Las conversaciones telefónicas difícilmente podían ser privadas. Cualquier individuo podía «pinchar» los cables. La propia AT&T, para mantener en secreto sus propias comunicaciones corporativas, donde los empleados de las centrales o del campo —en los tendidos— podían escuchar las conversaciones de sus directivos, fue pionera en el desarrollo de sistemas de encriptación telefónicos.
Los primeros encriptadores se basaron en la alteración de los parámetros de los sonidos: la frecuencia, el retardo o la amplitud. ¿Lo consiguieron? ¿Cómo estaban diseñados aquellos encriptadores?

Voces secretas. Encriptación telefónica en los años 20

Luis Fernando Real Martín.
Ingeniero Técnico de Telecomunicación

Luis Fernando Real Martín.
La primera generación de estos complejos ingenios militares combate ahora mismo en primera línea de batalla en Afganistán.

«Los hombres-máquina no tenían nombre, sino que empleaban letras y números. Hablaban mediante impulsos de pensamiento, pues no necesitaban producir vocalmente un sonido ni oírlo.»

«El satélite Jameson». Neil Jones, 1931.
(en «La Edad de Oro de la Ciencia Ficción» Isaac Asimov)

Poste telefónico. Fotografía del autor

TELEGRAFOS DE BAUDOT Y ENCRIPTADORES DE VERNAM

Como siempre en telecomunicaciones, el telégrafo es el origen. Gilbert S. Vernam inventó durante la Primera Guerra Mundial un método para encriptar los telegramas enviados con aparatos del sistema Baudot (Figura 1). Las letras del alfabeto en el código de Baudot, a diferencia del Morse, constan siempre de cinco dígitos y dos estados posibles en el

Figura 1. Baudot fabricado por J. Carpentier, Paris, 1902 Num. serie: 1982
Cortesía Asociación de Amigos del Telégrafo de España.

Teléfono de campaña del ejército francés, Primera Guerra Mundial. Musee de l'Armee. París. Fotografía del autor.

circuito: con señal o sin señal. El telegrafista pulsa las cinco teclas del manipulador y un distribuidor rotativo envía las corrientes de cada una seriadas a la línea (Figura 2). El receptor decodifica, traduce y escribe automáticamente el mensaje en una cinta u hoja de papel.

Vernam añadió al Baudot unos relés y un mecanismo tractor de cinta de papel perforada, similar a los utilizados en el telégrafo Wheatstone. La funcionalidad consistió en que el mensaje del telegrafista, convertido en las señales eléctricas del código baudot, se modificaba por otras señales eléctricas activadas por los relés. Los relés actuaban según un orden de intervención preestablecido marcado con las perforaciones de la cinta de papel. La selección de perforaciones en la cinta constituía la clave para la codificación y decodificación de cada letra del mensaje original. Ver Figura 3. Las tensiones del teclado alimentaban los bobinados de cinco relés, T_1 a T_5. Cinco agujas, Cl_1 a Cl_5, pasaban por los orificios de la cinta de papel y cerraban el circuito de una batería. Los relés del segundo grupo se excitaban dependiendo de la combinación de tensiones que recibían, por un lado, de las teclas del telegrafista: o sea, del mensaje, y por el otro, de las agujas, la clave de la cinta. Las armaduras de los segundos relés, en reposo o excitados, enviaban los pulsos cifrados, S_1 a S_5, al distribuidor rotativo. La rotación servía para avanzar la cinta y así cambiar la clave para cada letra. El receptor realizaba la decodificación con otra cinta idéntica antes de imprimir los caracteres tipográficos con el Combinador Baudot.

Los relés realizan una suma algebraica binaria en módulo 2 entre el código del mensaje y la clave. Se conoció como «Suma Vernam». El sistema funcionaba muy bien con el sistema de clave creado por Blaise de Vigenère allá, en 1586.

El sistema Vernam se utilizó hasta los años treinta. Pero en esa década se inventaron otros sistemas electromecánicos más complejos que culminaron en la Segunda Guerra Mundial con «Enigma» en Alemania (Figura 4) o «Purple» en Japón entre los más conocidos.

El telégrafo Baudot nos dejó dos herencias. En honor a su inventor Jean-Maurice-Émile Baudot (1845-1903) se denomina «baudio» a la unidad con la que se expresa el número de símbolos (o unidades de código) que se transmiten durante un segun-

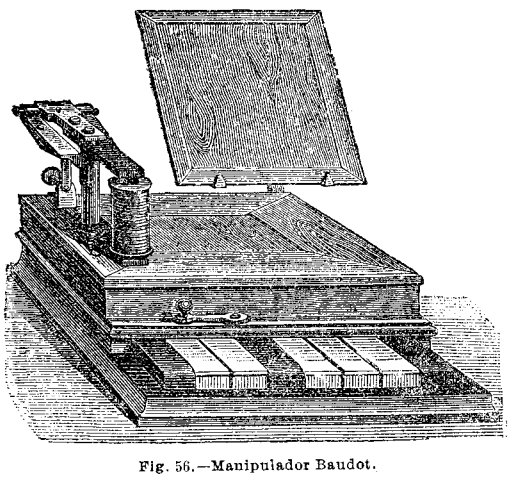

Fig. 56.—Manipulador Baudot.

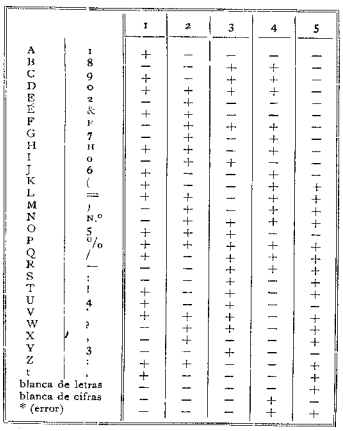

Figura 2. Grabado del Telégrafo y código Baudot. En «Telegrafía eléctrica», F. Villaverde. Ed. Espasa Calpe (sin fecha).

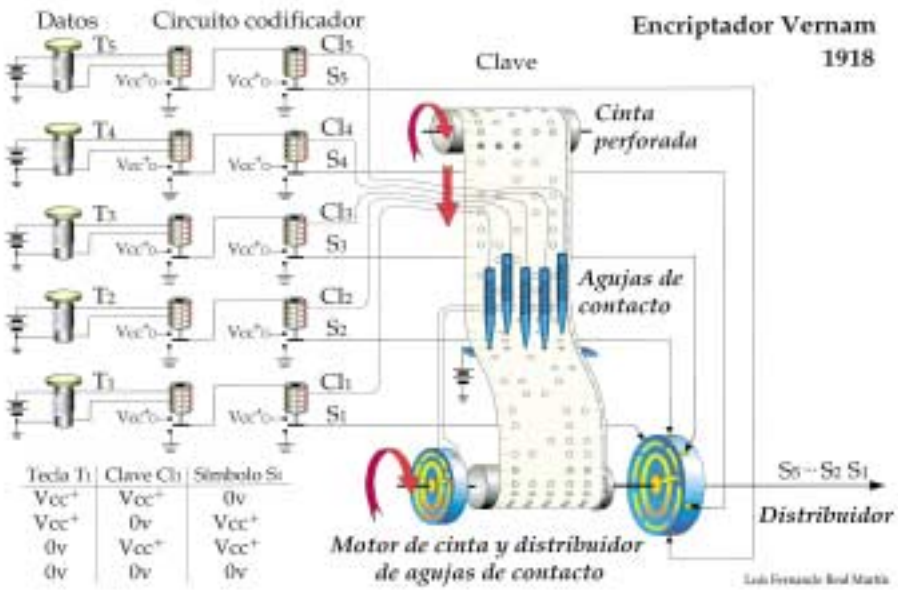

Figura 3. Telégrafo Vernam, 1918. Dibujo del autor.

Figura 4. Máquina Enigma. Musee de l'Armee. París. Fotografía del autor.

do. La segunda es el estándar Código Alfabético Número 2 (Figura 5) del CCITT (ahora ITU-T) que realizó Donald Murray en 1903 modificando el código Baudot, éste fue el Código Alfabético Número 1.

ENCRIPTADORES TELEFÓNICOS

Los telegramas, con claves conocidas solo por los interlocutores son fáciles de ocultar. Pero las conversaciones telefónicas son más complejas. ¿Cómo se puede manipular la señal analógica sin distorsionar la voz que saldrá por el altavoz? En los años veinte no fue fácil conseguirlo. El trabajo fue lento y laborioso, no existía la tecnología digital, ni siquiera el transistor. Desde el punto de vista tecnológico el reto fue enorme, tanto como su olvido histórico.

Figura 5. Alfabeto Telegráfico CCITT nº 2. Cortesía Asociación de Amigos del Telégrafo de España.

Los primeros métodos de encriptación se basaron, por un lado en alterar algún parámetro de la señal eléctrica vocal analógica: la frecuencia, la fase o la amplitud y por otro, en utilizar la recién descubierta técnica de la modulación, tanto para transmitir la voz por radio como por cable. Con la modulación, la encriptación parecía segura. Pero como se demostraría durante la Segunda Guerra Mundial, el rastreo de ondas con oscilógrafos y detectores superheterodinos tarde o temprano descubría y demodulaba las señales y desvelaba los mensajes.

Conozcamos dos ejemplos de estas técnicas.

NYQUIST Y LAS LÍNEAS DE RETARDO

Harry Nyquist basó su encriptador en los resultados de los estudios sobre la voz humana de Irving B. Crandall y Harvey Fletcher. Crandall llegó a estimar que un retardo de 0,1 segundos en los sonidos de algunas consonantes era suficiente para que fuesen confundidas y algunas palabras no se entendiesen. Nyquist pensó que un circuito capaz de provocar un retardo similar haría ininteligible los mensajes de voz que se escuchase «pinchando» en los cables telefónicos.

En 1927 diseñó su circuito. Se basaba en la alteración de varios intervalos de frecuencia del espectro telefónico (de 300 a 3.500 Hz), Figura 6. Consistía en una línea de retardo, Red 1, construida con secciones de filtros de resistencias, bobinas y condensadores encadenadas en serie. Cada sección producía un retardo diferente en un grupo de frecuencias. La línea se intercalaba en los cables del teléfono. En el otro extremo, otra línea con la función de transferencia complementaria, Red 2, devolvía a la señal vocal sus características originales.

El resultado práctico no fue el deseado. El ajuste de cada filtro repercutía en los adyacentes alterando los resultados previamente conseguidos. La tarea fue tediosa y complicada. Los componentes eran disipativos con el consiguiente consumo de energía. Hubo que recurrir al uso de amplificadores de válvulas, complicando y encareciendo el circuito. La línea del transmisor tenía 265 secciones (filtros en celosía con 8 componentes cada uno), pero la línea del receptor, para conseguir la función complementaria, tenía 735 secciones. Esto da idea de la magnitud y complejidad del circuito y su inviabilidad práctica.

HARTLEY Y LA MODULACIÓN SIN PORTADORA FIJA

Ralph L. V. Hartley inventó su sistema de encriptación de voz en 1920. Al transmitir una señal modulada hay que enviar la portadora para su demodulación en el receptor. Cualquier persona ajena que «pinchase» los cables telefónicos dispondría de la señal portadora, y fácilmente podría recuperar la información original. Hartley propuso que se modulase con una portadora variable dentro de

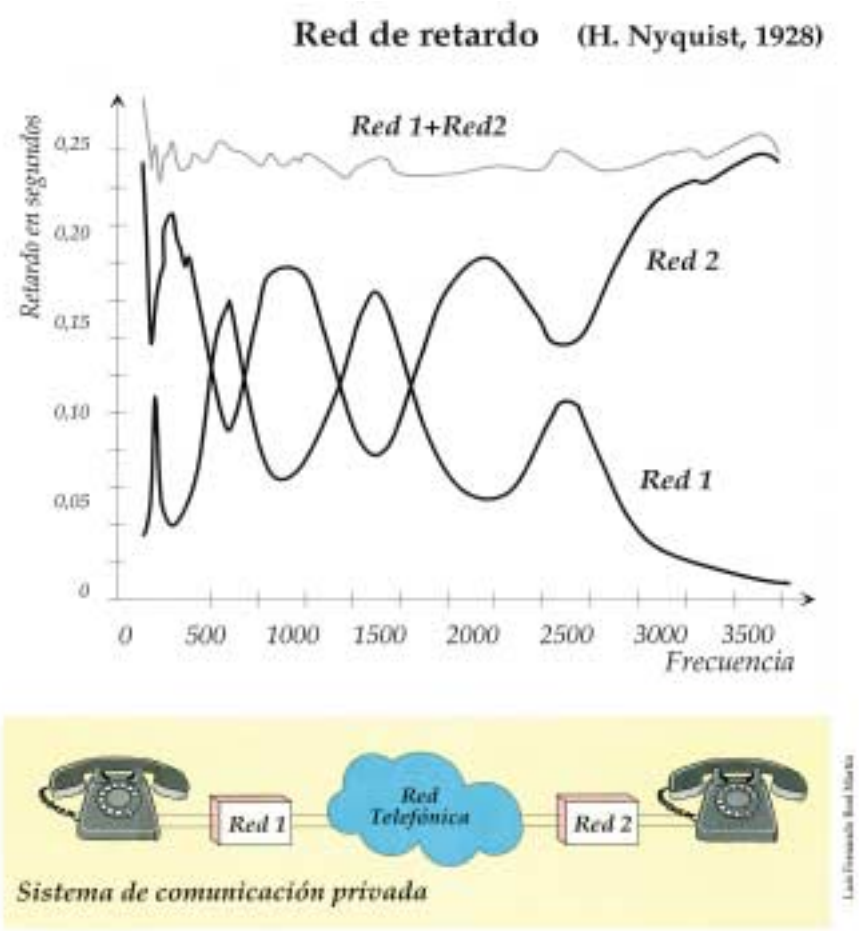

Figura 6. Redes de retardo de H. Nyquist, 1928. Dibujo del autor.

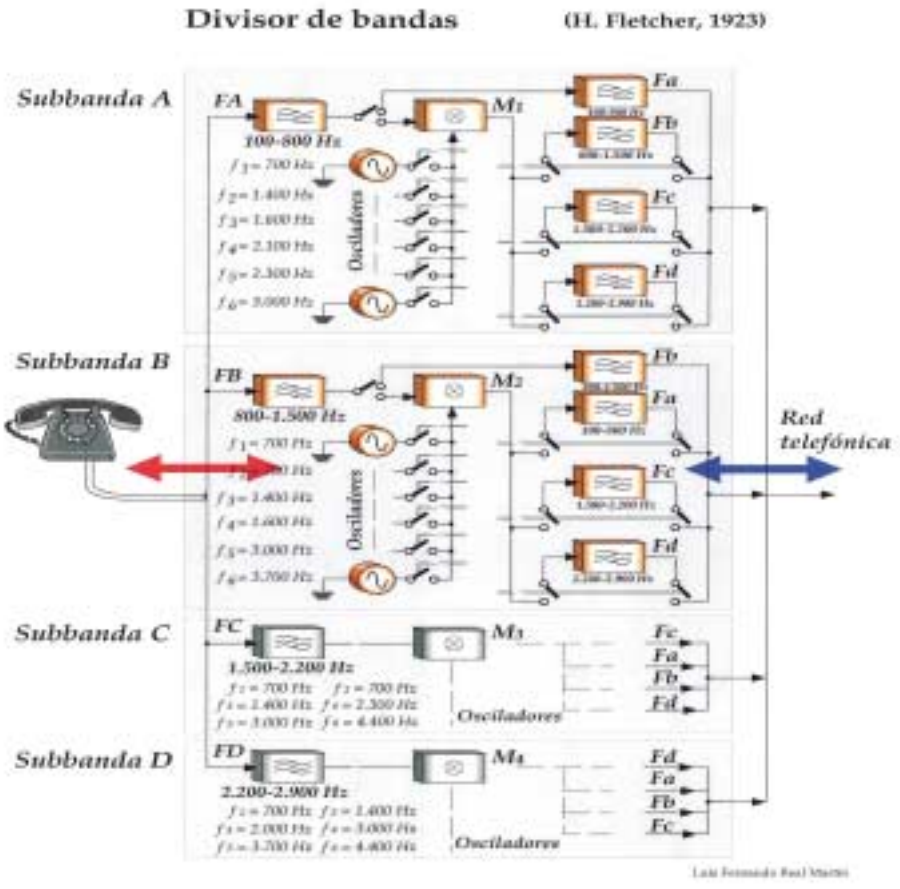

Figura 7. Sistema encriptador de H. Fletcher, 1923. Dibujo del autor.

un rango limitado de frecuencia. Al receptor se le transmitirá sólo el intervalo de la variación porque la frecuencia patrón para la portadora variable estaría preestablecida secretamente entre ambos interlocutores y se generaría localmente. A partir de la patrón, el receptor comenzaría a variar la frecuencia y demodular la señal recibida.

En 1925 publicó un artículo que exponía las ventajas de transmitir por radio una banda lateral sin portadora, resultado de sus experiencias.

ENCRIPTACIÓN POR TRANSPOSICIÓN: TÉCNICAS DE DIVISIÓN DE FRECUENCIA

En los años treinta cambia la forma de trabajar y considerar las señales eléctricas. Con nuevos conceptos y herramientas matemáticas, se abordan en el dominio del tiempo y en el de la frecuencia. Se emplean técnicas múltiplex (Time División Multiplexing, TDM) ya ampliamente utilizadas desde el siglo XIX en telegrafía. En el dominio de la frecuencia, son los circuitos encriptadores los que contribuyeron decisivamente al desarrollo de las nuevas técnicas múltiplex de frecuencia (Frequency División Multiplexing, FDM).

Los técnicos comenzaron a trabajar por la sencilla técnica criptografía de *transposición*. En un texto escrito por ejemplo, esta técnica consiste en que son las propias letras del mensaje plano las que se intercambian de posición según una «regla» o criterio que tienen en común el emisor encriptador y el receptor desencriptador. Una regla sencilla sería intercambiar cada letra con la siguiente; u otra más compleja intercambiar la quinta con la octava, la novena con la segunda, etc. La regla de transposición es la clave. Con las señales eléctricas, ¿cómo se pueden fragmentar, trasponer y volver a recuperar?. La respuesta está en el dominio de la frecuencia. El espectro se fragmenta en subbandas y estas son recolocadas en posiciones diferentes, como las letras del texto plano. Uno de los pioneros en estas técnicas fue Harvey Fletcher.

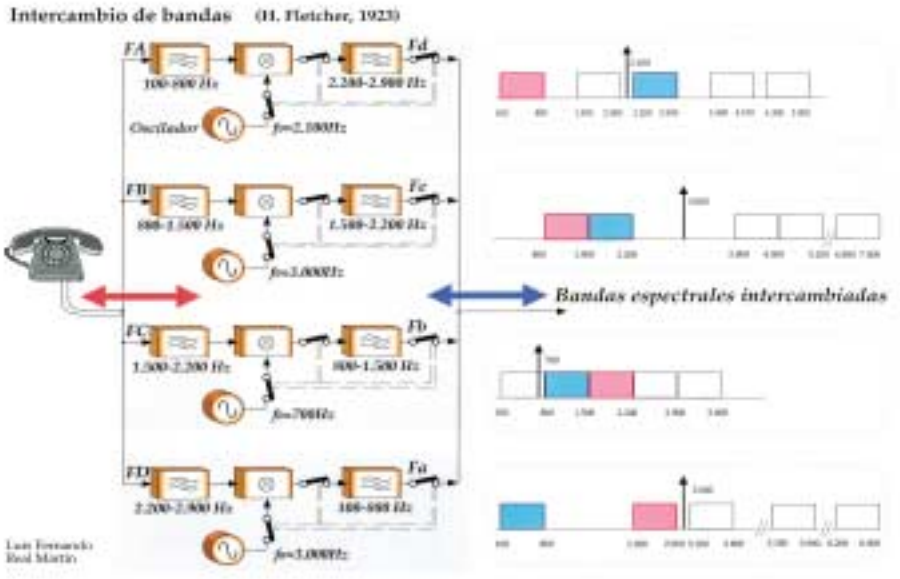

Figura 8. Ejemplo de subbandas traspuestas. Dibujo del autor.

HARVEY FLETCHER , LLOYD ESPENSCHIED Y CHARLES WEIS

Durante su estancia en los laboratorios de Western Electric, H. Fletcher desarrolló aparatos y técnicas para medir la calidad y eficiencia de la señal vocal en los teléfonos. La comprensión de las cualidades y características de la voz le llevó a la conclusión que no existía una relación directa entre el grado de inteligibilidad de una subbanda y la energía que posee, de modo que sería posible dividir el espectro vocal en subbandas de la misma anchura o del mismo contenido en energía y cada una con diversos grados de inteligibilidad (Ver Tabla).

Entre 1922 y 1924, diseñó un sistema de encriptación basado en la división del espectro vocal en subbandas. El secreto de la comunicación se conseguía «transponiendo» el orden de las posiciones de las subbandas para formar un nuevo espectro con la misma ocupación que el original. Estas manipulaciones no debían alterar la inteligibilidad del mensaje una vez recuperado el espectro original.

El aparato de Fletcher se representa en la Figura 7. Cuatro filtros dividían el espectro vocal: *FA*, *FB*, *FC* y *FD*. Sus salidas eran moduladas con los moduladores M_1 a M_4 y generaban las bandas laterales. Otros filtros, de *Fa* a *Fd*, seleccionaban una de ellas, (los subíndices indican la posición a la salida con respecto a la original de entrada). Con la elección de las portadoras y los filtros adecuados se conseguía recolocar las bandas laterales sin solaparse. La Figura 8 muestra en rojo las subbandas iniciales *A*, *B*, *C* y *D* y en azul su transposición en *a*, *b*, *c* y *d*.

La recuperación del espectro original se hacía del siguiente modo. La banda lateral seleccionada en cada salida era realimentada en la entrada de su mismo modulador. Esta sufría una segunda modulación donde la posición de una de las nuevas bandas laterales coincidía con la subbanda original de entrada. De este modo se convierte a la vez en el sistema bidireccional, modulador en un sentido y demodulador en el otro.

La selección de un oscilador de una portadora u otra y los filtros de entrada y de salida se efectuaba mediante conmutadores. La información de cuáles son los que se conectan y desconectan constituía la «clave».

Ancho de banda	Energía (%)	Inteligibilidad (%)
0 – 800 Hz	72	16
800 – 1.600 Hz	18	27
1.600 – 3.000 Hz	6	25

Fletcher simplificó este circuito para la radio, Figura 9, resultando mucho más práctico.

Años más tarde, en 1925, Lloyd Espenschied y Glenn Gillett copiaron el diseño de Fletcher. Sustituyeron los conmutadores manuales por relés, automatizando parcialmente el sistema, Figura 10. Añadieron un panel con numerosas clavijas que conectaban los relés necesarios para conmutar los osciladores y filtros. Las clavijas proporcionaban las combinaciones para la selección de las subbandas.

El panel con las clavijas añadía una nueva cualidad dinámica al método de encriptación. Se podían seleccionar varias combinaciones durante el trascurso de la misma comunicación. Cinco relés eran los encargados de conectar y desconectar las clavijas. La activación de cada relé dependía de la traducción de un código leído en una cinta perforada. Una señal enviada desde el otro extremo sincronizaba el avance de las cintas.

Espenschied y Gillett añadieron más dificultad al sistema de Fletcher. Tanto por el número de clavijas como por el orden y la duración de su conexión, que se fijaba en el código de la tarjeta perforada. Toda esta información es la «clave» de la regla de transposición de las subbandas.

Espenschied provenía del mundo de la radio. Para él, era obvia una convergencia de las técnicas de la radio y de la telefonía para la comunicación y así lo dejó escrito en un artículo *Proceedings of the Institute of Radio Engineers*, IRE, de 1913. Sugirió el empleo de moduladores para enviar más canales telefónicos en bandas laterales y optimizar el rendimiento del cableado aprovechando un ancho de banda. En 1927 consiguió me-

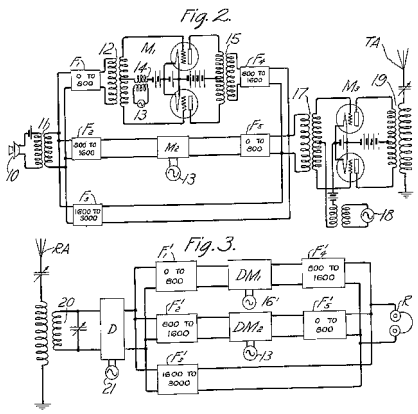

Figura 9. Sistema encriptador para radio de H. Fletcher, 1923. Dibujo de patente.

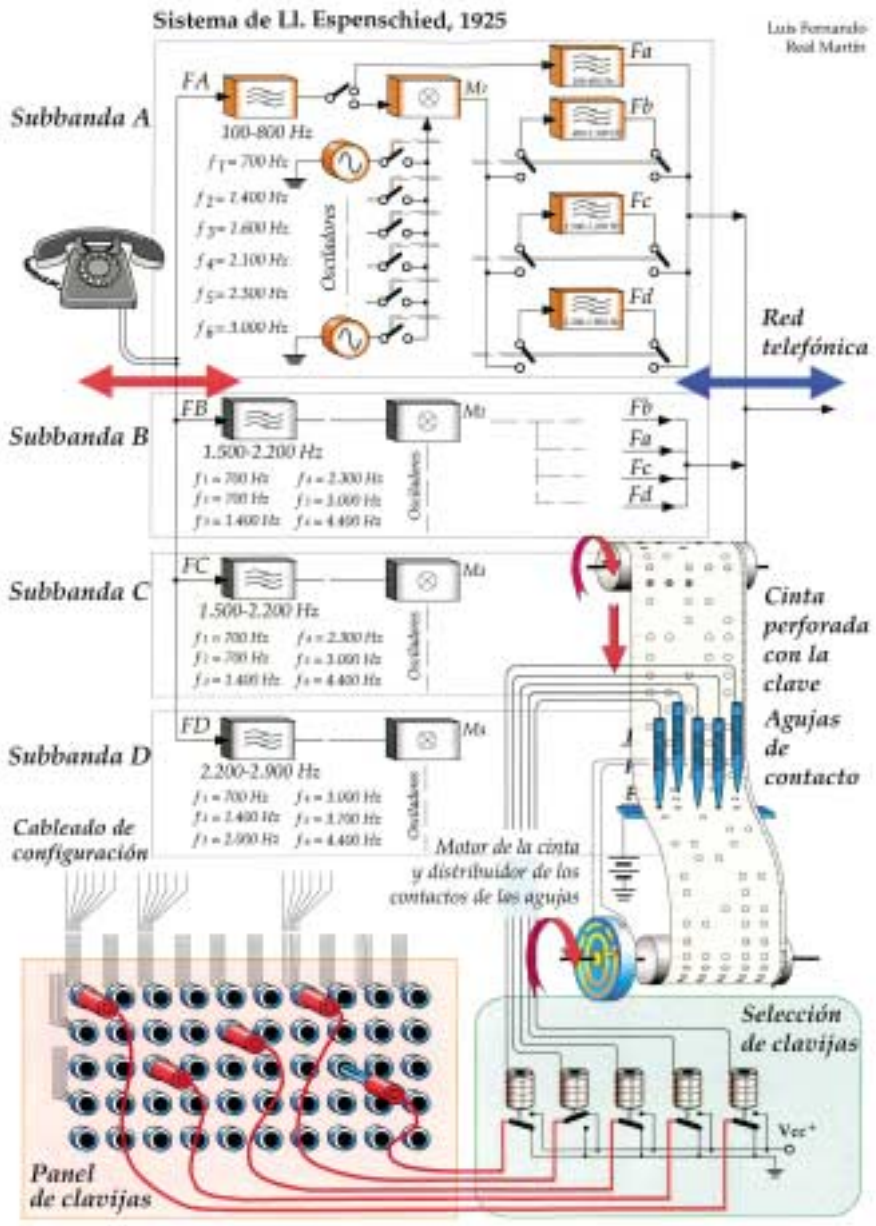

Figura 10. Sistema encriptador de Ll. Espenschied y G. Gillett, 1925. Dibujo del autor.

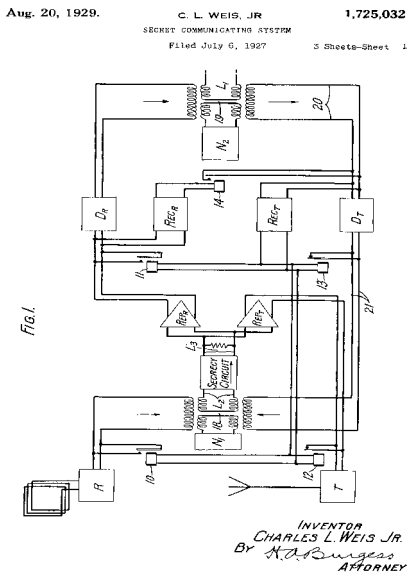

Figura 11. Hoja de la patente de Ch. Weiss, 1927.

REFERENCIAS

AT&T. www.att.com/history/index.html

BELL SYSTEM www.bellsystemmemorial.com

BELL TELEPHONE LABORATORIES.
www.bell-labs.com/about/history/index.html

ESPENSCHIED, LLOYD / FLETCHER, HARVEY
www.ieee.org/organizations/history_center/legacies/legaciestoc.html

ESPENSCHIED, Lloyd y Gillett D., Glenn. Estados Unidos patente núm: 1.709.901. «Secret signaling system». 23 abril 1929.

FLETCHER, Harvey. Estados Unidos patente núm: 1.573.924. «Secret signaling». 23 febrero 1926.

FLETCHER, Harvey. Estados Unidos patente núm: 1.533.311. «Secret signaling». 14 abril 1925.

HARTLEY, Ralph V. L. Estados Unidos patente núm: 1.571.005 y 6. «Secret signaling». 26 enero 1926.

NYQUIST, Harry y Merts, Perre. Estados Unidos patente núm: 1.726.578. «Secret telephone system». 3 septiembre 1929.

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

VERNAM, Gilbert S. Estados Unidos patente núm: 1.310.719. «Secret signaling system». 22 julio 1919.

VERNAM, Gilbert S. «Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications» *Transactions A.I.E.E.* Febrary 1926. EE. UU.

WEIS, Charles L. Estados Unidos patente núm: 1.725.032. «Secret communicating system». 20 agosto 1929.

jorar esta técnica con la invención del cable coaxial.

La novedad sobre el circuito de Fletcher fue el cambio dinámico de las portadoras durante la comunicación. Sobre esta idea, se desarrollarían las técnicas de expansión del espectro, siendo el circuito de Espenschied primigenio.

El sistema de intercambio de subbandas lo simplificó Charles Weis para la radio. Suprimió los conmutadores y filtros y añadió la posibilidad de una segunda modulación opcional para cada subbanda. La reubicación de las subbandas se conseguía con la combinación de los segundos moduladores, Figura 11.

CONCLUSIÓN

Hemos visto sólo unas muestras de sistemas de encriptación telefónica de los años veinte, a cuyo reto imaginativo no escaparon prestigiosos técnicos. Estos ejemplos fueron desarrollados por AT&T, habrá que investigar otras empresas.

El encriptador de voz más comercializado ha sido el Secráfono, heredero de los sistemas de modulación. Este dispositivo modula, e intercambia las bandas laterales.

Nos adentraremos en los años treinta. El siguiente paso será la división de la banda vocal en subbandas que se multiplexan en frecuencia y en el tiempo. La tecnología permite más complejidad. Lo veremos en otro artículo.