrecy from its World War II genesis at the Bell Telephone Laboratories (BTL).

Bell Telephone Labs: The Crucible of Telephone Secrecy

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.

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).

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 (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, R.C. Mathes, 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 shows a block diagram of the vocoder.) 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.

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

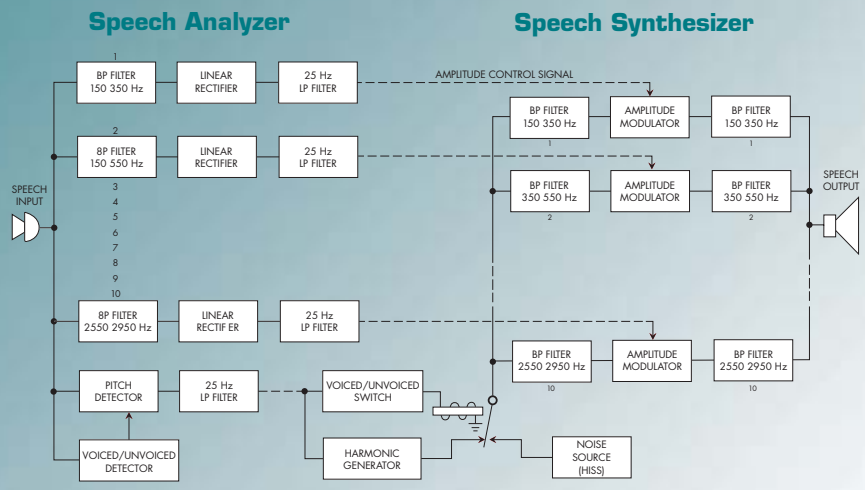

Figure 1: Vocoder (From A History of Engineering and Science in the Bell System, 1925-1975, M.D. Fagen, editor, 1978)

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 shows Vernam's encryption modulo2.) 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.

K \ S	0	1
0	0	1
1	1	0

Table 1: Vernam Algorithm Modulo 2

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. (See Table 2 for the Potter-Nyquist Modulo6 Encryption.) 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.

K \ S	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
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: Modified Vernam Algorithm Modulo 2

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.

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, one stepper for each level, firing at twenty millisecond intervals; the pitch frequency (main and venier) was similarly quantized.

The receiving radio translated and sent the encrypted signal over telephone lines to the distant SIGSALY terminal. The receive terminal separated the twelve enciphered channels, demodulated each channel, and synchronously decrypted with matching keys. The decrypted spectrum channels drove the vocoder synthesizer. Figure 3 shows a logical block diagram of the SIGSALY receiver.

A sixteen-inch record stored prerecorded one-time encryption key (SIGGRUV) that 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: SIGSALY alternate key generation system). It consisted of an array of clattering relays and telephone selector switches controlled by pseudorandom key from M-228 rotor machines (SIGCUM: teletype encipherment system). 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. Though not as secure or reliable as the SIGGRUV, SIGBUSE did not pose

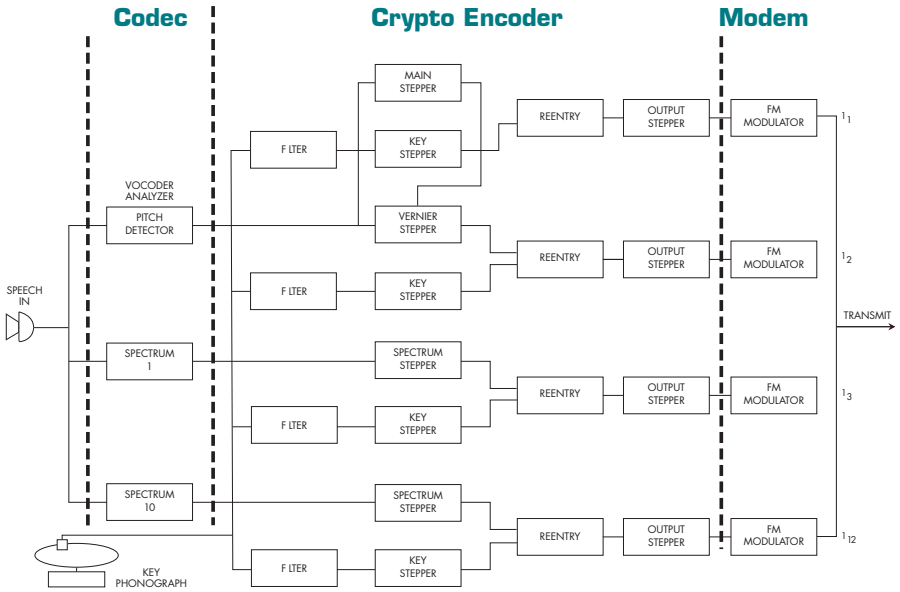

Figure 2: X System transmitter (From A History of Engineering and Science in the Bell System, 1925-1975, M.D. Fagen, editor, 1978)

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 onetime 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. 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: SIGSALY primary key generation system), the Signal Corps was able to manufacture two acetate recordings (SIGJING: acetate key records) 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. See Figure 4 for the patent diagram on which SIGSOBS was based.

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 overall 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.

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 the National Archives and Records Administration files where a Signals Intelligence Service (SIS) or an Army Communications Service (ACS) official had accredited SIGSALY.

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 intratheater, 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 transcripts and secure (SIGTOT: teletype encipherment system) message traffic. Captain Dorothy Madsen wrote a General Staff Circular for eligible users, set up the administrative procedures, and personally edited all transcripts.

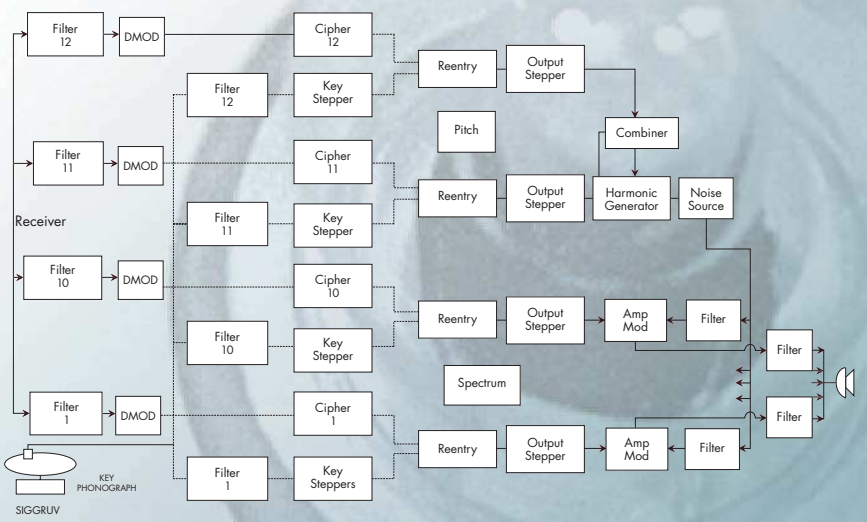

Figure 3: X System receiver (From A History of Engineering and Science in the Bell Sstem, 1925-1975, M.D. Fagen, editor, 1978)

Prime Minister Churchill spoke frequently to many senior officials including President Truman on SIGSALY but ironically FDR never used it.

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 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 the 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. The total program cost over its service life—R/D, procurement, training and Operation/ Maintenance (O/M)—was estimated to be $28M.

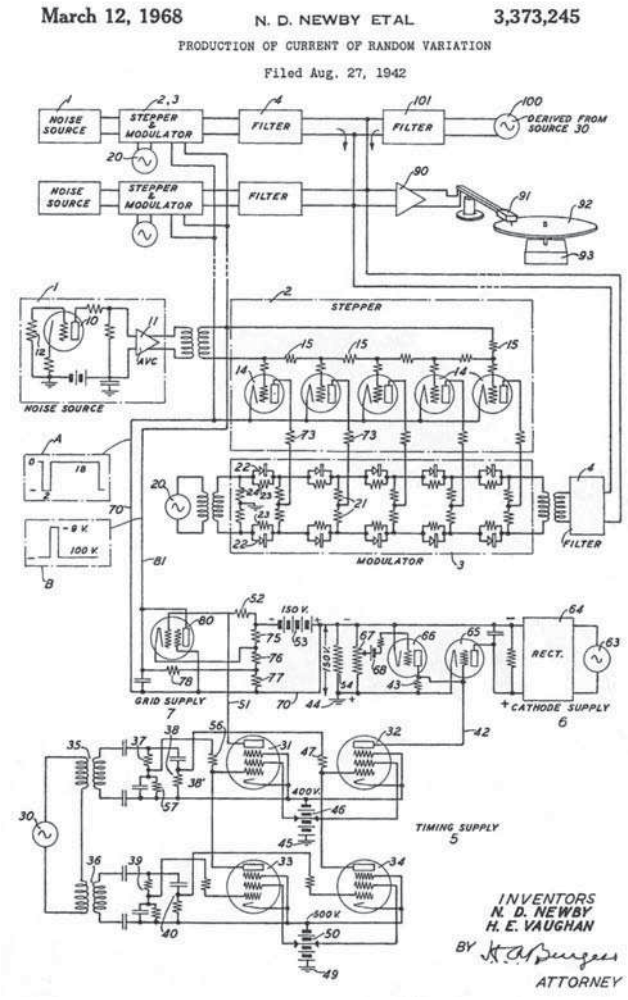

Figure 4: Patent diagram on which SIGSOBS was based.

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 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.

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 Zone of Interior (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. (See Figure 5 for a block diagram of the AN/GSQ-2,3.)

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)).

Prime Minister Churchill spoke frequently to many senior officials including President Truman on SIGSALY but ironically FDR never used it.

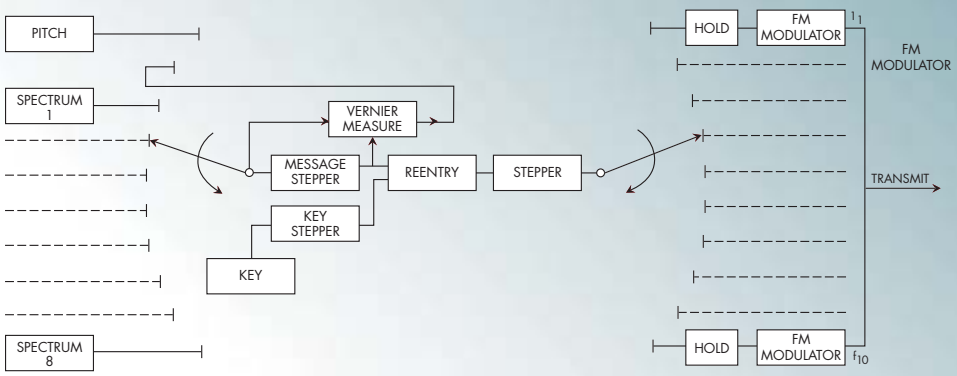

Figure 5: AN/GSQ-3 (From A istiry of Engineering and Science in teh Bell System, 1925-1975, M.D. Fagen, editor, 1978)

Conclusions

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 instead of being subordinate to the Office of the Chief Signal Officer .

Army Security Agency's mission remained the same as the SIS: 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.

References

Bell Telephone Publications

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

"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

Top Secret Communications of WWII—Sigtot, Donald Mehl

AIEE

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

National Archives and Records Administration

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

"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

Unpublished Notes

"A World War II Wac's Memoir: My Journey to the Pentagon's Top Secret Command Center," Preface, [Internet], Dorothy (Meg) Madsen, available at http://www.ww2wac.com/page11 html

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