Rachel Lundberg

In a wartime situation, speed of communication is drastically important. As the setting of World War II brought many new methods of encipherment into play, this became especially clear. The efficiency with which a message could be enciphered and transmitted was in direct correlation with the method's usefulness. The quickest way to transmit messages, of course, was by telephone, but telephone scramblers were usually not very secure. By the end of 1941, the Allies were beginning to suspect that the A-3, their primary telephone scrambler, had been broken. In fact, the German organization in charge of monitoring telecommunications, the Deutsche Reichspost, had been cracking it for several months, and was even capable of deciphering A-3 transmissions in real time (Weadon, Boone and Peterson). It was clear to the Allies that they needed a new way of protecting their telephone messages.

In 1942, Bell Telephone Laboratories stepped up to the challenge. The project was led by A. B. Clark, the researcher who originally patented the companding (compressing and expanding of waveforms) technique that would prove vital to Bell Labs' efforts (Weadon). Clark was assisted by Alan Turing, the British mathematician, during his trip to the United States to work on Naval Enigma, demonstrating that the Allies' policy of pooling their resources was beneficial to their efforts in cryptography (Copeland and Proudfoot). Clark called his machine "the Green Hornet" because the buzzing sound of an enciphered message resembled the theme song of the popular radio show of the 1930s. However, this nickname would eventually be abandoned and the machine would be officially called "SIGSALY," which was not an acronym, but merely a "cover" name (Weadon).

Clark's work was based on the "vocoder," or voice encoder, a device developed by Bell Labs six years earlier. The job of the vocoder was to split the recorded message into ten bands of low frequency (below 25 Hz). Each of these bands corresponded to an area of the speech range. This was possible because each sound made by the human voice has a unique set of frequencies. For example, an "s" sound has lots of high frequencies, but no low ones. Thus, an "s" sound in the message was recorded by the vocoder in the band that matched that range (Anderton). In addition to the ten primary frequencies, there was a signal to indicate whether or not the sound was voiced, and another to indicate the pitch of the voice, resulting in a total of twelve signals (Boone and Peterson).

The next stage of the process was to sample the amplitude of each signal every twenty milliseconds. This process results in what is known as a "discrete signal." Rather than the band's amplitude being represented by a line, it could be represented by a series of points on the line, each spaced twenty milliseconds apart. Now that the message had been reduced to a set of amplitude values, the values were sorted into six levels, numbered 0 to 5. Each sound was now a number. It is important to note that the six levels did not progress linearly—that is, they were not equally spaced; the distances between levels were greater at low amplitudes and smaller at high amplitudes. This is Clark's principle of "companding," which was so vital because equal spacing would have required more levels, thus tightening the ranges to be dealt with and making implementation nearly impossible. The pitch signal had to be more precise, and was split into a pair of six-level values, which multiply to produce a total of 36 pitch levels (Bennett).

Finally, the encrypting process could begin. Each sampled amplitude was assigned a random number from 0 to 5 (the same as the level designations). This set of random numbers made up the key. The random value was subtracted from the amplitude's level to produce the

encrypted amplitude. Modular arithmetic was employed in case of negative results so that they would "wrap around" and be contained in the appropriate interval (Bennett). 6 is the modulus because there are six levels. So, if the first sampled amplitude was in level 0, and the key stated that its random number was 4, the encryption would proceed like this:

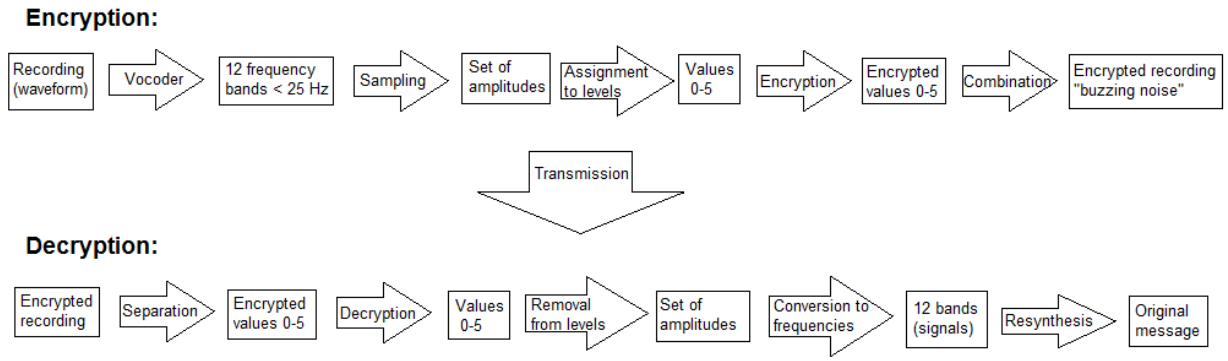
$$0 - 4 = -4 \equiv 2 \pmod 6$$

This shows that an amplitude in level 0 with a random value of 4 would be transmitted as an amplitude of 2. The encrypted amplitudes of all twelve bands transmitted together are what produced the buzzing sound that potential eavesdroppers would hear.

Once they had demodulated the multichannel signals, thus allowing each separate amplitude to be distinguished, the recipients of the message would take the first encrypted amplitude of 2, check their key to see that the random value is 4, and perform the following calculation in order to decrypt:

$$2 + 4 = 6 \equiv 0 \pmod 6$$

Thus, they had determined that the amplitude belongs in level 0. The process was repeated for each value of each of the ten discrete signals, and the recipients had all the data they needed to listen to the original message. All that remained was to turn the information back into a voice waveform. This was done by inverting the original vocoder process: the amplitudes were turned back into the twelve signals, which were resynthesized into one waveform (Boone and Peterson). Because the recording had been sampled (resulting in some loss of data), the resulting transmission was of a low quality and voices sounded mechanical, but the message was still distinguishable. The communication was complete. The entire process can be summed up like this:



This may seem like a lot of work to send a single message, but most of it was done by machine. A separate piece of machinery was needed for almost every one of the steps in the encryption and decryption process, and as a result, SIGSALY terminals were massive. A single terminal was made up of about 40 racks of equipment and weighed around 55 tons. The technology of the time was not very energy-efficient, resulting in an increase in the already huge amounts of energy needed to power SIGSALY. The equipment generated so much heat that the rooms had to be outfitted with special air-conditioning systems to keep the machinery from overheating (Boone and Peterson).

SIGSALY was formally deployed in 1943, and twelve terminals were installed over the next three years, the first being in Washington, D.C. and London. The Army Signal Corps realized immediately that the system would require a large staff to operate, and the 805th Signal Service Company was created to fill the need. The recruits were trained in a Bell Labs school in New York City (later moved to the Pentagon) and sent out to SIGSALY locations across the globe (Weadon). The 805th had 356 members—81 officers and 275 enlisted men—and a higher average grade than any other company in World War II. Every member was specially chosen for his skills and experience, usually in electronics or telephony (Boone and Peterson).

The 805th Signal Service Company was charged not only with the operation of SIGSALY, but also with its maintenance. On a typical day, the machinery was operated for

about eight hours, and maintenance was performed during the remaining sixteen. Each detachment was expected to work round-the-clock in this fashion. Vacuum tubes, power supplies, and stepper circuits had to be checked constantly. The amount of disassembling and reassembling done on a daily basis was so great that a schedule had to be adapted to prevent substantial damage to the equipment. Despite the amount of repair work that had to be done, SIGSALY, as a whole, operated efficiently and with very little disruption to its operational schedule (Boone and Peterson).

SIGSALY was not only efficient, but effective—the Germans did not succeed in cracking it. In fact, it was not even subjected to any serious cryptanalysis because none of those who had intercepted it could figure out what sort of signal it was, let alone formulate a method of breaking it (Bennett). The Green Hornet signal was so secure that its key was never even put to the test. Even if the interceptors of the signal could have understood it, it is reasonable to conclude that it could not have been cracked. The key was based on the onetime pad principle, with a random number assigned to each amplitude in an entirely random fashion (Bennett). The only way to discover the original message would be to test every possible key. Considering that there were twelve bands, and the amplitude and random number changed every twenty milliseconds, the impossibility of the task is apparent.

Though SIGSALY provided unprecedented security for telephone communication, it had two fundamental drawbacks: the first was, simply put, its size. The materials, energy, and manpower needed to operate the system limited the number of terminals, and as such only the most important conversations were encrypted this way (Boone and Peterson). Second, generation and distribution of random keys was extremely difficult. The keys, which were converted into audio tones and recorded on phonograph records, were changed both on a

schedule and with every conversation, so delivering the keys each time there was a change was a constant challenge. Also, each record had a maximum capacity of about twelve minutes of key, so longer conferences needed more than one. Each record had to have its own turntable to keep it rotating at a speed that recorded one piece of the key every twenty milliseconds, and when there was more than one record, they had to be synchronized as well. This was done by starting both ends of the link (for example, the terminal in Washington and the terminal in London) at the exact same moment, at which point a clutch was activated that would release a spring and keep the turntables in lock with a synchronous motor. The continued function of this mechanism required constant attention from the operators (Boone and Peterson).

SIGSALY was in use from 1943 to 1946, and was used to encrypt more than 3,000 top-secret communications (Weadon). Because the system was used for only the highest-level conferences, specific records of its use are scarce. However, it is known to have been implemented at the Yalta Conference of 1945, an indication of the trust that the Allies came to place in it over the course of the war. SIGLSALY was, in many ways, a huge breakthrough, being the first realization of enciphered telephony, the first quantized speech transmission, and several other scientific "firsts"—it was a huge step toward the digital communication technology of today (Bennett). For the unparalleled security it provided the Allies during World War II, SIGSALY's contribution to the Allied victory cannot be underestimated. Throughout the war, radios all across America proclaimed: "The Green Hornet strikes again!" The listeners had no idea that another Green Hornet had done just that.

Works Cited

Anderton, Craig. "How Vocoders Work." *PAiA*. PAiA Corporation, n.d. Web. 22 Oct 2010.

Bennett, William. "Secret Telephony as a Historical Example of Spread-Spectrum Communication." *IEEE TRANSACTIONS ON COMMUNICATION* COM-31.1 (1983): 98-104. Web. 22 Oct 2010.

Boone, J. V., and R. R. Peterson. "Sigsaly - The Start of the Digital Revolution." *National Security Agency / Central Security Service*. National Security Agency, 15 Jan 2009. Web. 19 Oct 2010.

Copeland, Jack, and Diane Proudfoot. "Alan Turing, Codebreaker and Computer Pioneer." *AlanTuring.net*. Jack Copeland, May 2004. Web. 23 Oct 2010.

Weadon, Patrick. "Sigsaly Story." *National Security Agency / Central Security Service*. National Security Agency, 15 Jan 2009. Web. 17 Oct 2010.