Durante la Segunda Guerra Mundial funcionó un equipo de encriptación vocal denominado SIGSALY. Permitió la comunicación radiotelefónica directa entre el alto mando americano y el británico a través del Atlántico norte y entre los almirantes y los generales en las operaciones del Pacífico sur. Este desconocido equipo es un hito muy importante en la historia de las telecomunicaciones.

Voces Secretas. "SIGSALY", sistema encriptador de la Segunda Guerra Mundial

Luis Fernando Real Martín,
Ingeniero Técnico de Telecomunicación

"Esta no es hora de amargura ni de regocijo. Es hora de preparación, resolución y esfuerzo. La guerra continúa todavía."

Discurso a la Cámara de los Comunes sobre la marcha de la guerra.
22 de febrero 1944
Winston S. Churchill.

GUERRA EN EL PACÍFICO

El alto mando militar norteamericano esperaba un ataque japonés para el mes de noviembre en la región de Indonesia, rica en el imprescindible petróleo, pero la sorpresa llegó el domingo 7 de diciembre de 1941 a las 8 de la mañana, cuando la aviación japonesa atacó la base naval Pearl Harbor, en las islas Hawai. El lunes 8, Estados Unidos y Gran Bretaña declararon la guerra a Japón. La contienda había tomado proporciones mundiales.

Cuando entra en guerra, el gobierno americano toma el control de las industrias. Técnicos y científicos son movilizados para desarrollar proyectos bélicos. El trabajo en los Laboratorios Bell es supervisado por personal militar.

LAS COMUNICACIONES EN TIEMPOS DE GUERRA

Las comunicaciones militares difieren bastante de las comerciales. Las ac-

Figura 1. Maqueta de Sigsaly en el National Cryptologic Museum. Cortesía National Security Agency.

tuaciones se basan en el rápido análisis y correcta interpretación del contenido de cientos de mensajes que reciben los centros de mando. Los mensajes deben ser simples y precisos y su encriptación rápida y segura. Como expone Sigh en su libro, los métodos basados en cuadernos de claves o los que requieren personal especializado son lentos, complejos y sobre todo, vulnerables.

El antiguo sistema de comunicación entre el gobierno americano y el británico fue descubierto por los alemanes en 1941 y todos los mensajes interceptados. Los aliados necesitaban un nuevo sistema rápido, directo, adaptado a las instalaciones transoceánicas existentes y que no fuese detectado por los rastreos de radio.

SIGSALY DURANTE LA GUERRA

En 1942 el Jefe del Estado Mayor George Catlett Marshall[1], pidió al presidente de los Laboratorios Bell, Oliver E. Buckley un aparato de comunicación verdaderamente secreta. Sería la puesta en práctica de diversos proyectos que habían experimentado (descritos en los números anteriores de la revista *Antena*, consultar la bibliografía). El avance fue rápido y al año siguiente presentaron el equipo denominado Sigsaly. (también Proyecto X, Sistema X o Ciphony 1).

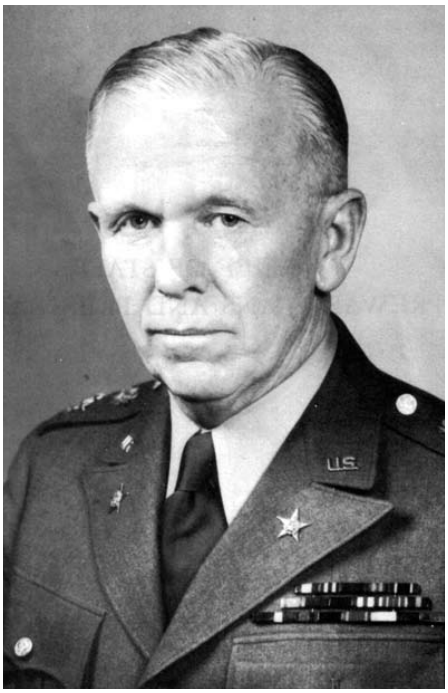

Figura 2. General George Catlett Marshall. Cortesía U. S. Army Center of Military History.

El equipo estaba formado por cuarenta bastidores y pesaba cincuenta toneladas, con estas dimensiones el uso quedó restringido a las comunicaciones telefónicas de alto nivel. Un equipo se situó en el Pentágono en Washington y otro se trasladó a Gran Bretaña. Como no cabía en las habitaciones del Ministerio de Marina de Londres se instaló en el sótano de los almacenes Selfridge. El terminal telefónico se situó en la Sala de Comunicaciones del Ministerio (reconstruida en el "Imperial War Museum"). En el frente del Pacífico, un equipo se instaló en los sótanos del edificio del Cuartel General del Área Sureste del Pacífico en la ciudad Australiana de Brisbane (actualmente el edificio se llama "McArthur Chambers"). Otro parece que fue instalado a bordo de un pequeño barco del centenar de embarcaciones que acompañó a la flota del General McArthur por el océano. Entre 1943 y 1946 entraron en servicio una docena de equipos distribuidos por el mundo y posteriormente se incrementó hasta la veintena.

Los equipos Sigsaly realizaron 3.000 conferencias. Indudablemente la calidad de la voz era muy mala pero la comunicación era completamente segura. El sistema de encriptación nunca fue descubierto.

1 Artífice del "Plan Marshall" para Europa y Premio Nobel de la Paz en 1953.

Figura 3. Oliver E. Buckley. Cortesía AIP Emilio Segrè Visual Archives

La llegada del transistor permitió reducir el volumen y el peso manteniendo la misma filosofía de funcionamiento que se mantuvo durante la siguiente década.

SIGSALY DESPUÉS DE LA GUERRA

Firmada la rendición, muchos aparatos y documentos técnicos de los servicios secretos fueron desmantelados y destruidos. Los primitivos computadores británicos Colossus o Bombe que albergó la casona de Bletchley Park y ayudaron a descifrar los mensajes de Enigma fueron desmontados. Sigh razona que no fue una resolución acertada. Por el contrario, los americanos no destinaron sus máquinas a tan luctuoso fin. Esto les permitió continuar investigando, mientras que los británicos sufrieron un grave retraso al tener que construir nuevos aparatos y repetir las experiencias. Los equipos Sigsaly regresaron a su país de origen y se reconstruyó el modelo que se encuentra en el National Cryptologic Museum (Figura 1).

En los años setenta, algunos países desclasificaron muchos documentos de la Segunda Guerra Mundial, incluidos los relacionados con el proyecto Sigsaly. De este modo, se pudieron esclarecer muchos episodios ocurridos durante la guerra. El más notable fue sin duda, el desciframiento del código de Enigma por los británicos. Pero sobre todo sirvió para restablecer el honor de muchos civiles que al no combatir y no poder desvelar su labor en el manejo de las máquinas de los servicios secretos, fueron acusados injustamente de cobardes por sus conciudadanos (S. Sigh).

SIEMPRE EL VOCODER

Sigsaly se basaba en el Vocoder de H. Dudley, el primer compresor y sintetizador de voz (ver ANTENA n.º 173). Obtenía una información de los parámetros básicos de la señal vocal que transmitía en un ancho de banda muy estrecho. A partir de ellos, el receptor podía regenerar el mensaje original. Seguidamente se describe con más detalle.

En el analizador del emisor, las frecuencias captadas por el micrófono se dividen con filtros en subbandas, son los canales. Uno se denomina canal de frecuencia o "patrón de frecuencia". Selecciona la frecuencia fundamental vocal y realiza una conversión de frecuencia en tensión, cuya amplitud depende si el tipo de sonido es sonoro o sordo. En el sintetizador del receptor hay 2 generadores locales para este "patrón de frecuencia". Uno es un oscilador de relajación que genera los armónicos para los sonidos sonoros y el otro es un generador de ruido blanco para producir los sordos. El canal de frecuencia recibido selecciona de uno u otro o ambos para interactuar con los canales de amplitud.

Los otros 10 canales del analizador constituyen el denominado "patrón de amplitud". Sus niveles de tensión son proporcionales a las variaciones de energía de las subbandas. En el sintetizador del receptor a cada canal se le aplica la señal seleccionada del patrón frecuencia. Ambas señales modelan un fragmento del espectro. Las salidas se unen para reconstruir artificialmente el espectro original que se emite en el altavoz.

La Figura 4 esquematiza el Vocoder, en verde las etapas del canal de frecuencia y en naranja las del canal amplitud.

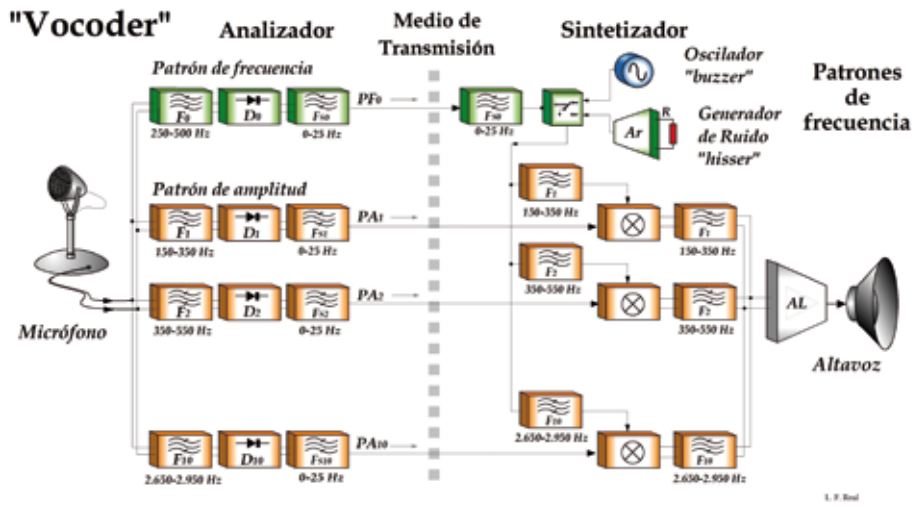

Figura 4. Esquema del Vocoder según R. L. Miller. Dibujo L. F. Real.

LA CLAVE ES EL RUIDO

La información de los canales de frecuencia y amplitud se encriptan añadiendo ruido blanco. Es completamente aleatorio, cumpliendo así una de las condiciones para tener una clave segura. El ruido producido por un triodo de relleno de gas mercurio se amplifica y se divide en las mismas subbandas que el analizador. Cada canal tiene su propia clave de ruido. El ruido se graba en discos fonográficos de vinilo (acetato o aluminio, según las versiones del proyecto Sigsaly). La duración del disco era de doce minutos; por lo tanto era necesaria la grabación de un segundo disco para ampliar el tiempo de utilización. Otro disco igual debía de llevarse al destino para descifrar el mensaje. La distribución de estos discos se realizó junto con los discos musicales que entretenían a los soldados en las bases militares. La Figura 5 muestra la creación del vinilo e ilustra su envío a las diferentes ciudades donde se ubicaba Sigsaly.

MUESTREO, CUANTIFICACIÓN Y SUMA

En 1941 R. K. Potter y R. C. Mathes habían resuelto el problema de la suma de la señal de los canales y del ruido (ver *Antena* nº 182). Las pruebas habían concluido con la necesidad de una con-

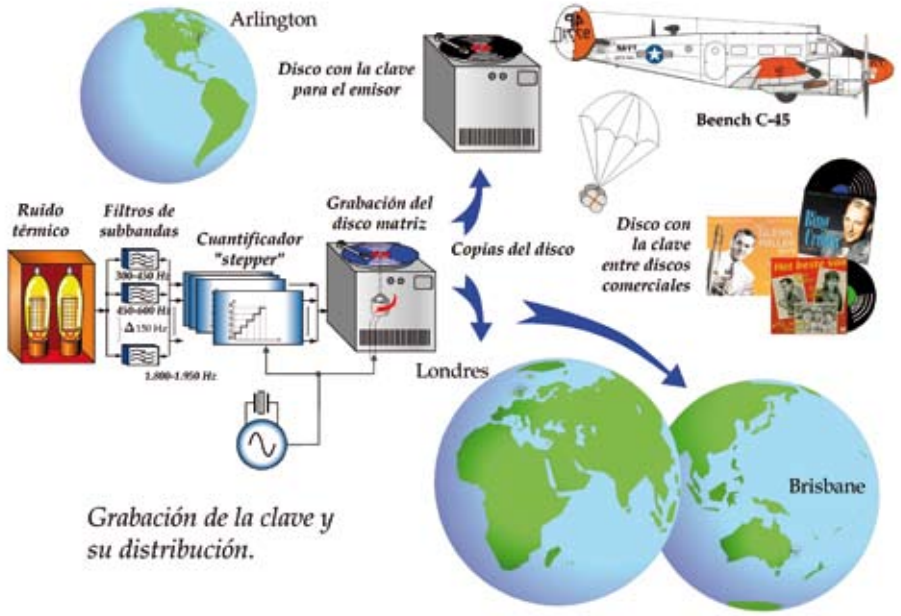

Figura 5. Distribución de la clave a los centros de comunicación. Dibujo L. F. Real.

versión analógica a pulsos discretos. Esta conversión, *stepping*, la realizó el *stepper circuit*, (primer nombre dado a los cuantificadores). La suma se realizó utilizando la aritmética modular que propuso H. Nyquist. El circuito se denominó circuito de reentrada, *reentry circuit*. En Sigsaly, los canales del analizador se muestrean y cuantifican en 6 valores posibles. El ruido filtrado y cuantificado también se grabó en los discos, así aparece en el esquema de las Figuras 7 y 9.

La cuantificación que funcionó no era uniforme. En esta cuantificación los niveles no son equidistantes, los superiores están más cerca entre sí que los inferiores. La fidelidad del oído es mayor para las frecuencias más altas y es necesario captar los cambios rápidos de éstos sonidos. La señal eléctrica cuantificada debe ajustarse a la señal original evitando que la distorsione. La posterior

Figura 6. Platos con los discos de vinilo. Cortesía Chris Christensen.

Pulse Code Modulation (PCM) se basó en la cuantificación no uniforme recién inventada.

El tiempo de muestreo fue un nuevo problema. Las señales de radio transoceánicas sufren breves desvanecimientos. La anchura de los pulsos del cuantificador debía de ser superior a estos lapsos para mantener la sincronía y no perder información. Experimentalmente se comprobó que 20 mseg de muestreo eran suficientes y se mantuvieron en el funcionamiento.

LA PRECISIÓN DEL CANAL DE FRECUENCIA

Las pruebas demostraron que la información del canal de frecuencia era mucho más sensible al número de niveles del cuantificador que los de amplitud. Para que el mensaje fuese inteligible era necesario aumentar hasta 30 niveles. El inconveniente es que el aumento de niveles incrementaba el ancho de banda a transmitir y esto es inaceptable en los radioteléfonos.

En este problema trabajaron R. H. Badgley y R. L. Miller y la solución la proporcionó el matemático y general francés del siglo XVII, Pierre Vernier. El lector puede encontrar un ejemplo del método de medida de precisión que Vernier inventó en el nonio del calibre o pie de rey.

La Figura 8 muestra cómo los ingenieros de Bell consiguieron con la idea de Vernier, la precisión en la cuantificación de la señal en el canal de frecuencia. El canal se muestrea en 6 niveles y constituye el canal principal del canal frecuencia. Estas muestras se restan a la señal original obteniéndose una diferencia que no alcanza el nivel de un escalón del cuantificador (áreas rayadas) por ser menor de 1/6. Esta señal diferencia se amplifica y se cuantifica por un convertidor de 6 niveles similar al anterior. Así se obtienen dos canales, el principal y el de la diferencia que cuantifican el canal frecuencia en 36 niveles, ambos se encriptan con sus respectivos canales de ruido.

En recepción, después de sustraer el ruido a los canales, el canal de la diferencia debe atenuarse para conseguir su valor original antes de añadirle al canal principal. De este modo se reconstruye el canal de frecuencia muy exacto.

LA TRANSMISIÓN DE LAS SEÑALES

Los niveles cuantificados se aplican a un modulador FSK (Frequency-shift keying). Cada nivel posible genera un tono de baja frecuencia. Los 6 tonos de cada canal se modulan con una portadora diferente de tal forma que el conjunto de los 72 tonos (6 para cada uno de los 12 canales) se distribuya en un espectro de audio que será transmitido por radio a su destino.

LA SINCRONIZACIÓN DE LA COMUNICACIÓN

Los responsables militares de los centros de mandos acordaban cuándo establecer una comunicación. Los preparativos comenzaban un par de horas antes. Los discos colocados en los platos estaban preparados para encriptar y desencriptar el mensaje en tiempo real, (Figura 6). Los sistemas mecánicos de los platos eran muy sofisticados. La velocidad de rotación se mantenía constante con un oscilador local, pero las revoluciones eran comparadas con frecuencias patrones recibidas por radio. Se evitaba el fenómeno del *jitter*. En los instantes previos se colocaba

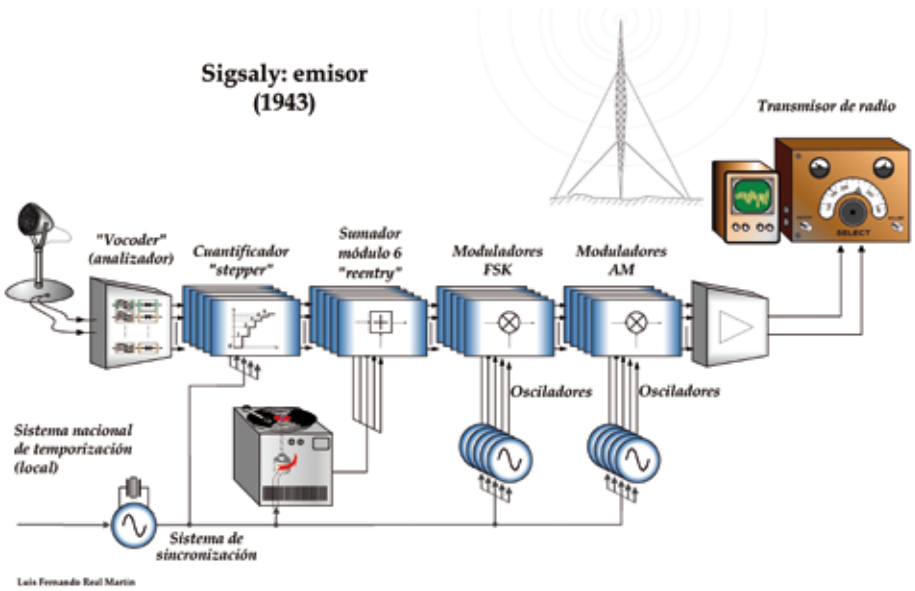

Figura 7. Esquema emisor de Sigsaly. Dibujo L. F. Real.

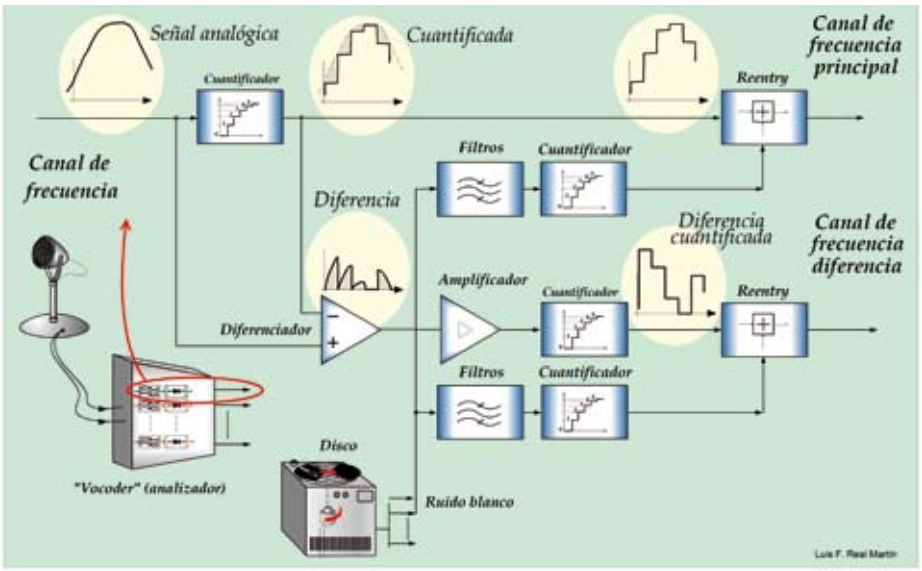

Figura 8. Esquema del canal de frecuencia. Dibujo L. F. Real.

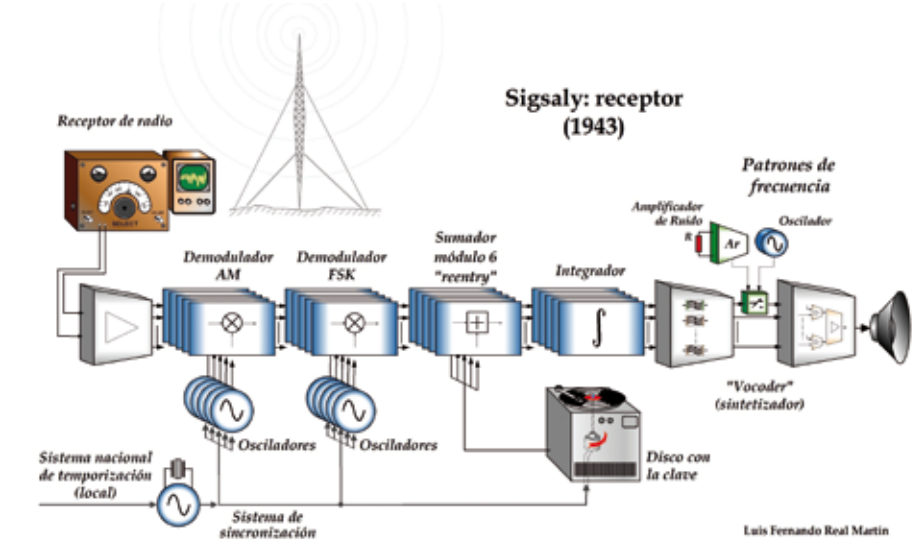

Figura 9. Esquema receptor de Sigsaly. Dibujo L. F. Real.

la aguja en el inicio del primer surco del disco y los saltos de la aguja provocaban un "tic" que facilitaba la sincronización. Cuando esto ocurría comenzaba la sesión de comunicación.

MANTENIMIENTO DEL SISTEMA

Cada instalación del sistema Sigsaly era completa y única, (Figura 10). Además del equipo y los platos giradiscos, se incorporaron otros aparatos auxiliares como osciloscopios o receptores de alta frecuencia que facilitasen la obtención de señales para la sincronización entre ambos extremos. Éstos añadían más peso y volumen al conjunto. Diariamente, se ajustaban los niveles de potencia y la precisión de los convertidores.

LAS PATENTES "SECRETAS"

Sigsaly originó más de treinta patentes. Algunas se han descrito en la serie de artículos anteriores de esta revista. Estas patentes han sido "secretas" durante tres décadas. Pero esta afirmación no es correcta porque una patente es un documento público depositado en la Oficina de Patentes y, por lo tanto, no puede ser secreto. Lo que ocurrió con las patentes solicitadas durante la guerra fue que el proceso de solicitud quedó en "suspenso" por motivos de seguridad nacional.

En 1936, el gobierno americano, a través de la United States Patent and Trademark Office, USPTO, decretó que la solicitud de una patente podía ser declarada como "reservada" y no se publicase en el boletín cuando afectase a la seguridad nacional. Esta etapa forma parte del proceso de declaración de una patente. Se publican las nuevas solicitudes para que terceras personas las conozcan y puedan reclamar si consideran que los inventos descritos ya están patentados. La USPTO dejó en reserva muchas patentes; aunque permitió la fabricación o comercialización de estos inventos, tal como hizo los laboratorios Bell.

En 1971, IBM comenzó a informatizar los archivos de la USPTO; y tal vez, por este motivo fue necesario actualizar la situación aquellas solicitudes reservadas.

Figura 10. Instalación de Sigsaly. Cortesía National Security Agency.

En 1974 la Oficina de Patentes pidió a los solicitantes si querían continuar con el procedimiento de concesión de la patente. En 1976, finalizó el periodo de reclamaciones y se concedieron las patentes, aunque para muchas había pasado el periodo de concesión. Por este motivo muchas de ellas asociadas al proyecto de Sigsaly tienen la fecha de la concesión de 1976. La U. S. Navy, la U. S. Energy y los Bell Telephone Laboratories fueron las entidades que tuvieron más patentes reservadas.

CONCLUSIÓN

En 1983, el Institute of Electrical and Electronic Engineers (IEEE) a través de W. Bennett reconoció, y reproducimos tal como lo expresó, que Sigsaly fue el primer aparato electrónico que:

— Encriptó comunicaciones telefónicas.

— Comprimió el ancho de banda vocal.

— Realizó una modulación de voz en PAM (Pulse Amplitude Modulation)

— Transmitió señal vocal con pulsos cuantificados en un modelo no lineal similar de compresión-expansión.

— Moduló por desplazamiento de frecuencia Frequency Shift Keying, FSK.

— Utilizó de forma combinada FSK - FDM (Frequency Shift Keying-Frequency División Multiplex) como método capaz de transmitir por radio.

— Aplicó la técnica de medida basada en el patrón de "ojo" de señales multinivel para ajustar los intervalos de las señales muestreadas.

La historia de las comunicaciones telefónicas encriptadas que se ha mostrado en los artículos "Voces secretas" de la revista *Antena* culmina con este equipo. A partir de este momento con la electrónica digital, comenzará otra forma de afrontar la encriptación de las comunicaciones. Pero hemos descubierto que los conceptos fueron experimentados y corroborados décadas antes de la llegada de los ordenadores.

REFERENCIA

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

BOONE, James V. y Peterson, R. R. "The start of the digital revolution" en: http://www.nsa.gov/about/cryptologic_heritage/center_crypt_history//publications/sigsaly_start_digital.shtml

CHRISTENSEN, Chris. "Gabinet War Rooms. Sigsaly" http://www.nku.edu/~christensen/SIGSALY.pdf

IMPERIAL WAR MUSEUM. http://cwr.iwm.org.uk

NATIONAL SECURITY AGENCY. Museo Nacional de Criptología. http://www.nsa.gov/about/cryptologic_heritage/museum/index.shtml

REAL Martín, Luis Fernando. "Voces secretas. El stepper circuit y la aritmética modular" *Antena* Núm. 183, abril 2011. Edita COITT. http://www.coitt.es/res/revistas/04b%20Voces%20secretas.pdf

"Voces secretas. El Vocoder, el ruido y los conmutadores" *Antena* Núm. 180, septiembre 2010. Edita COITT. http://www.coitt.es/res/revistas/05aRepVocesRH1.pdf.

"Voces secretas. Encriptación telefónica en los años 20" *Antena* Núm. 179, abril 2010 COITT. http://www.coitt.es/res/revistas/06a_Voces_PU1.pdf.

"El Voder, el mundo del mañana" *Antena* Núm. 176, junio 2009. COITT. http://www.coitt.es/res/revistas/08d_Rep_Voder_MN3.pdf

"El Vocoder, la voz de la lluvia" *Antena* Núm. 173, septiembre 2008. Edita COITT. http://www.coitt.es/res/revistas/05b_Vocoder.pdf

SINGH, Simon. *Los códigos secretos*. Ed. Debate 2000. Madrid.

WEADON, Patrick. "The Sigsaly story" en: http://www.nsa.gov/about/cryptologic_heritage/center_crypt_history//publications/sigsaly_story.shtml