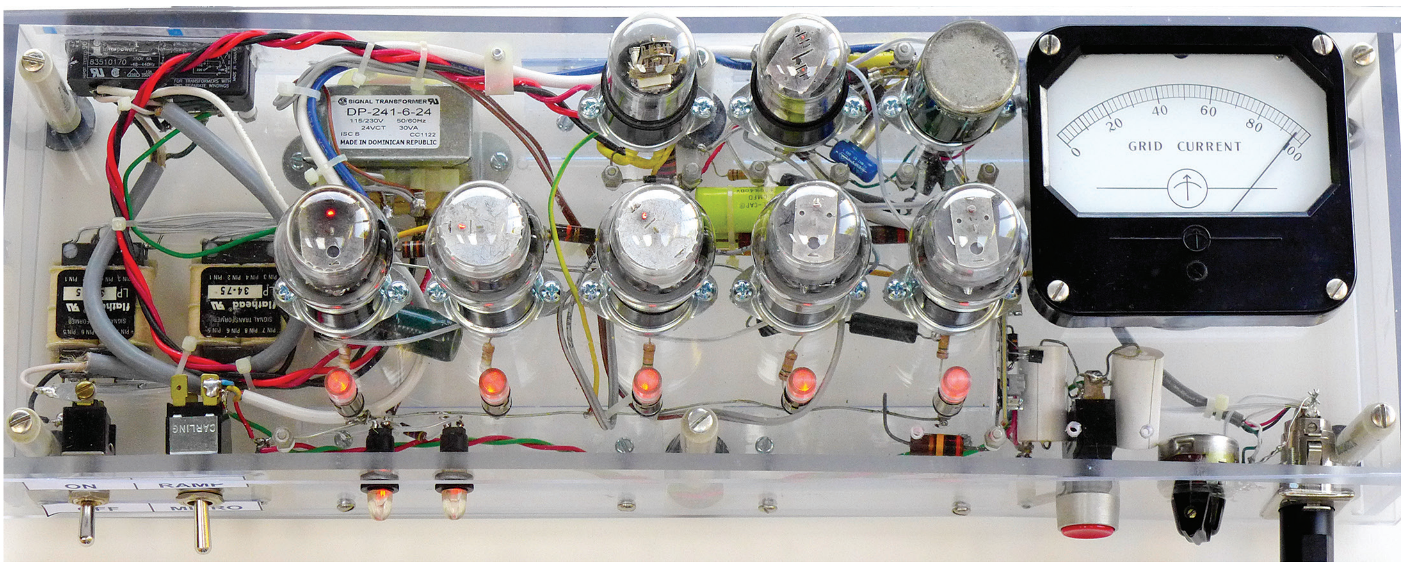
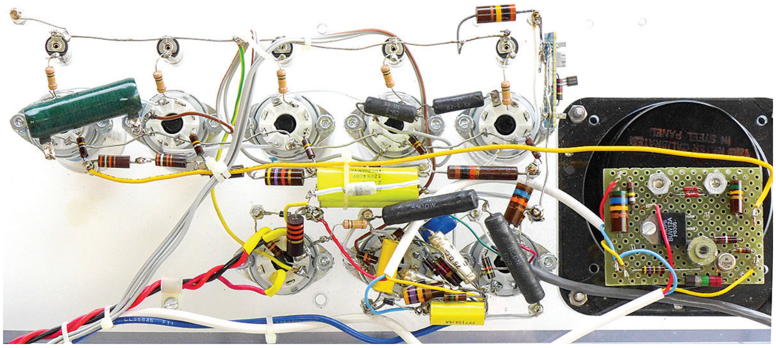


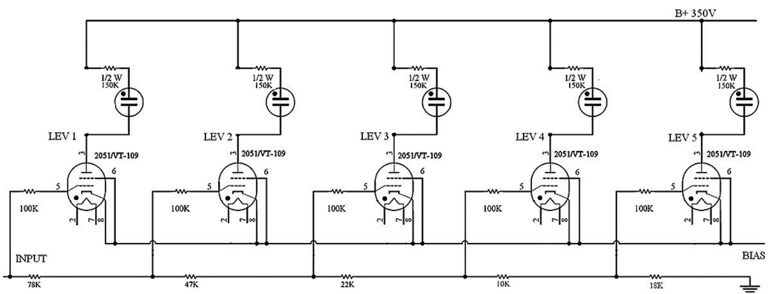
RE-CREATING THE SIGSALY QUANTIZER

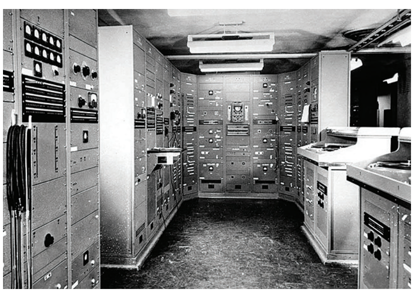
THIS 1943 ANALOG-TO-DIGITAL CONVERTER GAVE THE ALLIES AN UNBREAKABLE SCRAMBLER

IN THE YEARS BEFORE WORLD WAR II, GERMAN INTELLIGENCE COULD DECODE BAND-SCRAMBLED U.S. radiotelephone conferences. After Pearl Harbor, an unbreakable speech scrambler was developed with top priority, and by 1943, it was deployed. Known as SIGSALY, the device pioneered many advances critical to modern digital media technologies, including spread-spectrum communications and the first use of pulse-code modulation (PCM) to transmit speech. • SIGSALY was top secret, so even today information about the details of its construction are hard to come by. I've spent 20 years researching the history of digital technology and digital media, especially SIGSALY. I searched IEEE and U.S. National Security Agency (NSA) journals, and Bell Telephone Laboratories patents. Finally, I found Lieut. Donald Mehl, a WWII SIGSALY technician, who gave me invaluable assistance. In 2015, I realized that it might be possible to re-create a key element of SIGSALY—the quantizer—using vintage parts. • SIGSALY was unbreakable because, unlike earlier analog systems, it scrambled voices by using a one-time random digital encryption key. Before a digital key can be applied, a speaker's voice must first be converted from analog to digital, thus the quantizer. • Modern analog-to-digital conversion makes it easy to capture the entire audio spectrum. With the technology available at the time, the creators of SIGSALY used 12 speech parameters that best encoded speech. SIGSALY used vocoders to analyze incoming speech and classify them into 10 frequency sub-bands; a pitch parameter; and a bit that indicated whether the speech sound was voiced or unvoiced. • SIGSALY had 72 identical quantizers to digitize the 12 vocoder parameters and the encryption key (stored as a vinyl recording of noise). The digitized voice and key were enciphered by modulo six addition. Each quantizer employed five VT-109/2051 thyratrons. Thyratrons are a type of electronic tube, but they differ from conventional ones in that they

CLOCKWISE FROM LEFT: JON D. PAUL (3); NSA







DIVIDE AND CONQUER: The complete SIGSALY voice scrambler was a huge machine [bottom] that relied on many analog-to-digital converters. The heart of the converter was a resister divider ladder [top photo and schematic, middle] connected to thyratrons. In my re-creation, I have added neon indicator lights.

don't respond in a linear way: They are off until the grid voltage exceeds a trigger; then an arc forms and they "latch up" and conduct until the anode current falls to zero, resetting them. The five thyratrons formed a flash converter, in which an incoming signal is compared to a reference voltage at a number of tap points in the circuit. In SIGSALY, the analog input voltage is fed into a five-tap logarithmic resistor divider ladder, whose taps drive the thyratron grids. As the input voltage increases, the five thyratrons thus trigger in sequence (producing not binary but a logarithmic "thermometer code"). These five outputs were sampled every 20 milliseconds to form a six-level quantized output signal (it's a six-level output, not five, because zero is one level).

In reconstructing the SIGSALY quantizer I wanted to make something that could be used in practical demonstrations and also double as a wonderful museum piece. The design includes a 120/240-volt power supply, a microphone preamp, a ramp generator, a panel meter displaying the analog-to-digital conversion, and five neon lamps that light up in logarithmic sequence. One input is a dynamic microphone: It's plugged into a preamp that uses a 6SL7GT dual triode to amplify its audio signal by 60 decibels. A slowly increasing ramp signal is an alternate input.

My design uses the same five-tap logarithmic ladder and the same type of thyratron that SIGSALY used. Instead of SIGSALY's 20-ms pulsed sampling, I sample the input at the zero-voltage crossings of the AC power.

The full details of the quantizer's construction would take more room to explain than is available here, but a complete description is available as a supplement to this article online. One critical difference between thyratrons and their modern descendants—silicon controlled rectifiers and TRIACs—is that the thyratron filaments must be preheated before applying any anode voltage to prevent damage. A thermal time-delay relay gives the filaments 15 seconds to heat up.

For some parts, I turned to my own laboratory, which has vintage electronic parts I've collected since the 1950s. I searched eBay for original VT-109/2051 thyratrons, and porcelain octal tube sockets. I used other 1940s-era parts (such as Allen-Bradley carbon composition resistors) for the quantizer, while I used some modern components (like dual primary power transformers) for supporting electronics not present in the original quantizer. To display the components, I built the quantizer into a 49- by 17- by 8-centimeter clear plastic chassis. The overall cost was US $1,250.

Design and construction extended over three years, and the debugging was very challenging, especially with 350 V present! Construction finished and I started debugging just an hour before departing from California to Paris, where the quantizer was to be demonstrated at several crypto and InfoSec conferences. After I added power resistors to solve some problems with filament voltages and fixed a few wiring errors, the quantizer began to work a bit, but only two of the five thyratrons triggered, the microphone preamp had full-scale oscillations once a second ("motorboating"), and the anode power was heavily overloaded as each thyratron fired.

I had to stop debugging and depart. I packed the quantizer with a few tools and spare parts, and Air France kindly obliged me with special treatment for the delicate machine. In Paris, I had to finish debugging without a laboratory or instruments, save for a voltmeter. I scrounged parts and tools at the Marché aux Puces (Paris flea markets), and finally finished debugging at an old friend's ham-radio shack! Many of the problems arose because the thyratrons varied considerably in grid trigger voltages. (The same problems of thyratron inconsistency were tackled by the original SIGSALY engineers and technicians.)

Now, the finished unit works reliably. According to the NSA and the National Cryptologic Museum curators, this is the first attempt ever to re-create any piece of SIGSALY. But best of all, old and young, technical and nontechnical audiences alike are impressed and immediately comprehend the underlying principles and the close connections to today's digital age. **—JON D. PAUL**

POST YOUR COMMENTS at https://spectrum.ieee.org/sigsaly0219