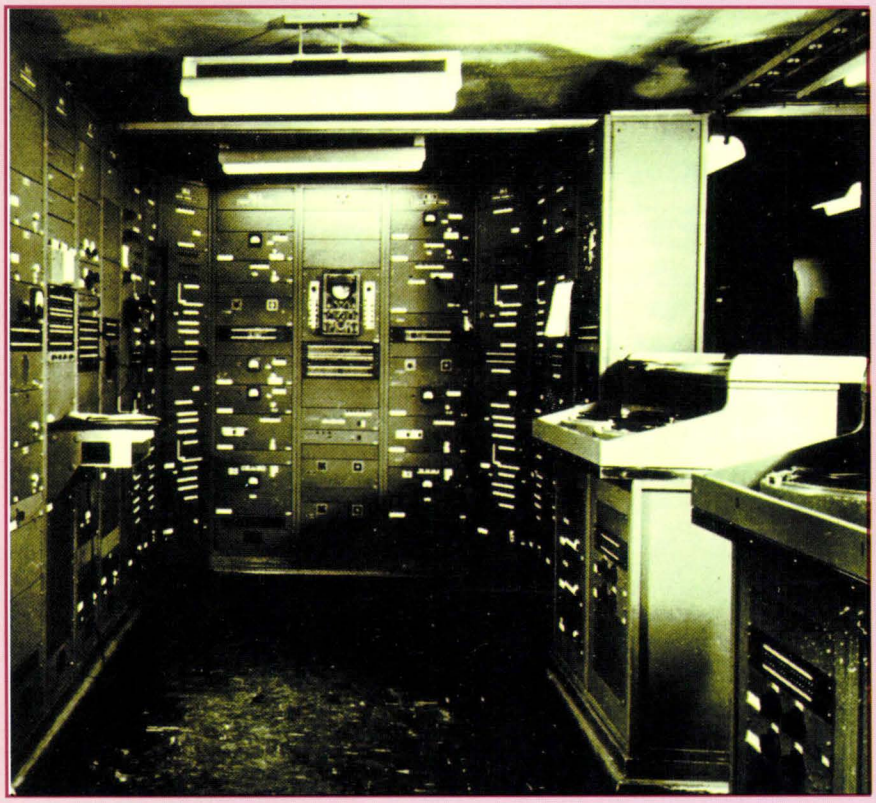
The Start of the Digital Revolution:

SIGSALY

Secure Digital Voice Communications in World War II



Introduction

Today, digital technology is the backbone of our entire information industry. As a part of this, the transformation of audio information into digital signals is now a routine process which is incorporated into our telephone, television, and music equipment (both recorded and live). Digital communication, measurement and data techniques are quite commonplace. This fairly recent situation was enabled by many things including the invention of the transistor in 1947 and the later evolution of semiconductor microelectronics techniques. However, the pioneering work for many of these capabilities was performed early in World War II in a successful effort to provide secure voice communications for high-level government officials. This brochure presents a brief overview of this revolutionary development.[1]

Background and Overview

Before the full involvement of the United States in WWII, the United States and the United Kingdom were using transatlantic high-frequency radio for voice communications between senior leaders. The analog voice privacy system in use, called the "A-3," provided reasonable protection against the casual eavesdropper, but it was vulnerable to anyone with sophisticated unscrambling capability. This system continued to be used during the early part of the war, and government officials were warned that they could be overheard. In fact, it was later discovered that a German station in the Netherlands was breaking out the conversations in real time. This situation was intolerable, but neither the U.S. nor the U.K. had a ready solution.

Fortunately, the technical groundwork for a solution was already in place. About 1936, Bell Telephone Laboratories (BTL) started exploring a technique to transform voice signals into digital data which could then be reconstructed (or synthesized) into intelligible voice. It was called a "vocoder," short for voice coder. An early demonstration of the voice synthesizer portion of the vocoder was even a part of the 1939 World's Fair in New York. The approaching war stimulated the investigation of true voice security. The BTL staff soon discovered that there were about eighty patents issued on the general topic, but analysis indicated that all of the methods were really unsatisfactory from a national security viewpoint. New technology was required. Spurred on by added

interest from the U.K. and some early research results, the vocoder was selected as the basis of a new high-tech voice security system. BTL proceeded on its own to develop this much-needed capability and was soon able to demonstrate it to the satisfaction of the Army. A U. S. Army contract was awarded in 1942 for the production of the first two systems. This system eventually came to be called SIGSALY[2] and was first deployed in 1943.

Fig. 1. The inaugural conference

This conference, on 15 July 1943, marked the official start of SIGSALY service. The encrypted transmissions were between the Pentagon and the London systems. Lt. Gen. J. T. McNarney, deputy chief of staff, USA, is at the head of the table on the right. Dr. O. E. Buckley, president of Bell Telephone Laboratories, is at the left end of the table. Lt. Gen. Brehon Somervell, USA, commanding general, Army Services Forces, is using the phone while others listen on headsets. The London end of the conference was attended by Lt. Gen. J. L. Devers, USA, commanding general, European Theater of Operations, and Maj. Gen. I. H. Edwards, USA, chief of staff, European Theater of Operations, among others.(Photo from the National Archives)

The system was formally put into use on 15 July 1943 in a conference between the Pentagon and London. A photograph of that event is shown in figure 1. As a part of this conference, the president of BTL addressed the participants. His comments, which predicted "far-reaching effects," are contained in Appendix A. Twelve terminals were eventually deployed. Before they were removed from service in 1946, they were to support over 3,000 official secret conferences. The mere existence of the capability to conduct secure voice communications during this period remained secret until 1976.

Development and Deployment

The BTL development group worked under the direction of A. B. Clark (who later led the Research and Development activities of the new National Security Agency from 1954 to 1955) and developed a vocoder-based system which emphasized the preservation of voice quality. They chose a twelve-channel system. Ten of the channels each measured the power of the voice signal in a portion of the total voice frequency spectrum (generally 250-3000 Hz), and two channels were devoted to "pitch" information of the speech as well as whether or not unvoiced (hiss) energy was present. This work was essentially completed in 1942, and patents were filed. Most of the patents would be kept secret until 1976! BTL had invented the fundamentals of digital, encrypted voice,[3] and they had also invented the means to transmit it.[4]

A 1983 review of this remarkable system for the Institute of Electrical and Electronic Engineers (IEEE)[5] attributes no fewer than eight "firsts" to SIGSALY. They are as follows:

1) The first realization of enciphered telephony

2) The first quantized speech transmission

3) The first transmission of speech by Pulse Code Modulation (PCM)

4) The first use of companded PCM

5) The first examples of multilevel Frequency Shift Keying (FSK)

6) The first useful realization of speech bandwidth compression

7) The first use of FSK – FDM (Frequency Shift Keying-Frequency Division Multiplex) as a viable transmission method over a fading medium

8) The first use of a multilevel "eye pattern" to adjust the sampling intervals (a new, and important, instrumentation technique)

The IEEE article also points out that the system can be thought of as being one of the very first successful applications of spread spectrum technology.

An overview of the general scheme for digitizing the voice information and encrypting it is shown in Appendix B. This was a completely new approach to the problem and was based on the extensive communications research then being conducted at BTL.[6]

It is a rare thing indeed to produce a new system with so many unique features. These were not simply "improvements"; they were fundamentally new and absolutely necessary for the system to work. The concepts were proven in the lab, but before the system was ready for final development and deployment, there were several important system features which needed refinement.

Key generation was a major problem. The basic requirements for the key (one essential part of the total encryption system) was that it should be completely random, and must not repeat, but could still be replicated at both the sending and receiving ends of the system.

This was accomplished for SIGSALY by using the output of large (four-inch diameter, fourteen-inch high) mercury-vapor rectifier vacuum tubes to generate wideband thermal noise. This noise power was sampled every twenty milliseconds and the samples then quantized into six levels of equal probability. The level information was converted into channels of a frequency-shift-keyed (FSK) audio tone signal which could then be recorded on the hard vinyl phonograph records of the time.[7]

The FSK signal was recorded on sixteen-inch diameter wax platters which were then transformed into "masters." The masters, which in commercial use would have been used to make thousands of records each, were used to produce only three records of a particular key generation segment. Key distribution, always a

problem, was accomplished by means of transporting and distributing the phonograph records. These records were taken to Arlington Hall Station in Virginia, and the masters were destroyed. Once the systems were deployed, the key-pair was distributed by courier from Arlington Hall to the sending and receiving stations.[8] Each recording provided only twelve minutes of key plus several other functional signals which were necessary for seamless key output.

Later advances in recording technology permitted the simultaneous direct recording of the key on two acetate disks backed by aluminum. This technique reduced drastically the time required to make each record and also reduced cost. Since the keys were changed for every conference and on a regular schedule, there were a very large number of recordings made and distributed under strict controls. The key recordings were destroyed after use.

The system required that the key be used in twenty millisecond segments. Therefore, it was necessary for each record to be kept in synchronism within a few milliseconds for fairly long periods of time (one hour or so). This was accomplished by the use of very precisely driven turntables. The turntables themselves were remarkable machines. Each was driven by a large (about thirty-pound) synchronous electric motor with hundreds of poles. The motor was kept in constant operation, and the power for it was derived directly from dividing down the terminal's frequency standard. The frequency standard was a 100 kHz crystal oscillator. The accuracy of the standard had to be maintained within about one part in ten million so that the system would stay in synchronism for long periods of time. The system frequency standard could be corrected by comparing it to an available national frequency standard (which was WWV in the U.S.).

Since one record held only about twelve minutes of key, it was necessary to have two transmit and two receive turntable subsystems at each terminal. In this way, a transition could be made from one key-pair to another. However, there was another problem: how did the system get started in synchronism?

There were no synchronizing signals passed from one terminal to another. Each terminal was a standalone which depended on its own internal clock referenced to a national time standard. Systems were started at prearranged times. For example, Washington and

London might agree to start at precisely 1200 GMT. Prior to starting, the phonograph pickup was indexed to the first record groove. This process consisted of listening to the pickup output click as it was slid along the edge of the record in order to determine when it fell into the first groove. This was easier with the original hard records than with the softer acetate records.

Once the pickup position was established and the time came to start the session, a clever mechanical device was used to obtain a simultaneous start at both ends of the link. The turntables were attached to the shaft of the synchronous motor by means of a clutch and spring arrangement. At the startup time, the clutch was automatically energized and a pinball type plunger was activated which provided the initial starting motion to the turntable by releasing a spring which then pulled the turntable from its starting position to the same speed and in lock with the rotation of the synchronous motor. All of this enabled the motor to keep its synchronized position. At the end of the process, each turntable would be running at a definite and precise rate, and the key-pair would be synchronized to the accuracy required for operation.

Of course, fine adjustments in relative timing were required. These were made by the use of 50-Hertz phase shifters (Helmholz coils) in the basic power/timing circuitry which drove the turntables. A separate phase shifter could be adjusted by the operator to control the timing within the receiving system to account for the transmission time, which was on the order of 16 milliseconds for a transatlantic circuit. Operators initially established the synchronization by carefully adjusting the phase of the synchronous motor and listening to the quieting in the audio output when the key-pairs were in synchronism. Operators often monitored the quality of the conversations and adjusted the system in a similar manner. The entire synchronization process was complex, but it worked. The turntable-based key-record system was called SIGGRUV when the vinyl records were used and SIGJINGS when the acetate records were used.

There was also a mechanical alternative to the recorded key. This was called Alternate Key, or AK. The AK subsystem consisted of a large number of stepping switches, relays and other devices. It started the key derivation process with a rotor device normally associated with teletype encryption systems. It was a very complex and relatively unreliable system which required constant

maintenance attention. There was also an interesting difference in system operating characteristics between using the recorded key and the AK subsystem.

When the system was using a recorded key and lost synchronization, there was almost always an abrupt and total loss of system capability. When the AK system began to deteriorate, it usually did so in small increments, which resulted in a sound like a horse galloping. In just a few seconds, a small "gallop" developed into a full gallop as the first small error (caused, for example, by a faulty relay contact) was multiplied and propagated throughout the system. AK was used by the system operators mainly for daily maintenance purposes. This subsystem was called SIGBUSE.

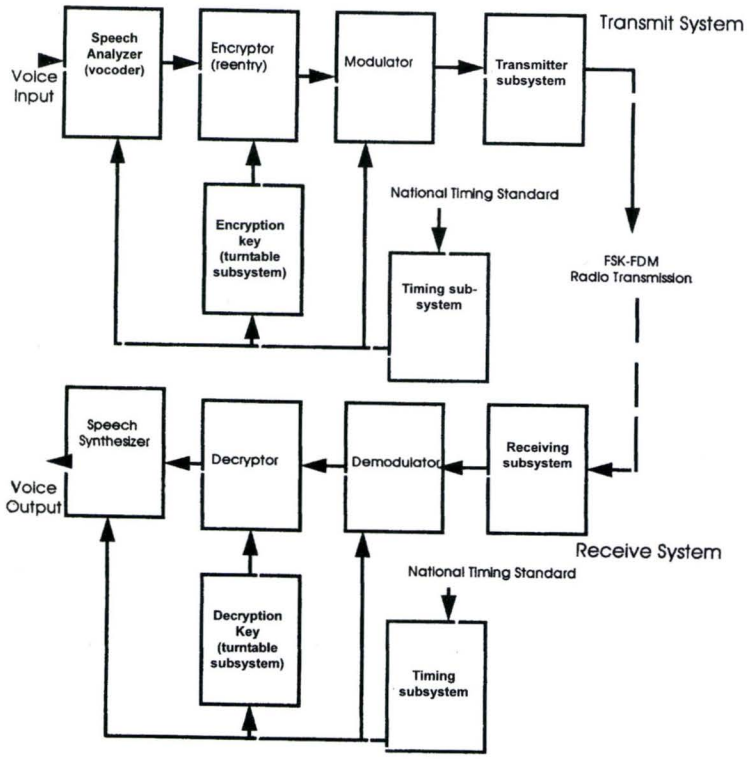


Fig. 2. Overview of the SIGSALY system

A very simplified overview of the total system is shown in figure 2 representing a one-way transmission. Return transmissions used the same key setup.

Each complete SIGSALY terminal consisted of about forty racks of equipment and was very heavy. A portion of a complete system is shown in the photograph in figure 3. Installations were customized to their surroundings, which resulted in a variety of actual physical configurations. Each system contained a large assortment of vacuum tubes,[9] relays, synchronous motors, turntables, and other unique electromechanical equipment. Because of the technology of the time, it also used large amounts of power. Special cooling systems were required to dissipate the heat.

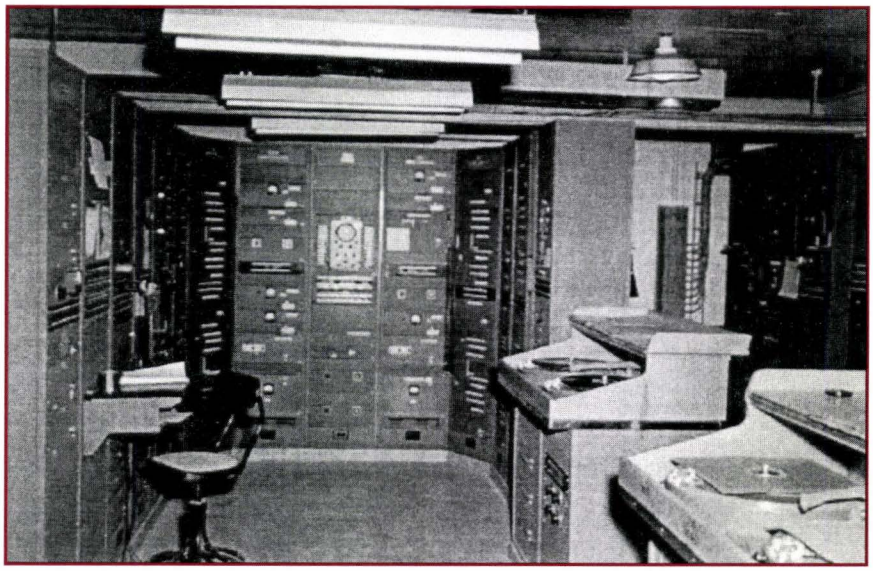


Fig. 3. A SIGSALY installation

Each installation was unique, but this photograph conveys the complexity and size of the system. The phonograph turntables which played the cryptographic key are on the right of the picture. The oscilloscope in the center of the rear rack of equipment had many uses, but, along with an HF radio receiver, was a major tool in the process of assuring that the local system time standard matched the international time signals. The approximate weight of the forty racks of equipment and other materials in a terminal was 55 tons! (Photo from the National Security Agency)

Terminals were eventually established in Washington, D.C., London, Paris, North Africa, Hawaii, Guam, Manila and Australia, among others. In each case, there were installation challenges. Systems were also deployed after the conclusion of the war to other locations, including Berlin, Frankfurt, and Tokyo.

In London, the bulk of the SIGSALY equipment was housed in the basement of an annex to Selfridge's Department Store while the actual instrument used by Churchill and his staff was about a mile away in the War Rooms under the Admiralty Building and near the prime minister's residence at 10 Downing Street. The Washington, D.C., end of the system was installed in the recently completed Pentagon in the summer of 1943. The original installation schedule called for a system to be in the White House itself, but the Pentagon location was chosen to permit the system to be more easily used by senior members of the military (and possibly to give President Roosevelt better control over his own schedule since he would not be interrupted at all hours by callers).

It was very clear from the start that this complex equipment was going to require a specially trained operations and maintenance staff. The Army Signal Corps responded by establishing the 805th Signal Service Company. Special training was provided in a BTL school, and members of the 805th were sent to all SIGSALY locations. The 805th was a very unusual company, to say the least. It consisted of eighty-one officers and two hundred and seventy-five enlisted. The officers were mostly lieutenants and captains, and the enlisted men were technical and master sergeants. This special company had the highest average grade of any company in World War II. A picture of part of the unit assigned to operate the equipment in the I. G. Farben building in Frankfurt, Germany, is in figure 4. Although technically not assigned to the 805th, members of the Women's Army Corps (WACs) performed a wide variety of duties related to SIGSALY including creating stenographic records of many of the important conversations.[10]

The members of the 805th had a challenging task. In addition to the requirements for special security, they had to deal with the complexities of the technology. Western Electric Company specifications were used, and immaculate daily records were kept. The equipment was normally operated for about eight hours a day, and the remaining sixteen were used for maintenance. The large number of vacuum tubes required constant checking. In some

cases they were removed and checked so often that the sockets started to go bad. Maintenance schedules were adapted with experience to avoid such problems, but maintenance remained a challenging job. Power supplies were critical elements in the system and were adjusted using a standard cell and galvanometer system to a probable accuracy of one-tenth of a volt in one hundred and fifty volts. Tens of power supplies were adjusted daily. Ninety-six stepper circuits also needed daily adjustment.

Fig. 4. A few members of the 805th Signal Service Company

At first, BTL provided members of the 805th their training in the system (called the RC-220-T-1) at the BTL School for War Training in New York City. Classes started in January 1943 and continued until the Army took over the training in July 1944. This photograph shows only a few of the members of the 805th and was taken circa 1945 in the I. G. Farben building in Frankfurt, Germany. L to R in the front row are TSgt. Jim Atkinson, Lt. Massey (the 1st C.O. of this unit), Lt. Golliday (the 2nd C. O.), Lt. Mc White, Lt. Chope, and MSgt. Charlie Haas. L to R in the rear row are: Staff Sgt. Fred Buck, TSgt O'Neil, Staff Sgt. Jim Biggerstaff, Staff Sgt. Ed Dessert, Staff Sgt. Frank Zylius and "Willy" Wilchenski. (Photo courtesy of Fred Buck)

Despite all the complexity, the efforts of the 805th, coupled with the fundamentally sound design, made the SIGSALY system operationally effective. There was surprisingly little operational downtime.

Conclusions

The ability to use truly secure voice communications at high organizational levels was a great advantage to the Allies in the conduct of the war and in the critical activities which followed it. Not only was SIGSALY a highly successful secure voice system, but it provided a springboard into the digital communications world. It encouraged the BTL staff and their government counterparts to think more about communications in digital terms rather than in the traditional analog processes.

The rapid development and deployment activities also offer a challenge for present-day members of the cryptologic community. We are all indebted to the development teams in both government and industry as well as to the members of the 805th Signal Service Company and all of the others associated with this remarkable system.

J. V. Boone and R. R. Peterson
July 2000

Notes

1. A much more detailed description of the system, as well as background on its development, deployment and operation, is available in a document entitled *The Green Hornet...America's Unbreakable Code for Secret Telephony*. This study was authored by Donald E. Mehl and was privately published in 1999. Copies are available for study in the library of the National Cryptologic Museum. It contains many diagrams, photographs, references and stories concerning this system. This work is the source of much of the information regarding the deployment of the system as well as some of the technical details which are presented in this short paper.

2. SIGSALY and similar names given to portions of the system are simply "cover" names, not acronyms.

3. Even today, the legalistic and somewhat arcane language used in patent applications is difficult to comprehend. Yet it is interesting to read the patent applications of the late 1930s and early 1940s on this topic. The BTL inventors were establishing a completely new way to transmit voice signals, and they were also inventing the nomenclature at the same time. For example, a portion of the United States Patent 3,967,067, "Secret Telephony," awarded to Ralph K. Potter in 1976 (filed in September 1941) reads as follows (under the heading "what is claimed is"):

> In secret telephony, means to derive from the speech to be sent a plurality of speech-defining signals each indicative of the energy variations with time of a different frequency region of the speech, means to translate each such signal above a certain amplitude into a mark and each such signal below said certain amplitude into a space, an individual key for each signal, consisting of marks and spaces of random occurrence, and means to combine each key with the marks and spaces obtained from an individual one of said signals, to render transmission of the latter marks and spaces secret.

Potter was describing a method of filtering the input speech signal into a set of individual channels, digitizing each of those channels, combining each of the digitized outputs with a digital key to produce a signal which was unreadable without the key. Digital, encrypted voice!

4. Once the encrypted signal was produced, they still needed the means to transmit it in a reliable manner. The BTL staff solved the problems by inventing multilevel frequency shift keying. And again, the patent application is descriptive. A portion of United States Patent 3,991,273, "Speech Component Coded Multiplex Carrier Wave Transmission," awarded to Robert C. Mathes in 1976 (filed in October 1943) reads as follows (under the "what is claimed is" heading):

> ...a group of frequency modulators of the same type and same average frequency, means to impress said signals of stepped wave form on the respective frequency modulators to produce a plurality of frequency modulated waves of the same average frequency, and means to translate the last waves into frequency modulated waves accurately positioned at different frequency levels comprising a separate amplitude modulator for shifting the frequency of each such frequency modulated wave, and means to supply to said amplitude modulators carrier waves of accurately spaced frequency comprising a source of base frequency waves of highly constant frequency and a harmonic generator for fixing the frequencies of said supplied carrier waves.

They had shown the practicality of the techniques for digitizing the voice, encrypting and decrypting it, and had also invented a practical way to transmit the signals over long distances.

5. William R. Bennett, Fellow, IEEE, "Secret Telephony as a Historical Example of Spread-Spectrum Communications," IEEE *Transactions on Communications*, Vol. COM-31, No. 1, January 1983, 99.

6. As with almost any large-scale development, many individuals made important contributions. Fortunately, the BTL team was highly skilled and had access to many experts. For example, historian David Kahn notes in his article in the IEEE *Spectrum* of September 1984, "Cryptology and the Origins of Spread Spectrum," that Harry Nyquist and Claude Shannon made important contributions. He also relates that the British cryptographer Alan Turing was briefly involved in the development and approved the security aspects of the system for the British.

7. This type of system is generally described as a part of another United States Patent, "Secret Telephony" 3,985,958, which was awarded to Homer W. Dudley in 1976 (filed in 1941).

8. The third, "spare," record was retained at Arlington Hall to guard against the possibility of the destruction of a record during shipment. This practice was eventually terminated.

9. For example, the digitization was accomplished by circuits which featured the use of model 2051 Thyratron vacuum tubes. There were 384 of these tubes used in a single terminal.

10. Many of the WACs were stationed in the Pentagon, but others served in overseas locations. There were also civilian women associated with the systems.

Appendix A

Remarks by Dr. O. E. Buckley, President, Bell Telephone Laboratories at the Formal Opening of SIGSALY Service, 15 July 1943

We are assembled today in Washington and London to open a new service, secret telephony. It is an event of importance in the conduct of the war that others here can appraise better than I. As a technical achievement, I should like to point out that it must be counted among the major advances in the art of telephony. Not only does it represent the achievement of a goal long sought – complete secrecy in radiotelephone transmission – but it represents the first practical application of new methods of telephone transmission that promise to have far-reaching effects.

To achieve the result represented by this system, there have been done several very remarkable things. Speech has been converted into low frequency signals that are not speech but contain a specification or description of it. Those signals have been coded by a system that defies decoding by any but the intended recipient. The coded signals have been transmitted over a radio circuit in such a way that an interceptor cannot even distinguish the presence or absence of the signals. At the receiving end, the signals have been decoded and restored and then used to regenerate speech nearly enough like that which gave them birth that it may be clearly understood.

To do these things called for a degree of precision and a refinement of techniques that scarcely seemed possible when the researches that led to this result were undertaken. That speech transmitted in this manner sounds somewhat unnatural and that voices are not always recognizable should not be surprising. The remarkable thing is that it can be done at all.

All of the elements of this system were developed by the Bell Telephone Laboratories in the interests of advancing the art of telephony. Early in the course of the development, the system was discussed with representatives of the Signal Corps, who at once recognized its possible military value and encouraged our efforts. When it had reached the point where its principles could be demonstrated, the Signal Corps took prompt steps for its procurement. In the present embodiment of the system, manufactured by the Western Electric Company, representatives

of the Signal Corps have worked closely with us and are prepared to install and operate it.

We of Bell Telephone Laboratories and the Western Electric Company are proud of this achievement in which the efforts of a large number of our people were involved. We hope that it will be a help in the prosecution of the war, and we are indebted to the Signal Corps for the opportunity to put into practical use this new system of telephony.

A secret War Department letter from the Adjutant General's Office dated July 9, 1943, published the "Operating Procedure for Overseas Telephone System" and announced that service between Washington and London on the SIGSALY system would be available by July 15, 1943. SIGSALY was "on the air." [1]

Note

1. This material was obtained from the work of Donald E. Mehl, *The Green Hornet*, previously referenced.

Appendix B

Overview of the Encryption Process

The general concept of the encryption process for a single vocoder channel is presented in figure A-1. In each of the lines of this figure, the vertical axis segment represents levels of quantization, and the segments of the horizontal lines represent time in the 20-msec increments used in the SIGSALY system.[1]

Line (a) in the figure represents the six-level quantization of the output of the vocoder channel. Although difficult to show in this diagram, the individual signal quantization steps do not represent equal power changes in the actual input signal. The steps were logarithmetic and a part of the "companding" process. This process had been shown to produce improved intelligibility in the reconstructed voice output.[2]

The random key is illustrated by line (b) in the figure. This is the information produced from the recordings played on the turntable subsystem. The key was combined with the quantized signal information in a process which was then called "reentry." The reentry combination process is mathematically described as "adding the two quantized values mod 6."

Line (c) represents the encrypted data stream which would then be transmitted by the FSK-FDM radio equipment. The essentials of the receiving and decryption process are the reverse of the encryption process. First, the transmitted multichannel signals are demodulated. Then each channel is decrypted by subtracting the key mod 6 from the signal. It is obvious that the 20-msec segments of the quantized signal information and the key information must be synchronized in exactly the same manner at both the transmitting and receiving ends of the system. It remains to recombine the vocoder channel outputs, incorporate the pitch information and then reconstruct the audio signal and transform it into intelligible speech. This entire new process was extremely difficult to implement in the technology of the 1940s.

Notes

1. This figure is adapted from one in an article on the SIGSALY techniques contained in M.D. Fagen, ed., *A History of Engineering and Science in the Bell System: National Service in War and Peace (1925-1975)*, Murray Hill, NJ: Bell Lab, 296-317.

2. This topic is discussed in the IEEE article by William R. Bennett, previously referenced.

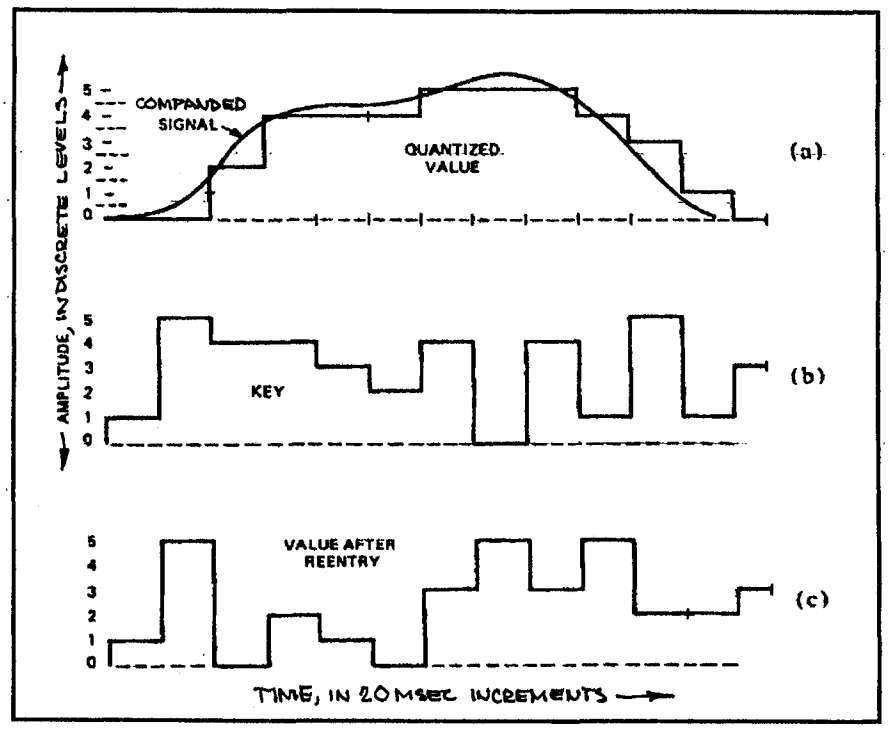

AMPLITUDE, IN DISCRETE LEVELS
5
4
3
2
1
0
COMPANDED SIGNAL
QUANTIZED VALUE
(a)
KEY
(b)
VALUE AFTER REENTRY
(c)
TIME, IN 20 msec INCREMENTS

Fig. A-1

For further information or additional copies, contact the Center for Cryptologic History, National Security Agency, Fort George G. Meade, Maryland 20755-6886, ATTN: N63


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA