F, 5 January

Cabinet War Rooms
SIGSALY

The first devices to secure transmission of voice were developed just after World War I. They were substitution devices; they inverted frequencies. High frequencies were substituted for low frequencies and low frequencies were substituted for high frequencies. This was easy to do electronically.

But, it was also easy to break. In fact, because much voice is in the middle frequencies and the middle frequencies are not changed much by inversion, it was sometimes possible to get a sense of the message just from the ciphertext.

The A-3 scrambler

> … was based upon 1920s concepts. It divided the voice-frequency band into five subbands, inverted each of them, and then shifted the voice from one subband to another every 20 seconds.
>
> David Kahn
> *Cryptology and the origin of spread spectrum*

In 1941, the United States was not at war although we were supporting the Allies, especially Britain, materially. The United States had a device to secure voice transmission called the A-3 Scrambler. This device used both substitution and transposition to encipher voice. Messages were chopped into small pieces, in each piece substitution was made by inverting frequencies, and the pieces were scrambled. This device was broken by the Germans during Fall 1941. The United States military was aware that the A-3 was not secure.

On December 7, 1941, cryptanalysts in Washington, D.C., were in the process of breaking a long ciphertext from Tokyo to the Japanese embassy in Washington, D.C. William Friedman's SIS team had earlier broken the Japanese diplomatic ciphers, but the naval ciphers had not yet been broken. The message had 14 parts.

About 10 days earlier, war between the United States and Japan seemed imminent, and United States forces in the Pacific had received a "warning of war." But, when and where?

The last part of the diplomatic message instructed the Japanese embassy to destroy its cryptographic equipment and meet with the United States Secretary of State at 1:00 pm on Sunday, December 7.

The message made war with Japan appear to be certain, and the 1:00 pm Sunday, December 7, time seemed significant. The Chief of Naval Operations Admiral Stark decided to reinforce the previous warning of war by sending a message to Admiral Kimmel at Pearl Harbor. Admiral Stark was aware that the A-3 Scrambler was secure, and he chose to send his message by radio telegraph. Unfortunately atmospheric conditions over the eastern Pacific preventing Hawaii from receiving the message; so, the message was sent by Western Union's undersea cable. When the message was delivered to Admiral Kimmel at Pearl Harbor, the Japanese planes had left, and the battleships of the Pacific Fleet were at the bottom of Pearl Harbor.

In 1942 the United States contracted with Bell Labs for a device to secure voice communications.

The device was based upon the Vocoder (*vo*ice *coder*) that had been invented by Homer W. Dudley of Bell Labs.

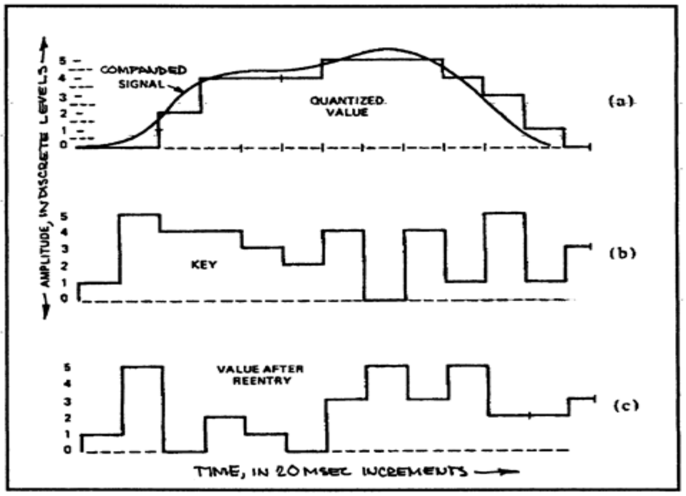
http://www.keyboardmuseum.org/pre60/1930/voder.html

In 1940, Homer W. Dudley of Bell Labs developed "the Vocoder" a device that digitized voice.

The device was called SIGSALY (this is not an acronym; it is just a made-up word).

SIGSALY chopped voice up into 20 millisecond intervals, spread the frequencies, and digitized. There were 10 intervals for speech and two intervals for background noise (hiss). (Voice sounds strange if all background noise is removed.) The digital levels were 0, 1, 2, 3, 4, 5.

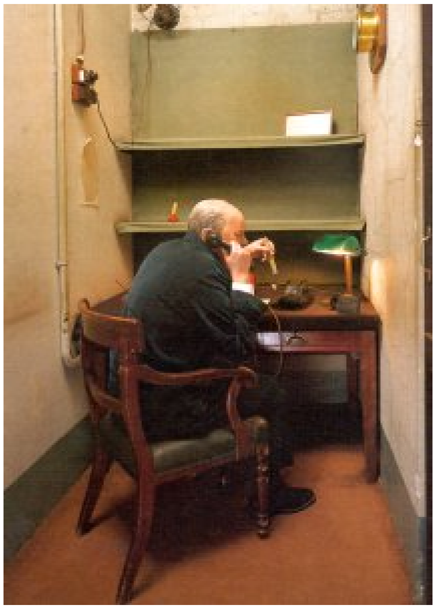
http://www.nsa.gov/publications/publi00019.cfm



Then noise was recorded. The recorded noise was noise from an electronic tube; this noise was thought to be random. The noise was chopped up and digitized as the voice was. Noise was recorded on large records. Two copies were made – one for the sending station and one for the receiving station.

The plaintext voice and the random noise were added together modulo 6 to produce the ciphertext that was transmitted. The receiving station recovered the plaintext voice by subtracting the noise modulo 6.

This procedure is a one-time pad and is completely secure.



http://cwr.iwm.org.uk/server/show/ConWebDoc.826/viewPage/5

The Transatlantic telephone room in the Cabinet War Rooms, London

Eventually, during the war, there were 8 SIGSALY devices: Washington, D.C., London, Paris, North Africa, Hawaii, Guam. Manila, and Australia.

Eventually, during the war, eight SIGSALY stations were built. The two most familiar were located in London (in Churchill's War Rooms in the basement of a building in Whitehall) and in Washington, D.C. (in the newly constructed Pentagon).

The picture shows the small room in Churchill's War Rooms that contained the SIGSALY telephone.   But, the picture is a bit deceiving because the actual SIGSALY station was located about a mile away in the basement of Selfridge's department store. The SIGSALY station was quite large. The next two slides are photographs from the SIGSALY display at the National Security Agency's National Cryptological Museum. The second of these two slides shows the turntables. Tow turntables were necessary because each record held only about 18 minutes of noise, and, because conversations might last longer than 18 minutes, and second record was available incase the 18 minutes of noise on the first record were not enough.

SIGSALY is a remarkable engineering feat – being able to synchronize the 20 millisecond pieces of voice and noise at stations on opposite sides of the Atlantic.

1943 SIGSALY 1946
SPEECH ENCIPHERMENT SYSTEM

STU-I