341955

341955

MEMORIA DESCRIPTIVA PARA SOLICITAR PATENTE DE INVENCION EN ESPAÑA POR: "GENERADOR DE MATERIAL DE CLAVE" A NOMBRE DE STANDARD ELECTRICA S.A. CON DOMICILIO EN MADRID, CALLE DE RAMIREZ DE PRADO Nº 5

Resumen de la descripción

El invento se refiere a un generador de material de clave para producir secuencias pseudo al azar, que tienen uno o más registradores de cambio no lineales conectados para realimentación.

Cada registrador comprende una pluralidad de circuitos flip-flop conectados de forma que el funcionamiento del registrador sea tal que los contenidos siguientes de un flip-flop arbitrario sean iguales a la suma de módulo 2 del contenido presente del flip-flop en cuestión y el flip-flop precedente.

Referencias a aplicaciones en relación con ésta.

Esta aplicación tiene relación con las aplicaciones copendientes de P.R. Abrahamsen - K. R. Meisingset (3-13) por Unidad de Cifrado y a la de K. R. Meisingset - I. Ho - P. R. Abrahamsen (12-5-2) Método para cifrar un texto de teleimpresor para canales telex.

./..

341955

Antecedentes del invento

El presente invento se refiere á un generador de material de clave para equipo criptográfico de teleimpresor y en particular a un generador de material de clave para producir secuencias pseudo al azar.

Se conocen muchos tipos de generadores de material de clave con rotores mecánicos o con contadores en anillo, electricos.

Estos generadores de material de clave no se consideran, sin embargo adecuados para dar secuencias suficientemente largas en todos los casos.

Resumen del invento

El objeto del presente invento es proporcionar un generador de material de clave que con circuitos relativamente sencillos sea capaz de dar secuencias pseudo al azar muy largas.

La característica principal del invento es que comprende uno o más registradores de cambio no lineales conectados realimentados.

Otra característica es que cada registrador comprende una pluralidad de circuitos flip-flop de disparo, estando conectadas las entradas de control de cada uno de estos circuitos a la salida del circuito precedente de forma que la operación del registrador es tal que el contenido siguiente de un flipoflop arbitrario es igual a la suma de módulo 2 de los contenidos presentes del flip - flop en cuestión y el flip - flop precedente.

Breve descripción de los dibujos

Las antes mencionadas y otras características y objetos del presente invento quedarán más claros como consecuencia

./..

de la siguiente descripción detallada de una realización el invento, dada en relación con los dibujos que se acompañan en los que:

La figura la representa un diagrama de bloque funcional de una realización del invento.

La figura lb representa un diagrama de bloque que muestra las interconexiones principales entre los bloques.

Las figuras lc-i y 2a-h representan los esquemáticos detallados de la mayoría de los bloques representados en las figuras la y lb.

La figura 3 representa un esquemático detallado del bloque 6 de la figura 2a, un generador de un impulso (OS),

La figura 4 representa un esquemático detallado del bloque 5 de la figura 2a, un circuito de reposición (RES) y un generador de impulsos de reloj (OSC de 25 KHz),

La figura 5 representa un esquemático detallado del bloque 14 de la figura 2a, un amplificador excitador de teloimpresor (DA) y un circuito de lectura (RC),

La figura 6 representa los diferentes símbolos lógicos que se usan en las figuras lc-i y 2a-h, y

La figura 7 representa como puede disponerse las figuras lc-i y 2a-h para constituir un diagrama completo de circuito.

Descripción de una realización preferida

DIAGRAMA FUNCIONAL DE BLOQUE

En la figura la se ha representado un diagrama funcional de bloque que tiene una estrecha relación con el esquemático de bloque detallado. Las partes principales siguientes del diagrama de bloque se explicarán con algún detalle a continua-

./..

ción.

El generador de elementos de clave pseudo al azar.- Generador del número "P" de 5 bits.- Contador "C(P)".- Registrador de entrada "Reg X".- Cuadro de terminales Clavija A. A continuación, el procedimiento de puesta en marcha y los procedimientos de cifrado y descifrado y el funcionamiento telex son tambien explicados en relación con el diagrama funcional de bloques.

Generador de elementos de clave pseudo al azar

El generador de clave comprende dos registradores de cambio no lineales realimentados, llamados REG I y REG II respectivamente. Los dos registradores tienen 15 pasos, teniendo REG I doce de ellos situados en el bloque 10 y tres en el bloque 12, y REG II tiene 12 pasos en el bloque 11 y tres pasos en el bloque 12.

Los circuitos lógicos no lineales de realimentación para ambos registradores están situados en el bloque 12.

Se verá del diagrama de bloques que las dos salidas de los registradores se suman juntas módulo-2- y que la secuencia resultante se almacena en REG Z del bloque 9. Durante el cifrado o el descifrado se cambiarán los dos registradores, para presentar siempre un caracter de clave nuevo en REG Z.

Todas las salidas de los dos registradores se llevan a columnas diferentes de un cuadro de terminales.

Las salidas usadas para las funciones de realimentación no lineal se eligen por medio de patillas en el cuadro de terminales.

Para el registrador I, las filas F, G, H y K determinan la función no lineal de realimentación, y para el registrador II las filas S, T, V y W.

./..

Generador del número "P" de 5 bits

"P" es un número de 5 bits pseudo al azar producido por los dos registradores principales por medio de cinco salidas de cada registrador, seleccionadas por medio de patillas en el cuadro de terminales.

Se verá que las filas del cuadro de terminales A, B, C, D, E, H, M, P, [illegible] y R se llevan al bloque 8, y a los circuitos de ajuste para el contador binario "C(P)".

Cada una de las cinco señales de entrada del juego es una adición de módulo 2 de una señal de salida de REG I y una señal de salida REG II. Así se comprenderá que estas señales combinadas son tambien pseudo al azar.

Contador "C(P)"

El contador binario del bloque 7 contará siempre hacia atrás.

La función de este contador es controlar el número de impulsos de cambio llevados al registrador de entrada REG X.

Durante el cifrado, el número "P" se ajusta inicialmente en el contador binario lo que quiere decir que REG X está alimentado con "P" impulsos de cambio, pero durante el descifrado se coloca inicialmente el número 31 - "P" en el contador.

Tambien durante el descifrado el contador se parará cuando contenga un 1 en vez de un 0, lo que quiere decir que ahora contará 31 - "P"-1, es decir 30-"P".

El significado de esto quedará claro cuando se describan los procedimientos de cifrado.

Registrador de entrada REG X.

El REG X del bloque 2 consta de 5 pasos iguales de los que uno típico se ha representado en la figura 1a. Además tiene un sexto paso que es una especie de paso separador. REG X tiene dos modos de

funcionar.

a) Trabaja como un registrador normal de cambio de 5 bits recibiendo los impulsos de cambio del contador de entrada del bloque 4. La entrada al primer paso viene del teleimpresor a través del circuito de lectura del bluqe 14. (Esta conexión no se ha representado en el diagrama funcional de bloque).

b) Trabaja como un registrador de cambio realimentado comprendiendo cada paso un sumador de módulo 2 y un circuito flip-flop, en el que cualquier salida puede conectarse a cualquier entrada por medio de conexiones soldadas en la clavija de clave representada a la izquierda, y estas dos conexiones se hacen de forma que resulte una longitud máxima de secuencias de $2^5 - 1 = 31$. Este comportamiento está simbolizado en la figura 1a por la X que viene a través de la clavija A a la izquierda a través del sumador de módulo 2 del bloque 1 y a través de la entrada lógica del bloque 2 al flip-flop.

Tambien es posible ajustar cada bit del registrador de 5 bits REG X al resultado de la adición de módulo-2 de un bit en el mismo registrador REG X y un bit correspondiente en REG Z. Esto se simboliza en la figura 1a por el sumador inferior de módulo 2 del bloque 1 con entradas X y Z.

Cuadro de terminales

El cuadro de terminales es un cuadro con 10 regletas terminales horizontales y 30 regletas terminales verticales dispuestas en una matriz con 300 posiciones de trabajo (puntos de cruce). Las regletas terminales verticales están conectadas a 30 salidas de los dos registradores principales. Salidas arbitrarias de estos dos registradores pueden conectarse a las filas horizontales por medio de patillas insertas en los puntos de cruce en este cuadro de terminales. Entonces estas salidas arbitrarias llevarán las funciones no lineales de realimentación y a los circuitos de colocación para el nú-

./..

mero "P", Tambien es posible, por medio de la fila L del cuadro de terminales ajustar los dos registradores inicialmente con un contenido inicial.

Clavija A

Cuando REG X trabaja como un registrador de cambio realimentado, las cinco señales de realimentación se realimentan a las cinco entradas a través de la clavija A representada en la esquina superior izquierda del diagrama de bloque funcional. Cuando se hacen adecuadamente los puenteados en esta clavija, REG X circulará a lo largo de una secuencia de longitud máxima, es decir un ciclo de 31.

Otras partes representadas en el diagrama funcional

Resulta claro del diagrama funcional de bloque que es posible ajustar REG Z a partir de un lector de cinta a través de la lógica de entrada del bloque 9. Este modo de operación puede ser usado por aquellos usuarios que requieran una completa seguridad de sus mensajes. Los registradores principales REG I y REG II no funcionan durante este modo de operación, de forma que la entrada a la izquierda de REG Z es cero. En este caso, la secuencia de clave viene de una cinta al azar inserta en el lector de cinta.

REG Y, situado tambien en el bloque 9 se usa solamente durante la fase de arranque como registrador separador de la unidad de cifrado. El bloque 3 contiene tres circuitos de los que todavía no se ha hablado.

1) EL MEMO FF es un circuito flip-flop que recuerda si se ha detectado o no el caracter RETROCESO DE CARRO.
2) El circuito SET/RESET se usa durante la fase de arranque para reponer el registrador de entrada y los dos registradores principales.
3) El bloque llamado K1 - K5 es un registrador normal de cambio que está conectado como un contador de anillo, y que se usa para controlar los procesos de cifrado y descifrado. Durante el cifrado

./..

el contador de programa funciona como sigue: En K_1 se lee el caracter de teleimpresor en el registrador REG X, en K_2 se prueba el contenido de este registrador para ver si contiene un CAMBIO A CIFRAS o un RETROCESO DE CARRO. Si se detecta un CAMBIO A CIFRAS este caracter se convierte en un RETROCESO DE CARRO. Sin embargo, si se detecta un RETROCESO DE CARRO, se convierte en un AVANCE DE RENGLON. La razón de ésto quedará clara cuando se describa el funcionamiento Telex. En K_3, el número pseudo al azar "P" de 5 bits se lleva al contador binario "C(P)", En K_4 el registrador de entrada REG X se conecta como un registrador de cambio realimentado. El contador "C(P)" cuenta hasta cero y los impulsos de éste se llevan a través de FF_{S1} del bloque 4 al registrador de entrada del bloque 2. En K_5 los contenidos de REG X y REC Z se añaden módulo-2 y el resultado se pone de nuevo en REG X. A continuación se prueban los contenidos para ver si el caracter resultante es un caracter permitido para el fundionamiento telex o no. En caso de que no lo sea se hace una vez más la adición módulo-2. El caracter resultante es siempre entonces un caracter permitido.

El bloque 7 contine dos contadores en anillo llamados $i_1 - i_4$ i_4 y j_1-j_3 respectivamente. La función de estos dos registradores es controlar la fase de arranque. Los dos registradores principales deben partir siempre de un punto al azar para cada nuevo mensaje que tenga que enviarse. Esto quiere decir que tiene que presentarse a él seis caracteres. Los tres primeros se dirigen a REG I y los tres siguientes a REG II por medio de los dos contadores de anillo mencionados.

En el bloque 5 hay un oscilador de alrededor de 25 KHz que dispara un multivibrador de un disparo del bloque 6 que a su vez dispara el contador de entrada del bloque 5. El multivibrador de un disparo puede ajustarse a diferentes retardos por medio de un selec-

./..

tor y así puede realizarse las diferentes velocidades posibles de teleimpresor.

El circuito de reposición (RESET CCT) del bloque 5 se utiliza en el funcionamiento con texto claro o con lector de cinta para reponer los dos registradores del generador de clave.

El circuito lógico TP representado en el bloque 4 es un circuito lógico que determina la señal dada a la bobina de recepción del teleimpresor. Esta señal consiste en un impulso de arranque y uno de parada suministrados por el contador de entrada, y cinco bits de información dados por el registrador REG X. En el modo "CLARO" esta información viene del paso registrador número 1 y el modo"EMISION" o "RECEPCION" del paso separador de REG X. Estas dos entradas están simbolizadas por las letras X_1 y X_6 del diagrama funcional en bloque.

Proceso de cifrado

El proceso de cifrado empieza cuando los circuitos de lectura reciben el impulso de parada de algún caracter de texto claro X por accionamiento del teclado o del transmisor automático del teleimpresor. El circuito de lectura pone en marcha el contador de entrada que a su vez da impulsos de cambio a REG X, REG I y REG II y REG Z a través del flip-flop FF_{S2}. En esta primera fase del proceso de cifrado se conecta REG X como un registrador normal de cambio con entrada de información al primer paso, lo que quiere decir que el caracter de texto claro entrará en REG X mientras que el caracter cifrado procedente es enviado al teleimpresor desde el paso número X_6 a través del amplificador excitador de teleimpresor. Cuando ahora REG X contiene los cinco bits de información, REG Z contiene cinco nuevos bits de clave, y "C(P)" se ajusta a un número nuevo "P". A continuación se conecta REG X como un registrador de cambio realimentado de periodo máximo de periodo 31 y los impulsos del generador de 25 KHz se llevan a "C(P)" y a REG X. El suministro de estos im-

./..

pulsos de cambio de 25 KHz se corta cuando "C(P)" es cero, es decir después de "P" impulsos. REG X ha pasado entonces por "P" estados y el estado actual es por lo tanto una función de "P" que puede simbolizarse por la expresión X(P). Al final REG X se pone en el resultado de la adición X(P) ⊕ Z en la que Z es la salida almacenada del generador de clave. Si la adición da como resultado cualquiera de los caracteres que no son permitidos, se hace la adición una vez más encontrándose así X(P) porque X(P) ⊕ Z ⊕ Z = X(P). En este caso X(P) se usa como un caracter cifrado.

Proceso de descifrado

El proceso de descifrado empieza cuando el circuito de lectura recibe el impulso de arranque del caracter cifrado X(P) ⊕ Z, que se cambia entonces en REG X, mientras que se lee el caracter descifrado precedente es leído por el teleimpresor mediante el amplificador excitador de teleimpresor. Entonces, los contenidos de REG X y de REG Z se suman módulo-2 y el resultado -X(P) ⊕ Z ⊕ A = X(P)- se pone de nuevo en REG X. Ahora puede encontrarse teóricamente el caracter de texto claro cambiando REG X "P" pasos hacia atrás en el ciclo, o cambiando REG X 30-"P" pasos en la dirección de avance. El último método se hace ajustando C(P) a 31 - "P" y contando hasta 1. En la estación receptora la adición REG X ⊕ REG Z se hace tambien, por supuesto dos veces si se detecta un caracter no permitido.

Procedimiento de puesta en marcha

Como se ha explicado antes se necesitan 6 caracteres para dar a los registradores realimentados de cambio principales la información de puesta en marcha. Estos 6 caracteres se insertan en la parte frontal de cada mensaje que tiene que cifrarse y se seleccionan al azar o de acuerdo con alguna lista que dé ciclos largos en el generador de clave. Estos caracteres se cifran antes de transmisión usando un ajuste inicial de los registradores principales desde el

./..

cuadro de terminales que se ha mencionado anteriormente.

Funcionamiento Telex

El texto cifrado no debe contener caracteres que no puedan ser perforados en un teleimpresor normal de una instalación telex o caracteres que puedan perturbar la transmisión en un canal telex, tal como la letra D en cifras. Estos caracteres se evitan no utilizando los caracteres TODO ESPACIO Y CAMBIO A CIFRAS en el texto cifrado. El alfabeto de texto cifrado consiste pues en 30 caracteres, mientras que se pueden usar 31 caracteres para texto claro. Por lo tanto una única transformación de estos 31 caracteres no es posible. Este problema se soluciona poniendo una restricción al uso del RETROCESO DE CARRO Y DEL CAMBIO DE RENGLON. Se observa que en un teleimpresor normal el accionamiento del AVANCE DE RENGLON está casi siempre precedido por un RETROCESO DE CARRO. Entonces el alfabeto de texto claro tiene de hecho 30 caracteres, haciendose así posible una transformación única. Los caracteres no permitidos se evitan muy facilmente, evitando simplemente los dos caracteres críticos en el registrador de entrada REG X cuando éste está trabajando como registrador de cambio realimentado lineal normal, así, REG X avanza a lo largo de un ciclo de 30 que contiene todas las combinaciones posibles de 5 elementos excepto las dos correspondientes a los caracteres de teleimpresor TODO ESPACIO Y CAMBIO A CIFRAS.

DIAGRAMA DE BLOQUE

En la figura 1b se ha representado un diagrama de bloque que contiene los hilos de control principal, para dar una mejor idea del esquemático detallado.

DESCRIPCION GENERAL

En las figuras 1c-i y 2a-h se ha representado un esquemático de bloque detallado de una realización del invento. El circuito representado muestra un equipo criptográfico sin cinta que no tra-

./..

baja en línea capaz de cifrar y descifrar mensajes normales de teleimpresor en una forma compatible con los procedimientos telex normales.

Los bloques principales están indicados por líneas de trazos y los terminales de cada bloque principal están numerados con números individuales para cada bloque principal. Los terminales tienen además designaciones de forma que sus interconexiones pueden comprendorse fácilmente.

En casi todos los bloques principales se han indicado puntos de prueba adecuados. Estos puntos de prueba se han designado TP1, TP2 ... TP5 y no se describirán más.

En los bloques principales se han usado simbolos lógicos que se describen con detalle en relación con el diagrama de símbolos de la figura 6. Todos los bloques lógicos tienen códigos que son individuales para cada bloque principal. Los flip-flops tienen además designaciones funcionales casi en centro del símbolo lógico.

El bloque 1, figura 1c, d contiene cinco pares de sumadores módulo 2. Todos los sumadores excepto el último comprende una puerta NAND y una puerta EXCLUSIVA OR. La puerta inferior comprende tres puertas NAND A1, A2 y A3. Las salidas de cada par están conectadas a las entradas de una puerta individual EXCLUSIVA OR. Mediante dos señales de puerta K'5 y K el sumador inferior o superior de cada par puede tener su salida conmutada a través de las salidas de cinco puertas OR EXCLUSIVAS E1, E2, K1, K2, B2.

El bloque 2 de la figura 1c, d contiene seis flip-flops $X_1 - X_6$, y los circuitos asociados. Los flip-flops $X_1 - X_5$ constituyen un registrador de cambio realimentado (registrador X) que se usa para almacenar y manejar los elementos de información del caracter de teleimpresor. El flip-flop X_6 se usa para los retardos. Además de los circuitos de entrada a los flip-flops $X_1 - X_6$, el bloque 2

./..

contiene también cuatro puertas NAND A2, D2, A1, D1 para detectar cuando el contenido de los flip-flops X1 - X5 corresponde a los caracteres de teleimpresor CAMBIO A CIFRAS (1...), RETROCESO DE CARRO (<) AVANCE DE RENGLON(≡) y TODO ESPACIO (BL, respectivamente.

El bloque 3 de la figura 2d, f contiene circuitos de puerta y de disparo misceláneos de los que los más importantes son el flip-flop MEMO usado para almacenar el caracter AVANCE DE RENGLON durante el descifrado, el flip-flop de COLOCACION (SET) usado para generar las señales necesarias para la colocación inicial de los registradores de generador de clave, y el contador principal de programa (contador K) que contiene cinco pasos contadores K1 - K5.

El bloque 4 de la figura 2c, b contiene el contador de entrada $\overline{FFo}$, FFe, FFa, FFb, FFd, y FF_{S2}, y los circuitos asociados. Este es un contador binario utilizado para gobernar el avance de los caracteres de teleimpresor a y fuera del equipo.

El bloque 5, figura 2a que contiene los bloques OSC de 25 KHz (generador de impulsos de reloj) y RES (Circuito de reposición) se ha representado con detalle en la figura 4. El circuito de reposición se usa para suministrar señales de corriente contínua a los registradores principales en el generador de material de clave.

El bloque 6 de la figura 2a que contiene el bloque OS (Circuito de un disparo o circuito monoestable con corto tiempo de recuperación) se ha mostrado con detalle en la figura 3. Este circuito se usa para la temporización del contador de entrada.

El bloque 7 de la figura 2d, e, f, g, h contiene un contador en anillo (contador I) con tres pasos $i_2 - i_4$ y otro contador en anillo (contador J) con tres pasos $j_1 - j_3$. Estos dos contadores se usan para gobernar el procedimiento de puesta en marcha del equipo. El bloque 7 tambien contiene un contador binario (contador P) con cinco pasos $C_1 - C_5$. El último es un contador binario usado para

./..

contar hacia atras desde el punto de colocación recibido como señales de corriente contínua desde el bloque 8.

El bloque 8 de las figuras 2e, g, h contiene circuitos de puerta miscelaneos. Los circuitos de puerta se usan para suministrar al contador C1 - C5 del bloque 7 la información adecuada del generador de material de clave en los modos de cifrado y descifrado respectivamente.

El bloque 9 de las figuras 1e, j contiene un registrador de caracteres de clave (registrador Z) con cinco pasos Z1 - Z5 Este registrador recibe normalmente en los terminales J, K del paso Z1 su información en forma serie desde el generador de clave. Sin embargo tambien puede suministrarse información en forma paralela desde un lector de cinta exterior designado TR. El bloque 9 tambien contiene el amplificador principal de impulsos de cambio formado por las puertas C2, C3, C4, y F, G, H1 y H2. Tambien contiene un registrador de cambio (Registrador Y) Y1 - Y5 que se usa como un registrador almacenador intermedio durante el procedimiento de puesta en Marcha.

Los bloques 10, 11 y 12 de las figuras 1e, f, g, h, i constituyen el generador de clave, que comprende dos registradores de cambio realimentados no lineales de 15 bits,, REG I_1 - REGI_{15}, REG II_1 - REG II_{15} con flip-flops de disparo y circuitos asociados de puerta de entrada y salida.

El bloque 14 de la figura 2a contiene los bloques RC (circuito de lectura) y DA (Amplificador excitador) que se han representado con detalle en la figura 5.

La PLUG A de la figura 1c, d contiene interconexiones puenteadas entre sus terminales que determinan el esquema de realimentación en los registradores de cambio realimentados X_1 - X_5, bloque 2 usados en el proceso de cifrado y descifrado.

El bloque TR de la figura 1f es un lector de cinta. Este

./..

dispositivo no está conectado normalmente, pero puede conectarse para hacer posible el uso de una cinta de clave como material de clave.

Las rejillas designadas PB en las figuras 1g, h, i, representan el esquemático del cuadro de terminales usado para insertar información de material de clave en el equipo. Los círculos alrededor de las intersecciones entre líneas verticales y horizontales indican que hay una conexión electrica por medio de una clavija de corto-circuito.

En las figuras 1e, h, 2b se han representado varios contactos de conmutación designados S ó $\bar{S}$. Estos son contactos de un conmutador de levas de tres posiciones. La posición central de este conmutador corresponde a reposo o modo claro del equipo. Las otras dos posiciones corresponden a emisión y recepción, o cifrado y descifrado respectivamente.

El bloque TP de la figura 1f indica un teleimpresor con su contacto transmisor y su bobina de recepción. Esto se ha representado tambien en la figura 5.

El bloque TB1, figura 2a es una regleta terminal. S4 de la figura 2a es un conmutador de tecla cuyas dos posiciones corresponden a funcionamiento del teleimpresor a simple polaridad y a doble polaridad. S3 de la figura 2a es un conmutador de tecla cuyas dos posiciones corresponde a una corriente de 20 y treinta miliamperios doble polaridad. o cuarenta y sesenta miliamperios, simple polaridad para el electroimán de recepción del teleimpresor. El conmutador de posiciones múltiples JB de la figura 2a se usa para seleccionar la constante de tiempo adecuada del circuito de un disparo del bloque 6 figura 2a.

DESCRIPCION FUNCIONAL

Introducción

Como se ha mencionado, el texto cifrado no debe contener

caracteres que no puedan ser perforados en un teleimpresor normal de una instalación telex o caracteres que puedan perturbar la transmisión normal de una instalación telex o caracteres que puedan perturbar la transmisión en un canal telex, tales como la letra D en cifras.

El proceso de cifrado empieza cuando el circuito de lectura recibe el impulso de arranque de un caracter de texto claro X por accionamiento del teclado o del transmisor automático de un teleimpresor. El circuito de lectura pone en marcha un oscilador que a su vez da impulsos de cambio al registrador X figuras 2c, d, I, figuras 1g, i, II, figuras 1h, i y Z, figura 1e.

Así, el caracter cifrado precedente se envía al teleimpresor desde el registrador X a través de un amplificador excitador de teleimpresor. Cuando el registrador X contiene los 5 bits de información, el registrador Z contiene 5 nuevos bits de clave y el contador P, figura 2g, h se coloca en un nuevo número P. Ahora, el registrador X está conectado como un registrador de cambio realimentado de máxima longitud y los impulsos de cambio se llevan al contador P y al registrador X. El suministro de impulsos de cambio de 25 KHz se detiene cuando el contador P = 0, es decir, después de P impulsos A continuación, el registrador X se conecta como un registrador normal de cambio y se coloca a la información REGISTRADOR X ⊕ registrador Z. Esta es la forma cifrada de un texto claro que se envía cuando el caracter de texto claro siguiente se cambia en el registrador X.

Este es el proceso normal de cifrado. Para evitar algunas complicaciones en relación con los canales telex, los caracteres del texto cifrado TODO ESPACIOS Y CAMBIO A CIFRAS no se utilizan. El primero de ellos porque algunos teleimpresores no pueden perforar TODO ESPACIOS. EL CAMBIO A CIFRAS se evita porque puede haber perturbacio-

nes en la transmisión para algunos caracteres en cifras.

Ahora, cuando se ha detectado una de estas dos combinaciones como texto cifrado, el registrador X no se coloca a Registrador Z, sino que permanece sin modificar. Así, la versión cambiada del texto claro en el registrador X es enviada como texto cifrado.

Se verá que este proceso es reversible, haciendo posible el descifrado.

Modo de cifrado

Para empezar supondremos que el procedimiento de arranque que se explicará mas tarde ha sido completado y que se va a hacer el cifrado normal. El caracter que tiene que cifrarse entra en el equipo en forma serie desde el contacto transmisor del teleimpresor TP, figura 2a que es excitado por el circuito de lectura RC del bloque 14, figura 2a. En el circuito de lectura RC, la corriente que circula o no circula al contacto transmisor se convierte en niveles lógicos adecuados para el resto del equipo. La señal de salida del circuito de lectura se pasa al bloque 4, (puerta A1), figura 2c que contiene el contador de entrada $\overline{FFo}$, FFe, FFa, FFb, FFc, FFd, figura 2c y los circuitos asociados. Al recibir el impulso de arranque del caracter que tiene que cifrarse, este contador de entrada pasará a través de un ciclo completo a una velocidad determinada por el circuito de un disparo OS del bloque 6, figura 2a. Las señales derivadas del contador de entrada se usan para gobernar el avance del caracter en el registrador de entrada $X_1 - X_5$ del bloque 2, figuras 1c, d, y tambien para avanzar los registradores de generador de clave de los bloques 10, 11 y 12, Cuando el contador de entrada ha completado su ciclo, los cinco elementos de información del caracter de teleimpresor se almacenarán en el registrador de entrada.

Entonces empezará el proceso de cifrado. Este proceso es gobernado por un contador de anillo $K_1 - K_5$ del bloque 3, figura

./..

2f, llamado contador K. El contador K permanece en su posición de reposo K_1 durante el ciclo del contador de entrada. Al final del ciclo del contador de entrada, es decir cuando el último elemento de información del caracter de teleimpresor ha avanzado en el registrador X, el contador K avanzará a la posición K2. En esta posición, K2 tendrá lugar la evaluación y posible modificación del caracter de texto plano en el registrador X. Esto es necesario porque el texto cifrado que resulta finalmente del proceso de cifrado no debe contener caracteres que no puedan transmitirse fácilmente en un canal telex. En este equipo los caracteres TODO ESPACIO y CAMBIO A CIFRAS no pueden estar presentes en el texto cifrado. El primero no está presente en el texto claro, pero el segundo si. Para tener excluído un CAMBIO A CIFRAS del texto cifrado, este caracter de texto claro debe cambiarse por RETROCESO DE CARRO. Para evitar confusión, el RETROCESO DE CARRO del texto claro debe convertirse en AVANCE DE RENGLON, Esto es posible porque se supone que en el texto claro los dos caracteres RETROCESO DE CARRO y AVANCE DE RENGLON se presentan siempre juntos. Si fuera necesario, las modificaciones del texto plano antes descritas se hacen en la posición de contador de programa K2 aplicando un impulso de cambio a los pasos del registrador de entrada X1 - X3. El contador de programa avanza entonces a la posición K3.

En esta posición K3, tiene lugar el primer paso del proceso de cifrado. El registrador de entrada X está ahora conectado como un registrador de realimentación de longitud máxima. Recibirá un número de impulsos de cambio determinados por el tcontenido del contador P, figura 2g, h, que está constituído por los flip-flops C1 - C5 del bloque 7, figuras 2g, h. Este contador retrocede desde su posición inicial a cero por la señal principal de reloj. La posición inicial está determinada por un número P pseudo al azar transferido desde el generador de clave REG I, REG II, figuras 1g, h, i al con-

tador P, figuras 2g, h en forma paralela cuando el contador principal de programa K, figura 2f está en la posición K2. Cuando el contador P ha llegado al estado cero, el contador de programa K avanzará de K3 a K4, y el segundo paso del procedimiento de cifrado tendrá lugar.

El segundo paso de cifrado comprende la adición de módulo 2, en el bloque 1, del contenido del registrador de entrada X con un número al azar suministrado en forma paralela desde el registrador Z en el bloque 9, figura 1e. Como se verá en el esquemático, el registrador Z comprende cinco pasos Z1 a Z5 conectados como un registrador de cambio normal recto. La información que pasa al registrador A se deriva de las salidas de los dos registradores de generador de clave, REG I y REG II, en la puerta D3 del bloque 12, figura 1i. El registrador Z se cambia junto con los dos registradores de generador REG I, REG II durante el avance del caracter de texto claro en la posición K1 de contador de programa. La adición de módulo 2 antes mencionada, de los contenidos del registrador de entrada X y del registrador de caracter de clave Z se hace en paralelo sin ninguna transferencia de la información llevada de paso a paso. Antes de que el contador de programa avance a K5, el contenido del registrador X se comprueba para controlar si puede transmitirse a la línea. Las puertas D1 y A3 del bloque 2, figura 1d, comprueban si el registrador contiene los caracteres TODO ESPACIOS o CAMBIO A CIFRAS, respectivamente, y la adición de módulo 2 se repetirá entonces. El contenido del registrador X será entonces como era después de avanzar uno de los procesos de cifrado. Puesto que TODO ESPACIO no estará nunca contenido en el ciclo normal de un registrador de realimentación de longitud máxima de registrador realimentado y puesto que la posición CAMBIO A CIFRAS es pasada automáticamente en este equipo, el contenido del registrador X después del primer paso del proceso de cifrado puede ser siempre transmitido a la línea. Como se puede ver, el segundo

paso del proceso descifrado no se utiliza, cuando resulta en un caracter que no puede transmisitrse a la línea.

El caracter cifrado ahora contenido en el registrador X se transfiere al electroimán de recepción del teleimpresor TP, figura 2a durante el avance del caracter de texto claro siguiente al registrador X, en el que se remite el proceso antes descrito.

El procedimiento de arranque primeramente mencionado es necesario para asegurar diferentes puntos de arranque de los registradores de generador de clave REG I REG II de mensaje a mensaje. En el modo de cifrar, este procedimiento de arranque comprende el avance de 6 caracteres de teleimpresor, es decir 30 bits, en los registradores de generador de clave. Simultáneamente, estos 6 caracteres se cifran y se transfieren al electroimán receptor del teleimpresor TP (y después a la línea). En la recepción, o extremo de descifrado, los 6 caracteres se descifrarán y transferirán a los registradores de generador de clave del equipo de descifrado. De esta forma se asegura que el mismo punto de arranque en el equipo de cifrado y descifrado. Los 6 caracteres que definen un punto de arranque se toman durante el funcionamiento normal de una tabla de puntos de arranque preparada con prioridad para un esquema de realimentación particular para los registradores de generador de clave. Durante el cifrado los caracteres de punto de arranque no se transfieren directamente de circuito de lectura a los registradores de generador de clave, sino que se pasan a través de un registrador de almacenamiento intermedio, registrador Y en el bloque 9, figura 1e. El registrador Y recibe los impulsos de cambio simultáneamente a los registradores de generador de clave REG I, REG II, y el registrador de caracter de clave Z mencionado anteriormente.

Las funciones de puerta necesarias durante el procedimiento de arranque son hechas por medio de dos contadores de anillo

./..

de tres pasos I y J del bloque 7, figuras 2f, h. El contador I, comprende los pasos $i_2 - i_4$, es disparado una vez por cada ciclo completo del contador K, figura 2f. El contador J, que comprende los pasos $J_1 - j_3$, avanza una vez por cada ciclo completo del contador I.

El cuadro de terminales PB, figura 1g, h, i, almacena información de como colocar los registradores REG I y REG II, figuras 12, f, g, h, i inicialmente. Hay $2^{30} \_ 10^9$ ajustes posibles. Las posiciones iniciales se usan para cifrar los 6 caracteres que se seleccionan para dar las longitudes de ciclo adecuadas en dichos registradores. Los contadores $i_2 - i_4$ y $j_1 - j_3$, bloque 7 registran el procedimiento de arranque y determinan cuando alimentar a los registradores con la información de arranque.

La señal de reloj principal que gobierna todas las funciones del equipo se derivan de un oscilador de onda cuadrada de 25 KHz del bloque 5, figura 2a. En el bloque 5 hay tambien un circuito de reposición que suministra la corriente necesitada para ajustar todos los flip-flops de los registradores de generador de clave a la posición cero cuando el equipo está en modo claro o en reposo.

Modo de descifrar

El descifrado de un caracter empieza con una transferencia de un caracter desde el contacto de transmisión del teleimpresor TP al equipo, como al cifrar. El impulso de arranque del caracter que tiene que descifrarse inidiará tambien en este caso un ciclo del contador de entrada en el bloque 4, figura 2c. Simultáneamente, los elementos de información del caracter del texto cifrado que tiene que descifrarse se hace que avancen en el registrador de entrada X. Esto sucede con el contador de programa K en su posición de reposo K1. Los dos pasos del proceso de cifrado tendrán que hacerse ahora en el orden inverso. Por lo tanto, en la posición K2 del contador de programa K, la adición de módulo 2 del contenido del regis-

./..

trador X y del Z será llevada a cabo. Si el contenido del registrador X después de la adición de módulo 2 es igual a TODO ESPACIO o CAMBIO A CIFRAS, es claro que la adición de módulo 2 ha sido hecha dos veces durante el cifrado. Por lo tanto, tambien se repetirá aquí, y esto significa que solamente se hará el proceso inverso al paso 1 durante el cifrado. El registrador de realimentación de longitud máxima tiene una longitud de ciclo de 31. En este equipo, la posición correspondiente a CAMBIO A CIFRAS es pasada automáticamente. Por lo tanto, la longitud efectiva de este registrador es 30 posiciones. Para producir el texto plano inicial durante el proceso de descifrado es ahora necesario avanzar el registrador X 30 - P pasos. Esto se hace con el ajuste adecuado del contador P mencionado durante la explicación del proceso de cifrado. El cambio del registrador X durante el descifrado se hace en la posición del contador de programa K3. Finalmente, en la posición K4 del contador de programa, debe hacerse una posible modificación opuesta de una de las hechas en el extremo de cifrado. Como se ha explicado antes, el caracter CAMBIO A CIFRAS se modificó en RETROCESO DEL CARRO y el caracter RETROCESO DEL CARRO se modificó por el de AVANCE DE RENGLON. Por lo tanto, si el caracter descifrado contenido en el registrador X es igual a RETROCESO DEL CARRO debe convertirse en AVANCE DE RENGLON. Esto se hace aplicando a un impulso de cambio a los pasos del registrador X en la posición del contador de programa K4. Si el contenido del registrador X después de la realimentación es igual a AVANCE DE RENGLON, esto puede deberse a un caracter de AVANCE DE RENGLON durante el cifrado o por un RETROCESO DE CARRO convertido durante las operaciones de cifrado. Como se ha mencionado antes, se supone que los caracteres RETROCESO DE CARRO Y AVANCE DE RENGLON se prestan juntos en el mismo orden que acaba de mencionarse. Cuando el caracter AVANCE DE LINEA resulta primero de la operación del registrador de cam-

bio realimentado, se cambia incondicionalmente por un RETROCESO DEL CARRO en la posición K4 del contador de programa. Esta modificación se almacena tambien colocando el flip-flop MEMO del bloque 3, figura 2d. Supuesto que el RETROCESO DEL CARRO y el AVANCE DE RENGLON se transmiten siempre a pares, el caracter siguiente resultante de la operación del registrador de cambio realimentado durante el descifrado será de nuevo AVANCE DE LINEA.

Puesto que el flip-flop MEMO está ahora colocado, las modificaciones del caracter AVANCE DE LINEA se omitirá ahora en la posición del contador de programa K4.

Esto quiere decir que el caracter descifrado que tiene que tranferirse al electroimán de recepción del teleimpresor TP, figur gura 2a durante el proceso de avance siguiente, será AVANCE DE RENGLON. Como se comprenderá el caracter RETROCESO DE CARRO tiene de esta forma que ser redundante, y la combinación de teleimpresor usada normalmente para transmitir este caracter se usa para transmitir el CAMBIO A CIFRAS. La omisión de la combinación de teleimpresor CAMBIO A CIFRAS del texto cifrado, se introduce para evitar el caso de una cifra en el alfabeto del texto cifrado. Esto es necesario porque no puede permitirse, cuando se transmite a una estación telex no atendida que se dispare la unidad de respuesta automática cuando se está recibiendo un texto cifrado. Como se sabe, la unidad de respuesta automática se dispara mediante la letra D en cifras.

Omitiendo el caracter CMBIO A CIFRAS totalmente en el texto cifrado, el teleimpresor nunca se pondrá en cifras cuando se reciba un texto cifrado.

DESCRIPCION DE LOS CIRCUITOSFUNCIONALES PRINCIPALES

Generador de clave

El generador de clave comprende dos registradores de cambio realimentados no lineales, REG I y REG II (Bloques 10, 11, 12,

./..

figura 1g, h, i) cada uno con 15 pasos, REG I_{1-15} y REG II_{1-15} respectivamente y con una señal de realimentación $F(A_i, A_j, A_k, A_l) + A_{15}$ en la que $F(A_i, A_j, A_k, A_l)$ es una función no lineal cuya tabla de combinaciones de las variables binarias A_i, A_j, A_k y A_l son las señales de salida de cuatro pasos de registrador. i, j, k y l son todos diferentes, y por otra parte están seleccionados al azar por medio de patillas del cuadro de terminales PB.

Esto se representa en la figura 1g, h, i en la que la señal de realimentación de REG I se toma de los pasos números 4, 14 10 y 9 de forma que i, j, k y l en este caso son igual a 4, 14, 10 y 9 respectivamente. Estas cuatro señales de salida se llevan a las puertas B4, C1, B3 y C2 en el bloque 12, figura 1i, y la señal combinada de la puerta C2 se añade módulo 2 en las puertas E4, F1 a la señal de salida A_{15} del último paso REG I_{15}. La señal de realimentación se aplica al registrador REG I en la puerta D1, bloque 10, figura 1e, g.

La señal de realimentación del registrador REG II se toma en forma semejante de los pasos número 7, 10, 3 y 6, se combina en las puertas B1, A1, B2, y A2, bloque 12, figura 1i. Esta señal combinada se añade módulo-2 a la señal de salida A_{15} del último paso de registrador REG II_{15} en las puertas E3, F2 y se aplica a la entrada del registrador en la puerta D2, bloque 11, figura 1f, h.

Este es un tipo de registrador que todavía no se ha explicado totalmente matemáticamente en la literatura pero es evidente que un ciclo largo de un registrador de este tipo presentará siempre una forma pseudo al azar. Además, las secuencias tienen usualmente longitudes diferentes, lo que quiere decir que las longitudes físicas de los registradores de generadores de clave puedan ser iguales. Sin embargo, hay ciertas probabilidades de que una secuencia pueda ser muy corta. Así, en este sistema, los puntos de arran-

que no son totalmente al azar sino que se seleccionan para dar unas longitudes de ciclo adecuadas. En el presente equipo que tiene dos registradores de 15 bits, deben seleccionarse 6 caracteres para cada mensaje que tenga que enviarse. Las señales de salida de los dos registradores se suman módulo 2 en las puertas D1, D2, D3 y D4, figura 1i para dar la secuencia deseada de bits de clave pseudo al azar. Esta secuencias se almacenan en un registrador de 5 bits $Z_1 - Z_5$, bloque 9, figura 1e. El número de conexiones diferentes es,

$$\binom{15}{4} \times \left\{\binom{15}{4} - 1\right\} \simeq 1{,}86 \times 10^6$$

En los dos registradores REG I y REG II se usan flip-flops de disparo. En un flip-flop de disparo el contenido después de un impulso de reloj depende de la señal de entrada y de la señal presente en flip-flop mismo. Así el siguiente sistema de ecuaciones define el comportamiento de un registrador.

$$A_i = F(A_i, A_j A_k A_l) \oplus A_{15} \oplus A_1$$

$$A_2' = A_1 \oplus A_2$$

$$A_3' = A_2 \oplus A_3$$

- - - - - - - - - -

$$A_{15}' = A_{14} \oplus A_{15}$$

Al es la señal presente en el paso registrador nº. 1 antes del impulso de reloj y A_1' es la señal presente en el mismo paso después del impulso de reloj. Semejantemente para los otros pasos, y el comportamiento es idéntico para los dos registradores.

Generador para "P"

P es un número pseudo al azar de 5 bits. tomado de los dos registradores REG I y REG II, bloque 10, 11, 12 , figura 1g, h, i en la forma representada en el bloque 8, figura 2e, g, h. Cada bit es el resultado de una adición de módulo 2 de señales de salida de bits seleccionados al azar en ambos registradores. El bloque 8, figura 2e, g, h comprende complejos de 5 puertas a cada una de las cua-

les se aplican dos señales del cuadro de terminales PB. El primer complejo de puerta comprende las puertas C1, C2, C3, C4, B1, B2, B3 y D2, bloque 6, figura 2e y se le aplican señales procedentes de los múltiples del cuadro de terminales PB/A y PB/B. Como se verá en las figuras 1g, h, PB/A está asociado con REG I, mientras que PB/B está asociado con REG II. Una conexión semejante se asigna a los otros cuatro complejos de puerta. El número de conexiones utilizables diferente es

$$\binom{15}{5} \times \binom{15}{5} \approx 9 \times 10^6$$

La salida de cada uno de los complejos de puerta que constituyen juntos el número P se aplica a un contador $C_1 - C_5$, bloque 7, figura 2g, h.

Durante el cifrado, el número P se lleva al contador binario C1-C5, pero durante el descifrado este contador recibe el número 31-P. En ambos casos el contador cuenta hasta cero, mientras recibe los impulsos del generador de 25 KHz.

Registrador de entrada

El REG X (Bloque 2, figuras 1c, d) que está formado por los pasos $X_1 - X_5$ tiene dos formas de funcionamiento.

a) Trabaja como un registrador normal de cambio de 5 bits, recibiendo impulsos de cambio de 50 Hz (para una velocidad de teleimpresor de 50 baudios)

b) Trabaja como un registrador de cambio realimentado comprendiendo cada paso un sumador módulo-2, por ejemplo, la puerta M1, y un flip-flop, por ejemplo X1. Cualquier salida puede conectarse por medio de conexiones soldadas en una clavija PLUG A, y estas conexiones se hacen de acuerdo con algún polinomio resultando de ellos una secuencia de longitud máxima $2^5 - 1 = 31$. La combinación de 5 bits que representa el caracter CAMBIO A CIFRAS se quita del ciclo. Así, REG X pasa a través de un ciclo de 30 que contiene todas las combinaciones

posibles de 5 bits excepto TODO ESPACIO Y CAMBIO A CIFRAS. Estos son aproximadamente 15.000 ciclos diferentes para elegir entre ellos. Los impulsos de cambio en este caso viene del generador de 25 KHz, y el número de impulsos es igual al número de pasos que el contador C_1 - C_5 está contando.

Cuadro de terminales

El cuadro de terminales (PB), figuras 1g, h, i es un cuadro con regletas terminales horizontales y verticales dispuestas en una matriz con aproximadamente 300 puntos de cruce (agujeros). Una patilla conductora inserta en un punto de cruce conectará las regletas terminales horizontales y verticales en ese punto de cruce particular. Las patillas del cuadro de terminales determinan las salidas que tienen que usarse para las funciones de realimentación, las salidas que tienen que usarse para generar el número P y que flip-flops tienen que ajustarse inicialmente.

Multivibrador de un disparo

La figura 3 representa con detalle el diagrama esquemático del bloque 6 de la figura 2a. Este circuito OS da la referencia de tiempo para las señales de entrada y salida del teleimpresor. Se obtiene intervalos definidos de tiempo por medio de un multivibrador monoestable que comprende los transistores Ts1 y Ts2 y los componentes asociados. En la posición de reposo, el transistor Ts1 es conductor mientras que Ts2 está al corte. Un impulso de disparo aplicado a través de un diodo D3 cortará el transistor Ts1. A través de la acción regenerativa del circuito el transistor Ts2 será ahora conductor. Este estado durará hasta que el condensador C1 se haya descargado a través de la resistencia R3. El transistor Ts1 empezará a conducir de nuevo y Ts2 se pondrá al corte. El transistor Ts4 se hace conductor durante un corto período de tiempo cuando el circuito oscila de nuevo a la posición de reposo. De esta forma, el con-

denssador de temporización se cargará rápidamente. Por lo tanto se obtiene un tiempo muy corto de recuperación. La longitud de los impulsos del circuito no será afectada por una relación de trabajo elevada. Los transistores Ts3 - 4 y Ts5 - 6 constituyen la red de entrada. El circuito se dispara cada vez que el transistor Ts3 se conecta. La resistencia R8 conectada a la base de Ts3 se usa para inhibir los posibles impulsos de disparo, cuando el circuito está en su posición casi estable. La señal de salida se toma del colector del transistor Ts7. En la posición de reposo, el transistor Ts2, es, como se ha establecido antes, no conductor. Entonces Ts7 será tambien no conductor y el nivel de salida será alto. Cuando se dispara el circuito a este estado casi estable, Ts2 se hace conductor y así también lo será Ts7. Entonces la señal de salida será baja, es decir casi el potencial de tierra, El condensador de tiempo C1 comprende cuatro elementos designados C1a - C1d. La finalidad de esta disposición es la de obtener por medio de un puenteado exterior impulsos de diferente longitud para adaptar el circuito a varias velocidades de teleimpresor. La interconexión de los terminales 3 - 4 da una velocidad de 75 baudios, la de los 6 - 4 corresponde a 50 baudios y la 5-4 corrospondo a 45 baudios.

Los transistores pueden ser de los siguientes tipos: Ts1: 2S 301; Ts2-3: 2S 302; Ts4: 2N 1711; Ts5-7: BSY 95A o componentes equivalentes y todos los diodos pueden ser del tipo 1S 920 o equivalentes.

Generador de impulsos de reloj

La figura 4 representa un esquemático detallado de dos circuitos diferentes del bloque 5, figura 2a. El superior es el generador de impulsos de reloj, OSC de 25 KHz. Este es un multivibrador estable que comprende los transistores Ts1 y Ts2 y los componentes asociados. Los transistores Ts3 y Ts4 son los amplificadores de sa-

./..

lida del circuito. La finalidad de los diodos D1, D2 y del condensador de aplanamiento C3 es evitar un estado estable con ambos transistores conduciendo simultaneamente, lo que puede ocurrir con un multivibrador estable convencional.

Circuito de reposición

En la parte inferior de la figura 4 se ha representado un circuito de reposición RES cuya función es suministrar una señal de corriente contínua a los registradores realimentados de generador de clave. Cuando uno de los transistores de entrada Ts6 ó Ts7 es conductor el transistor de salida Ts5 será tambien conductor y suministrará corriente a la carga. Si los dos transistores de entrada están al corte, el transistor de salida Ts5 tambien lo estará. Los transistores pueden ser de los siguientes tipos: Ts5: 2S 302; Ts1-4, 6-7: BSY 27 o componentes equivalentes, y los diodos D1-2 pueden ser del tipo 1S 920 ó equivalentes.

Circuito de lectura

La figura 5 representa el diagrama esquemático detallado de l do los circuitos contenidos en el bloque 14 de la figura 2a. En la parte superior de la figura 5 se ha representado el circuito de lectura Rc. Una corriente de aproximadamente 40 miliamperios se lleva de la alimentación de +50 voltios a través de las resistencias R17 y los terminales 6 y 3 a través del contacto del teleimpresor TP y de vuelta al circuito de lectura RC. Si el contacto del teleimpresor está cerrado, el transistor de entrada Ts9 será conductor. Si el contacto del teleimpresor está abierto, Ts9 será no conductor. La señal de salida tomada del colector de Ts9 será baja cuando el contacto del teleimpresor está cerrado lo que corresponde a MARK y alta cuando el contacto del teleimpresor está abierto lo que corresponde a SPACE. Para tener disponible la fase opuesta de la señal de salida se añade un paso inversor que comprende Ts8 y los com-

./..

ponentes asociados al circuito de lectura.

Amplificador excitador

En la parte inferior de la figura 5 se ha representado el esquemático detallado del amplificador excitador de teleimpresor DA. Este circuito comprende los transistores de entrada Ts1, Ts2 y Ts3 con los componentes asociados, dos generadores de corriente constante, Ts6 y Ts7 con los componentes asociados y dos transistores de conmutación de corriente de teleimpresor Ts4 y Ts5 con los componentes asociados. Por medio de conexiones exteriores S3, el circuito puede adaptarse a funcionamiento a simple o doble polaridad y a diferentes niveles de corriente. En funcionamiento a simple polaridad se conectan en paralelo los dos generadores de corriente constante. En la condición de MARK el transistor Ts5 será entonces conductor y Ts4 no conductor. La corriente de los generadores de corriente constante circulará entonces a través del electroimán de recepción del teleimpresor M. En la condición de SPACE, el transistor Ts4 será conductor y Ts5 será no conductor. Entonces no circulará corriente a través del electroimán de recepción del teleimpresor M. En el lado de entrada, MARK corresponde a la señal de entrada alta y SPACE a la señal baja de entrada. Los transistores pueden ser de los tipos siguientes: Ts1, Ts2, Ts3, Ts8, Ts9: BSY 95A; Ts4, Ts5: 2N 1893, Ts6, Ts7: 2N 2904A o componentes equivalentes, mientras que los diodos D1, D2 pueden ser del tipo ZF 5.6 o equivalentes.

Simbolos lógicos

En la figura 6 se han representado los diferentes símbolos lógicos que representan las distintas funciones lógicas del diagrama principal. Estas son: Inversor, puerta NAND de dos entradas, puerta NAND de tres entradas, puerta NAND de 5 entradas, flip-flop JK con preajuste y una puerta OR EXCLUSIVA.

./..

Estos símbolos lógicos y sus funciones se describen con detalle en la publicación "Series 73 solid circuito semi-conductor networks", Bulletin Nº. DL-S567650, de Julio de 1.965 publicado por Texas Instrumentos Incorporated. Los símbolos representados en la parte alta de la figura 6 corresponden a las redes TI siguientes: 1/4 SN 7350, 1/4 SN 7360, 1/3 SN 7331, 1/2 SN 7311, 1/2 7302 y 1/2 SN 7370. Los símbolos correspondientes a 1/4 SN 7350, 1/2 SN 7302 y 1/2 SN 7370 son algo diferentes para simplicación del dibujo.

Aunque los principios del invento se han descrito en conexión con aparatos específicos se sobrentiende claramente que esta descripción se ha hecho solamente a título de ejmplo y no como una limitación del alcance del invento según se establece en sus objetos y en las reivindicaciones que se acompañan.

Este invento corresponde a una solicitud de patente formulada en Noruega el 17 de Junio 1966 señalada con el nº. 163.527 y se acoge por lo tanto a los beneficios que otorgan los convenios in internacionales vigentes.

- - - - - - - - - - - - - - - - N O T A - - - - - - - - - - - - - - - - -

Los puntos de invención propia y nueva que se presentan para que sean objeto de esta patente de veinte años son los siguientes:

1.- Un generador de material de clave para equipo criptográfico de teleimpresor caracterizado en éste porque comprende uno o más registradores de cambio no lineales conectados realimentados (REG I, REG II).

2. Un generador de material de clave como el del punto 1 caracterizado en éste porque cada registrador comprende una pluralidad de circuitos flip-flop de disparo, estanto conectadas las entradas de control de cada uno de estos circuitos a la salida del circuito precedente, de forma que el funcionamiento del registrador

es tal que los contenidos siguientes de un flip-flop arbitrario es igual a la suma módulo-2 de los contenidos presentes del flip-flop en cuestión y del flip-flop precedente.

3.- Un generador de material de clave como el del punto 2 caracterizado en éste porque cada registrador de cambio tiene un bucle individual de realimentación en el que las salidas de dos o más pasos de registrador elegidos arbitrariamente se combinan para producir una señal de realimentación no lineal.

4.- Un generador de material de clave según el punto 3 caracterizado en ésto porque dichas salidas se eligen insertando clavijas en un cuadro (PB) en el que están accesibles las salidas de todos los pasos de registrador.

5.- Un generador de material de clave como el del punto 4 caracterizado en éste porque las salidas combinadas de los pasos elegidos arbitrariamente se suman módulo-2 a la salida del último paso de registrador.

6. Un generador de material de clave como el del punto 5 caracterizado en éste porque las salidas de los registradores se suman módulo 2 para producir el material de clave deseado.

7.- Un generador de material de clave como el del punto 6 caracterizado en éste porque se obtiene un material de clave deseado combinando los contenidos momentáneos de los pasos de registrador elegidos al azar.

8. Un generador de material de clave,

tal y como se describe en la memoria que antecede, representado en los dibujos que se acompañan y a los fines especificados.

./..

341955

33.

Esta memoria consta de treinta y tres hojas escritas por una sola cara.

Madrid,

17 JUN. 1967

Teléfonos Standard cables

EUGENIO BARROSO
Secretario General

341955

341955

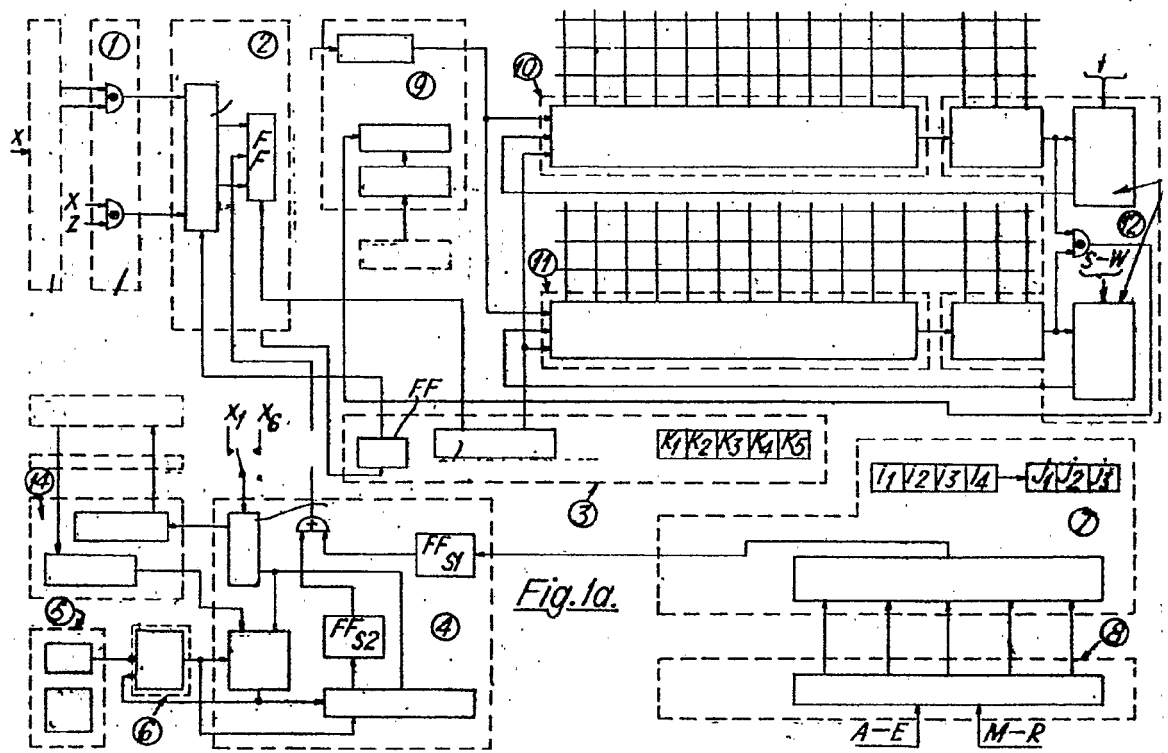


Fig. 1a.

17 JUN 1967

EUGENIO BARROSO
Secretario General

341955

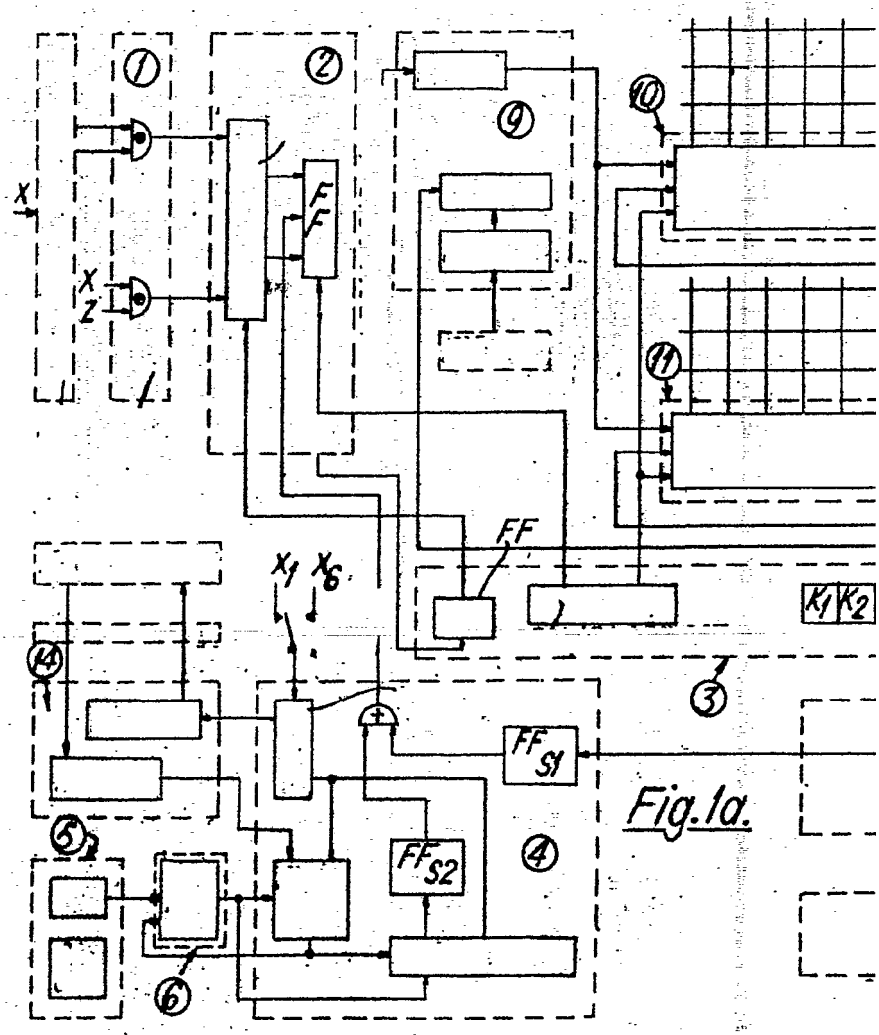
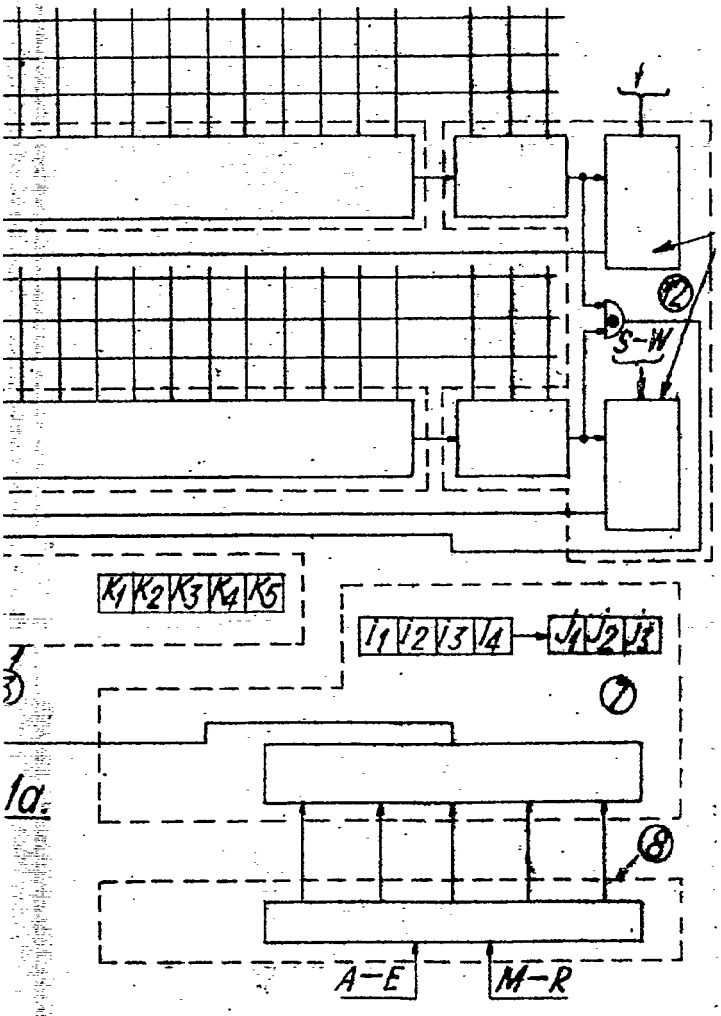


Fig.1a.

STANDARD ELECTRICA, S. A.

341955



17 JUN 1967

EUGENIO BARROSO
Secretario General

341955

341955

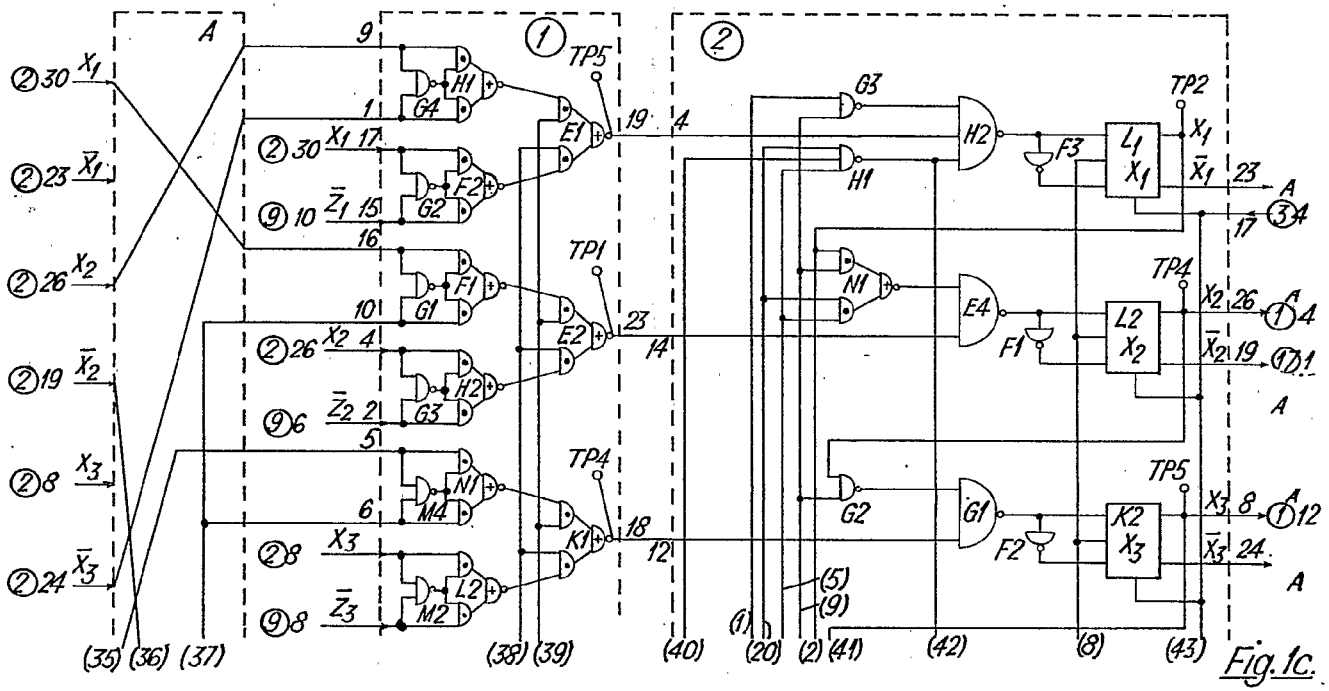


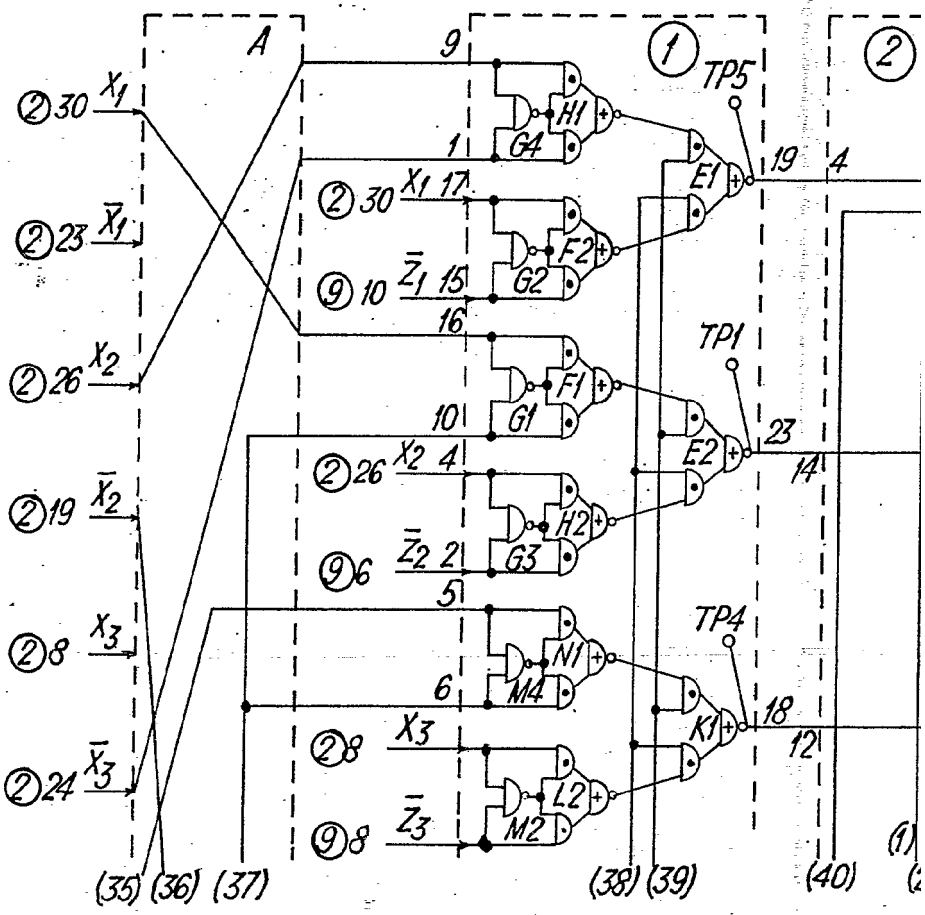
Fig. 1c.

17 JUN 1967

Telefonos Standard Cable

EUGENIO BARROSO
Secretario General

341955


A
1
2
TP5
TP1
TP4
H1
G4
F2
G2
F1
G1
H2
G3
N1
M4
L2
M2
E1
E2
K1
(35)
(36)
(37)
(38)
(39)
(40)

341955

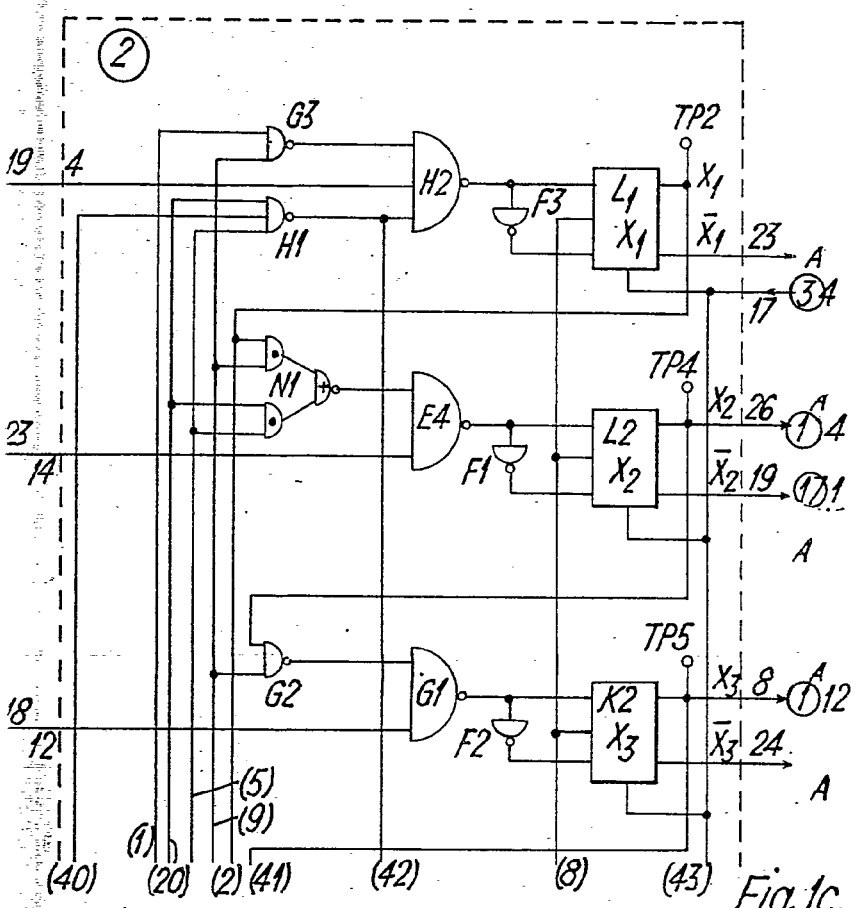


Fig. 1c.

17 JUN. 1967

EUGENIO BARROSO
Secretario General

341955

341955

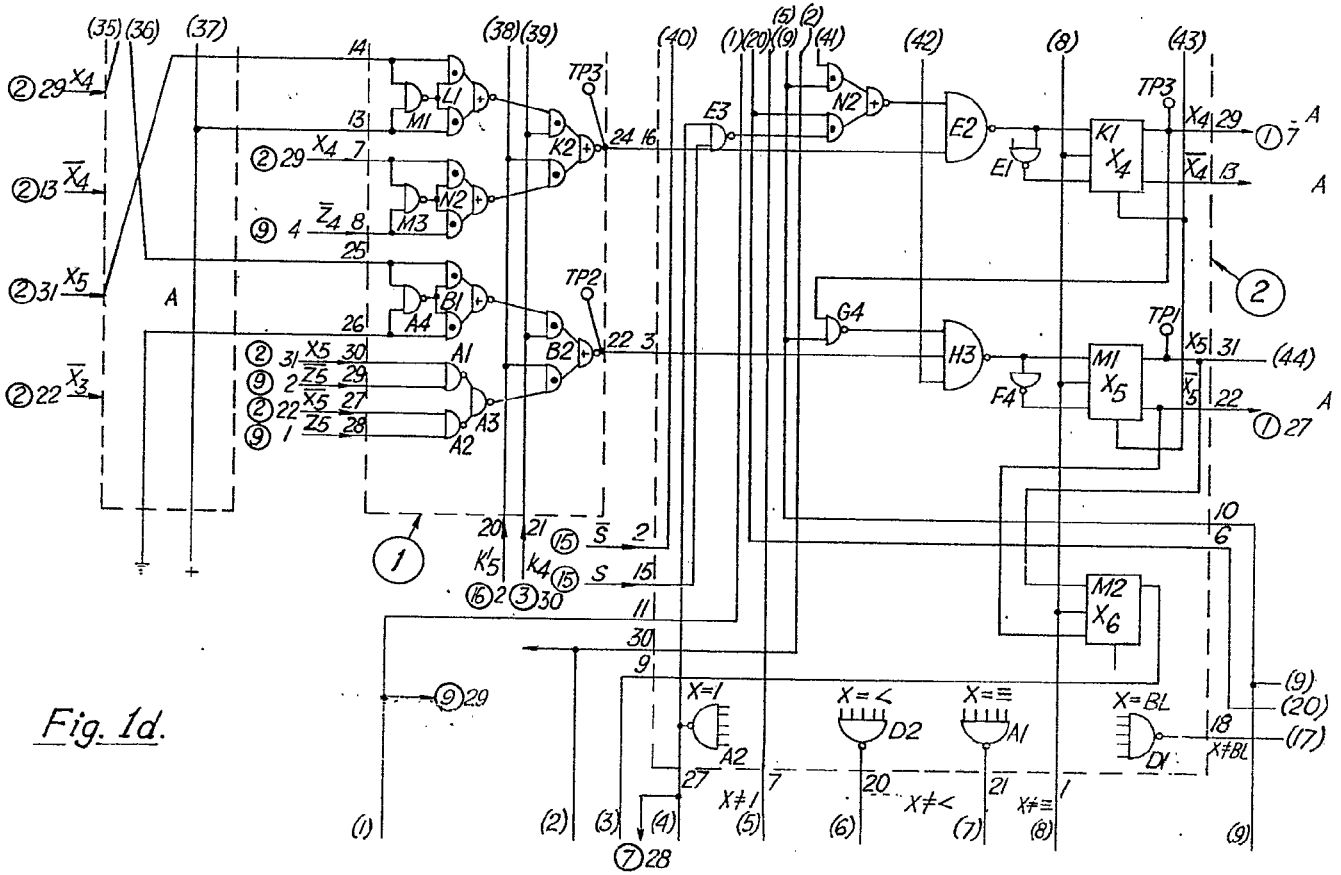


Fig. 1d.

17 OCT 1969

EUGENIO BARROSO
Secretario General

341955

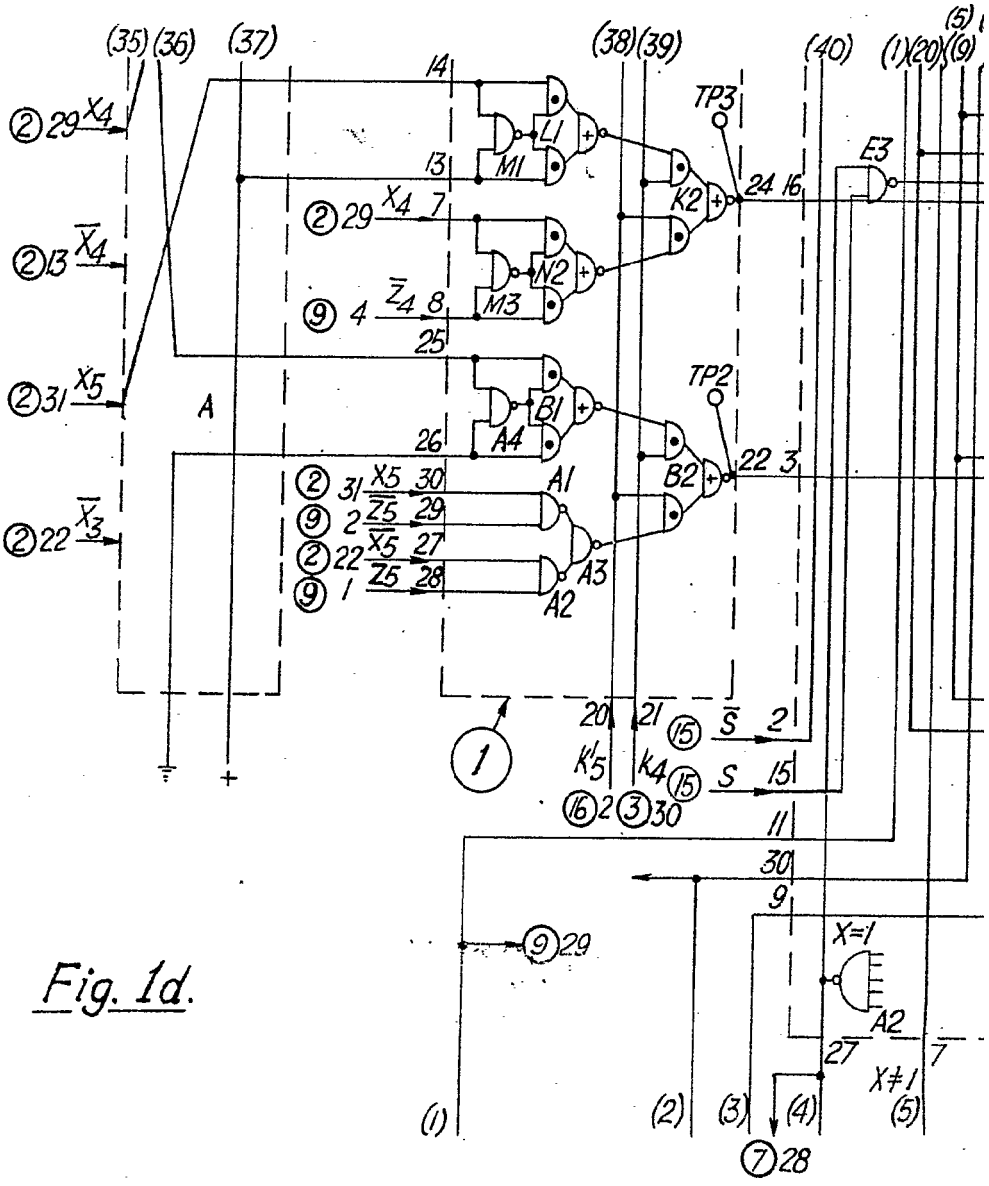
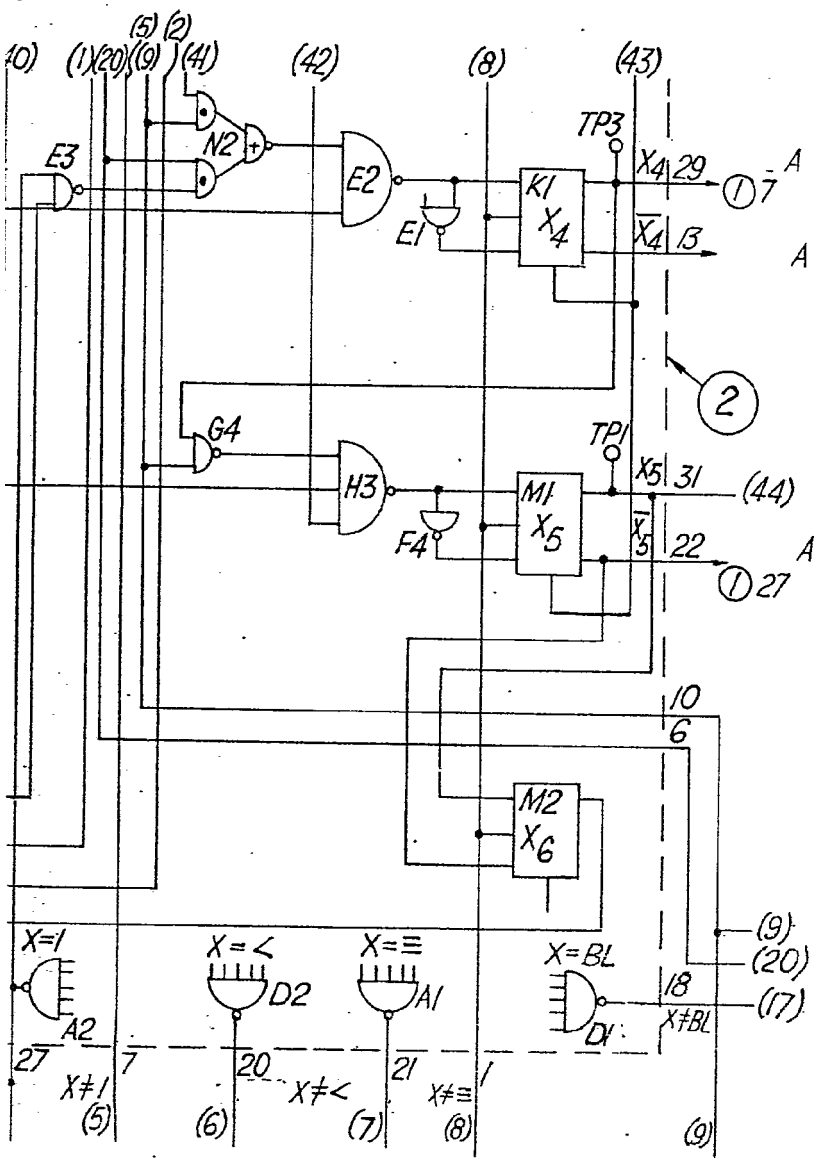


Fig. 1d.

341955



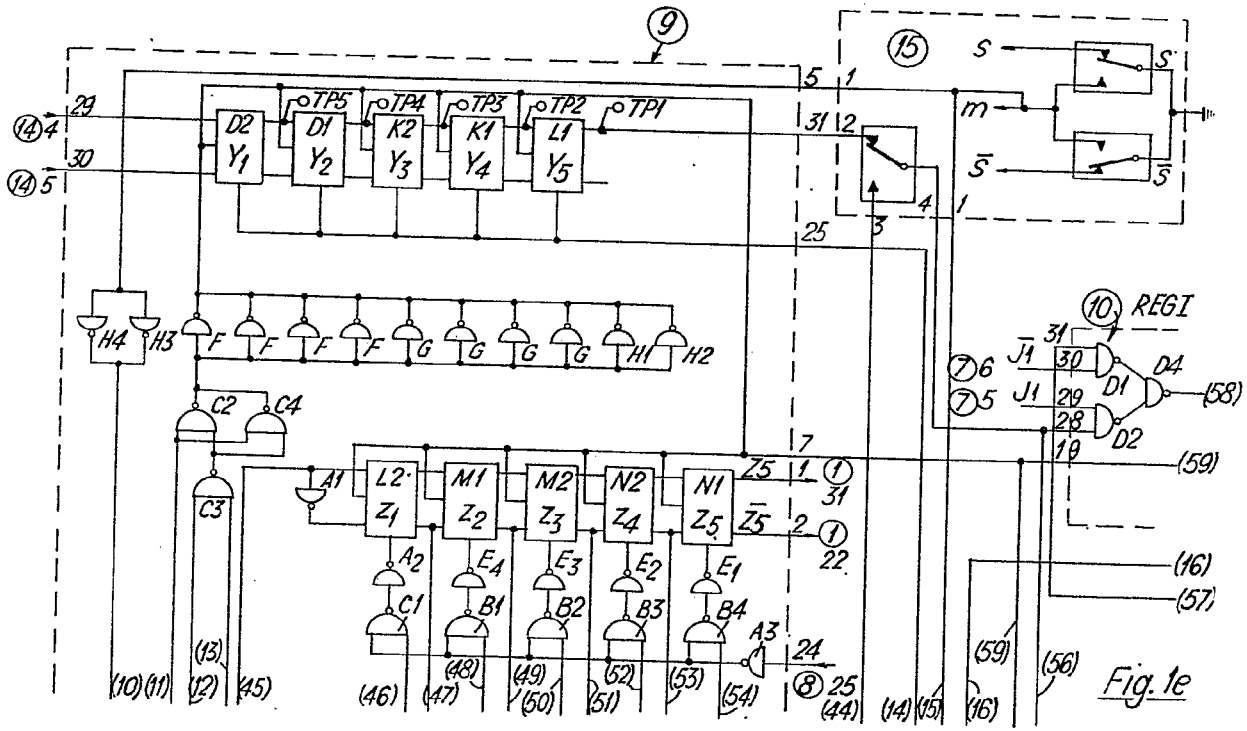
17 JUN 1967

Teléfonos Standard Chilena

EUGENIO BARROSO
Secretario General

341955

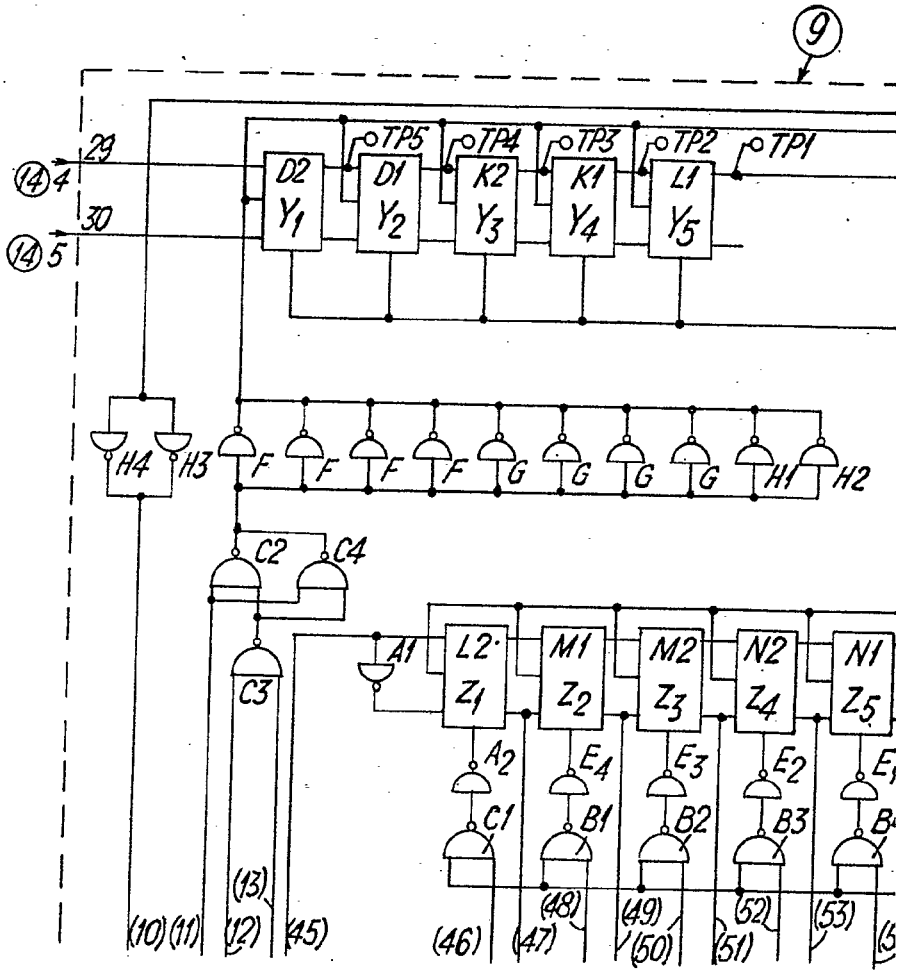
341955



17 JUN 1967

EUGENIO BARROSO
Secretario General

341955


9
TP5
TP4
TP3
TP2
TP1
D2
Y1
D1
Y2
K2
Y3
K1
Y4
L1
Y5
29
30
14 4
14 5
H4
H3
F
F
F
F
G
G
G
G
H1
H2
C2
C4
C3
A1
L2
Z1
M1
Z2
M2
Z3
N2
Z4
N1
Z5
A2
E4
E3
E2
C1
B1
B2
B3
(10)
(11)
(12)
(13)
(45)
(46)
(47)
(48)
(49)
(50)
(51)
(52)
(53)

341955

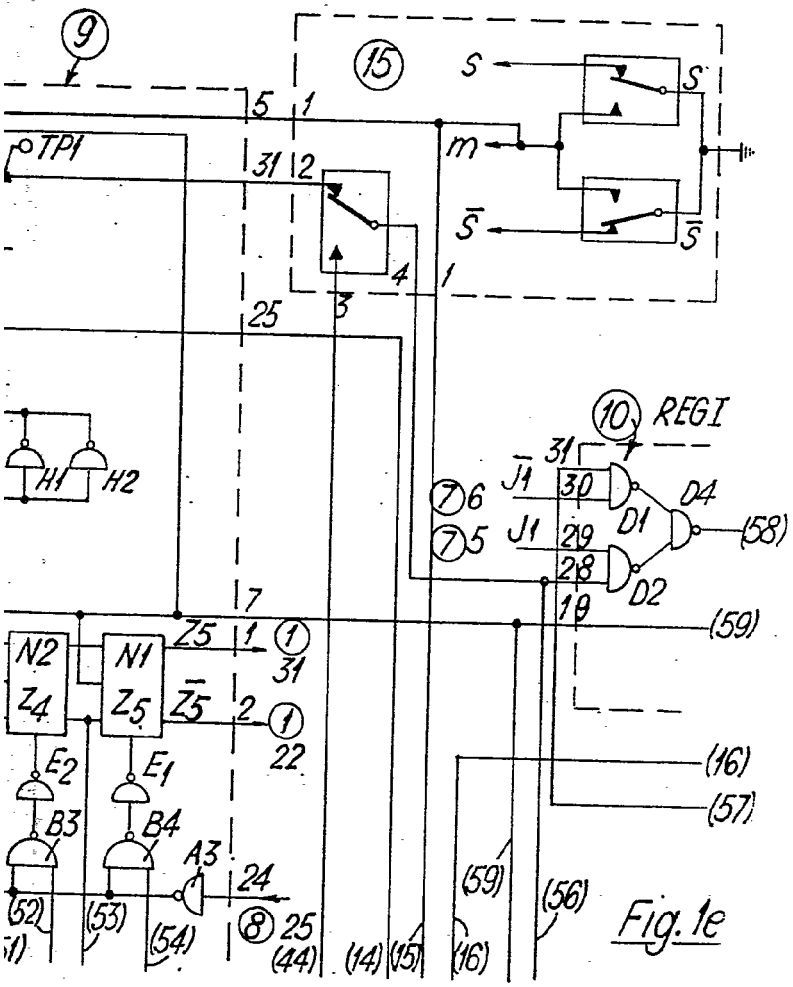


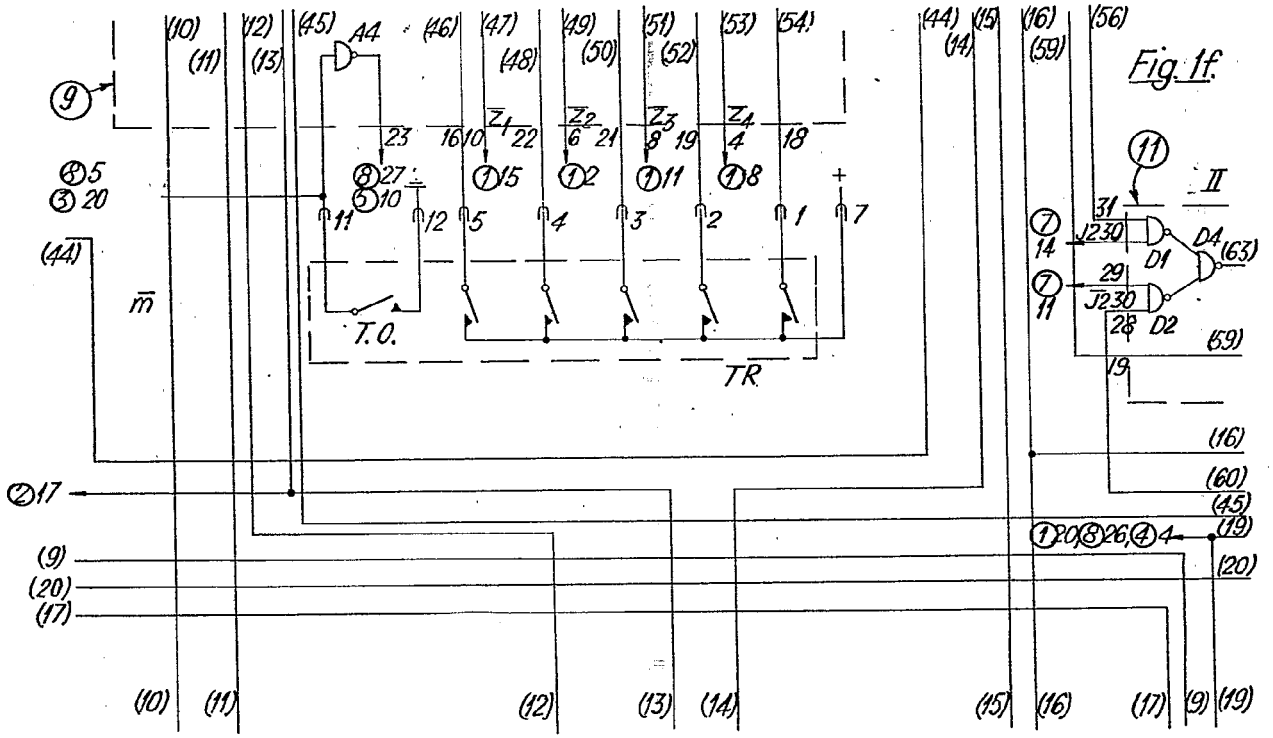
Fig. 1e

17 JUN. 1967

EUGENIO BARROSO
Secretario General

341955

341955

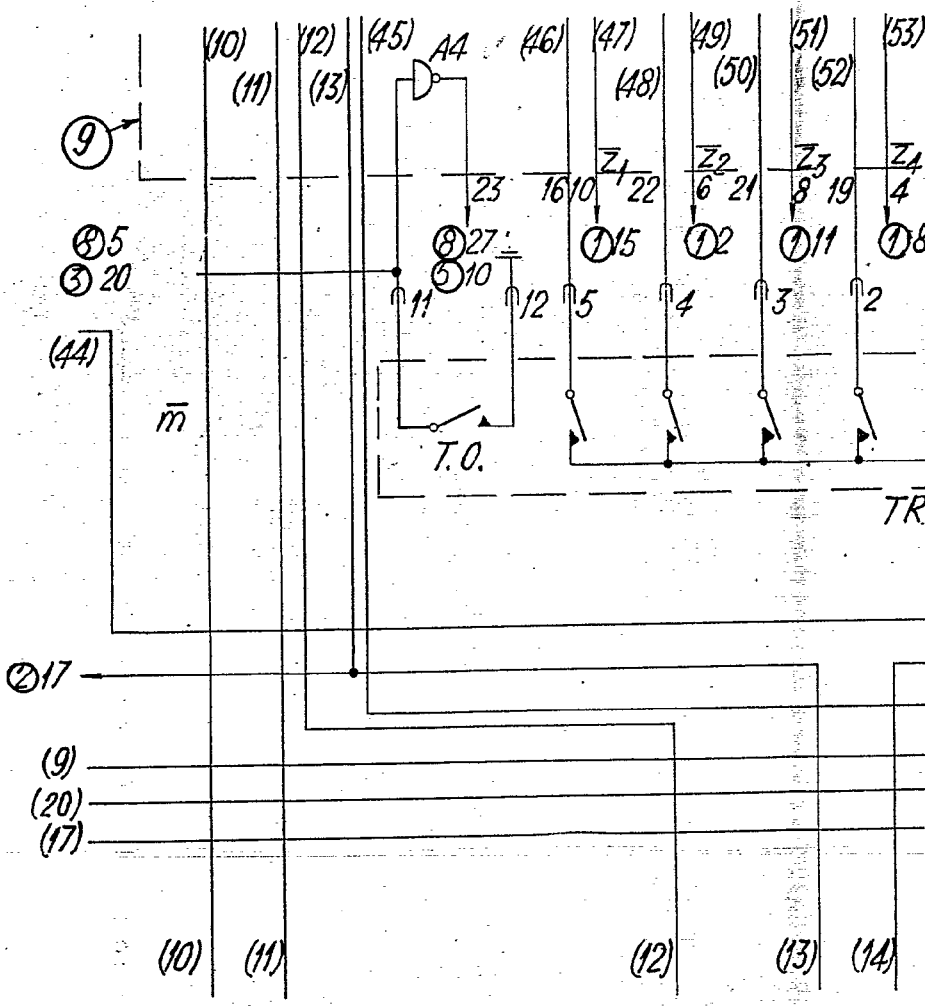


17 JUN. 1967

Teléfonos Standard Cables

EUGENIO BARROSO
Secretario General

341955


(10)
(11)
(12)
(13)
(45)
A4
(46)
(47)
(48)
(49)
(50)
(51)
(52)
(53)
9
23
16
10
Z1
22
Z2
6
21
Z3
8
19
Z4
4
8 5
3 20
8 27
5 10
11
12
5
4
3
2
(44)
m
T.O.
TR
2 17
(9)
(20)
(17)
(10)
(11)
(12)
(13)
(14)

341955

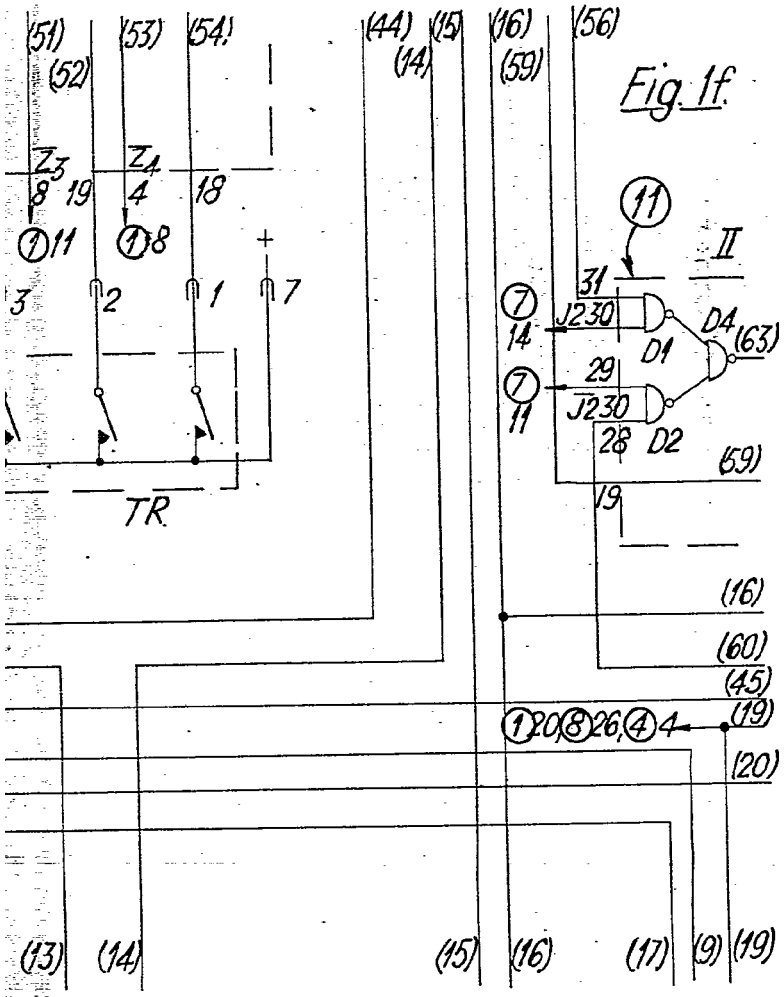


Fig. 1f.

17 JUN. 1967

Teléfonos Standard cables

EUGENIO BARROSO
Secretario General

341955

341955

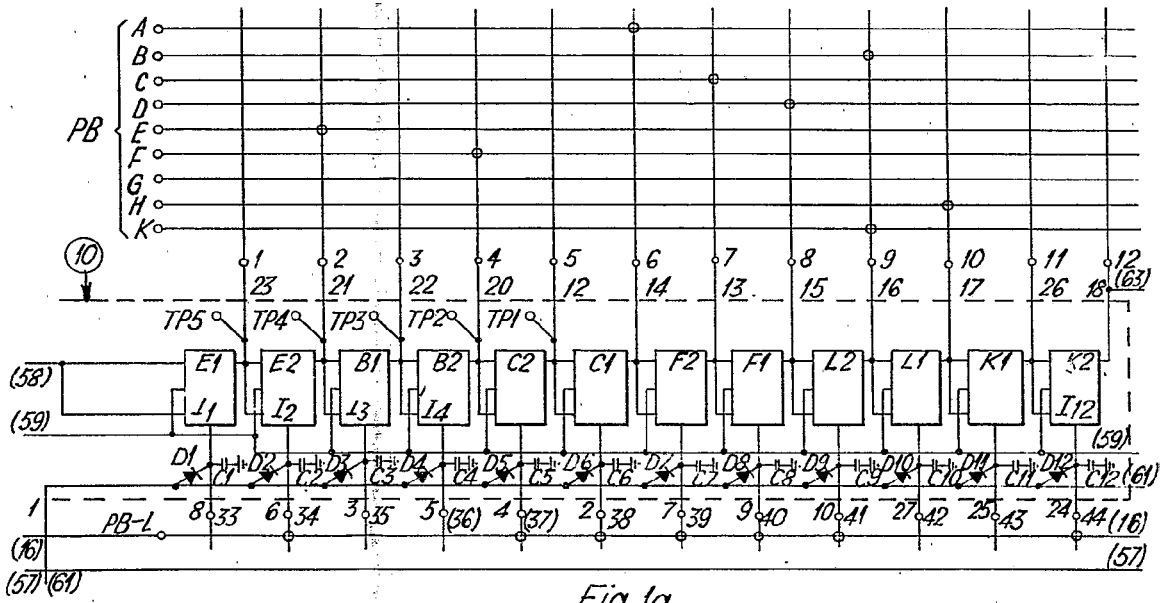


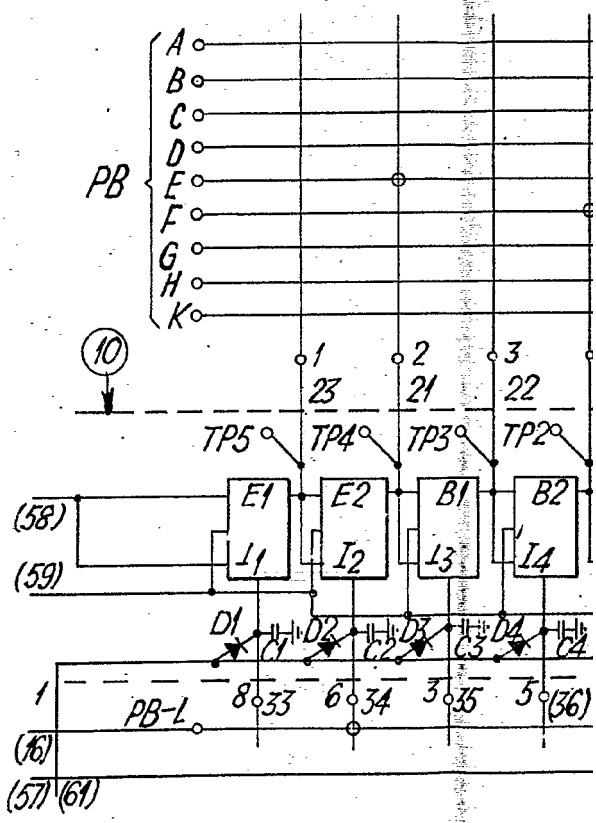
Fig. 1g.

17 JUN 1957

Teléfonos Standard cables

EUGENIO BARROSO
Secretario General

341955


PB
A
B
C
D
E
F
G
H
K
10
1
2
3
23
21
22
TP5
TP4
TP3
TP2
E1
E2
B1
B2
I1
I2
I3
I4
(58)
(59)
D1
D2
D3
D4
C1
C2
C3
C4
1
PB-L
8
33
6
34
3
35
5
(36)
(16)
(57)
(61)

341955

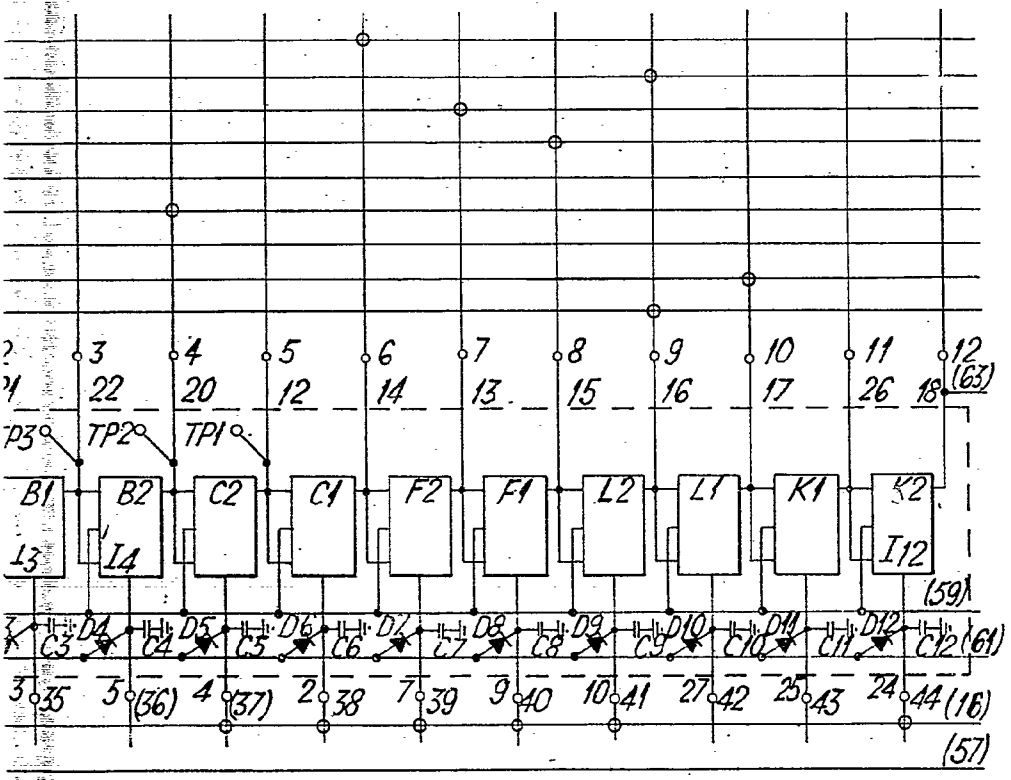


Fig. 1g.

17 JUN 1967

Telefonos Standard Cables

EUGENIO BARROSO
Secretario General

STANDARD ELECTRICA, S. A.

341955

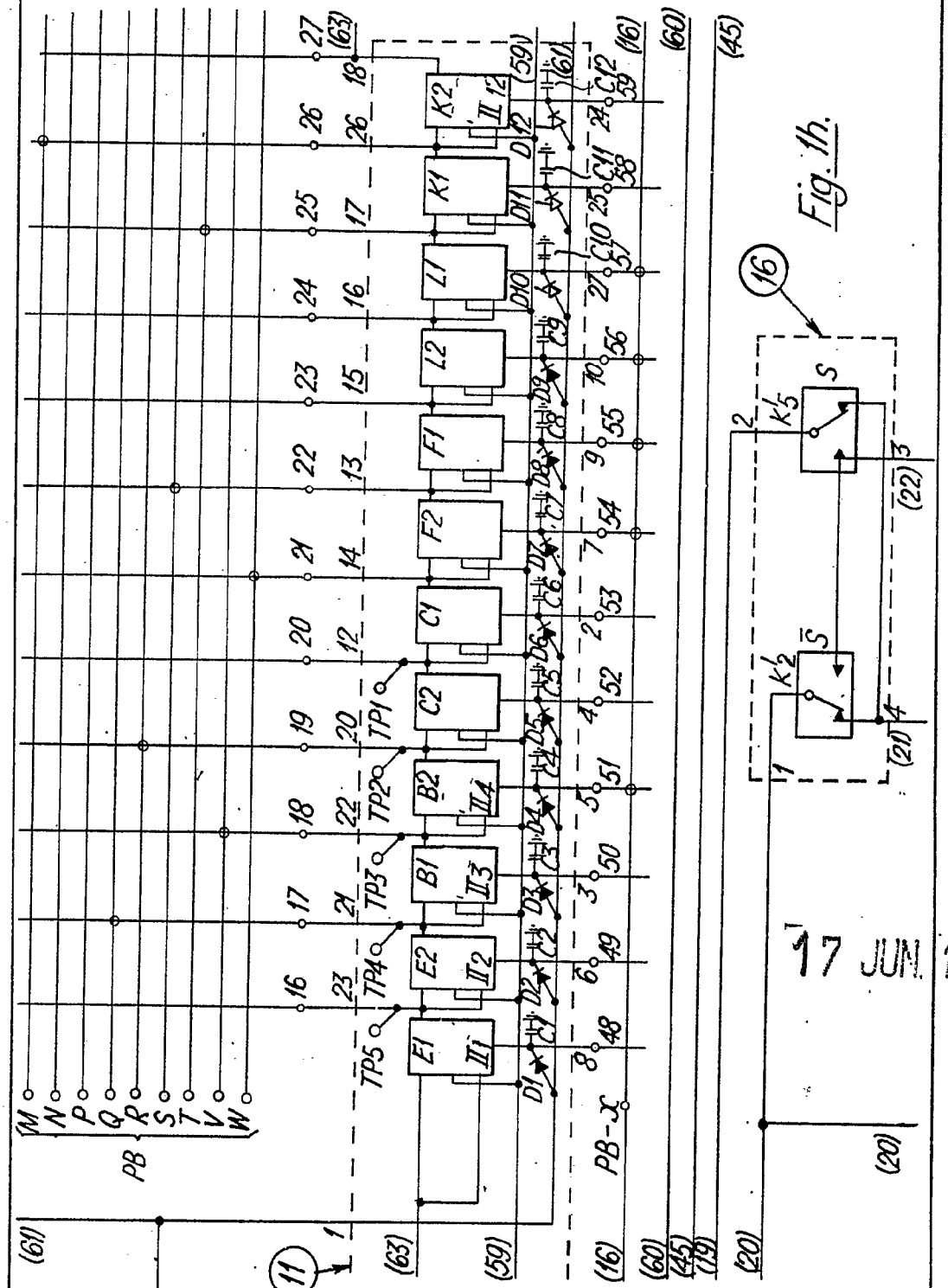


Fig. 1h.

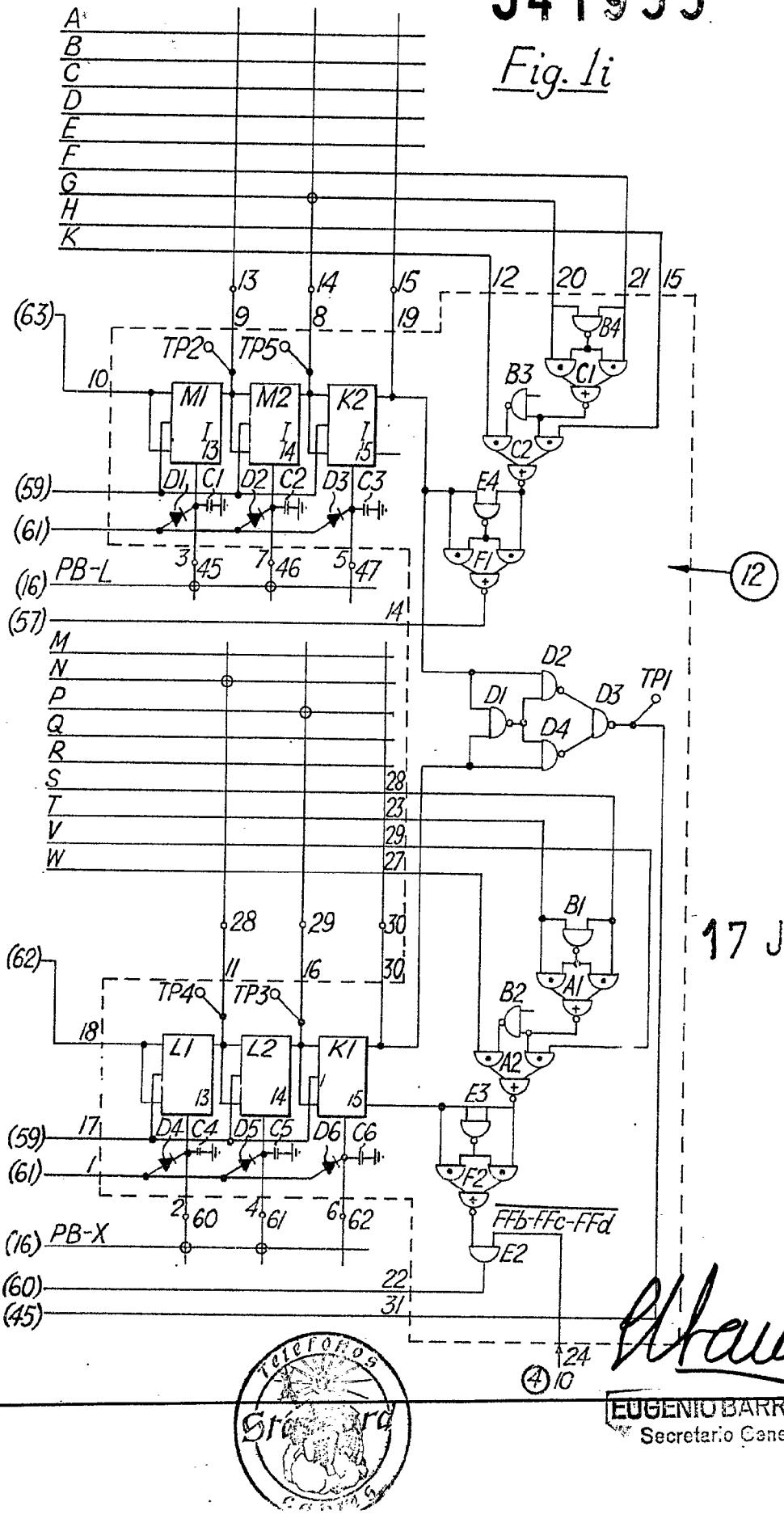
17 JUN. 1967

EUGENIO BARROSO
Secretario General

STANDARD ELECTRICA, S. A.

341955

Fig. 1i



17 JUN. 1967

EUGENIO BARROSO
Secretario General

341955

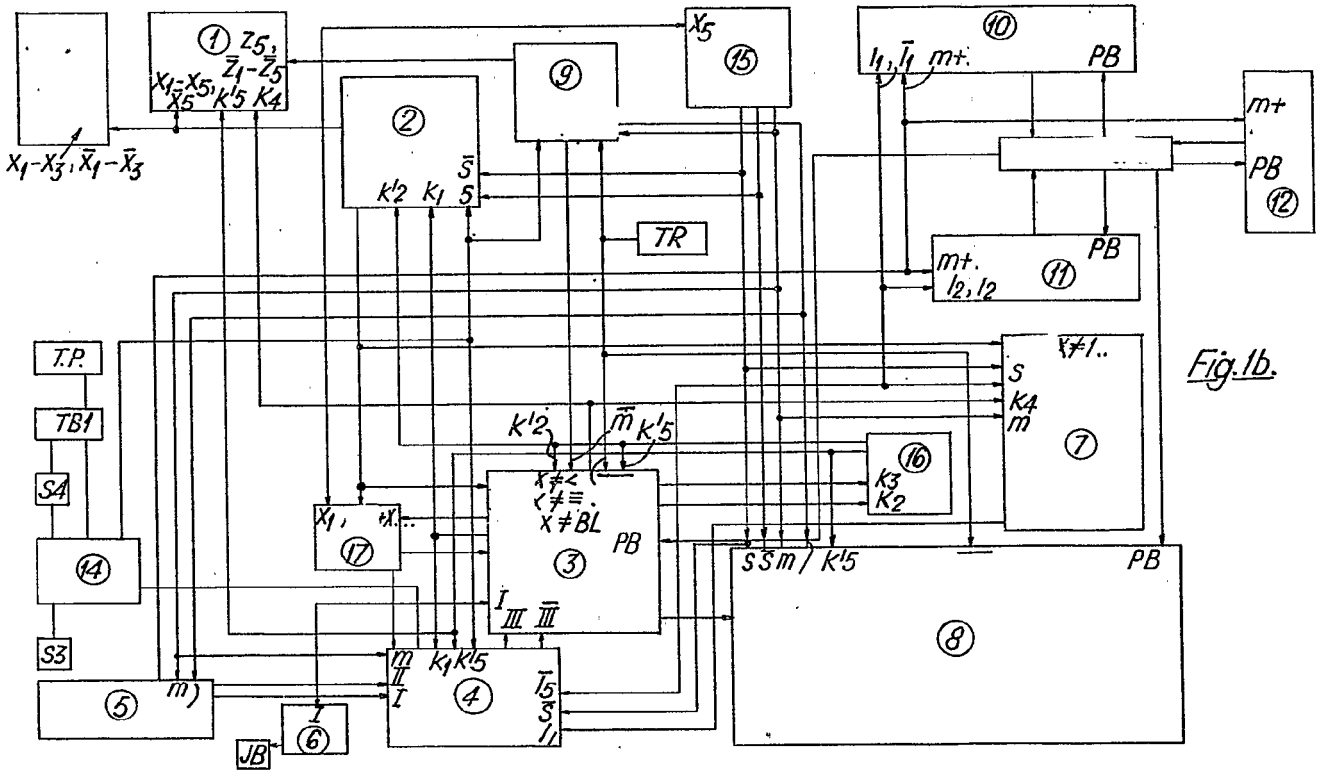
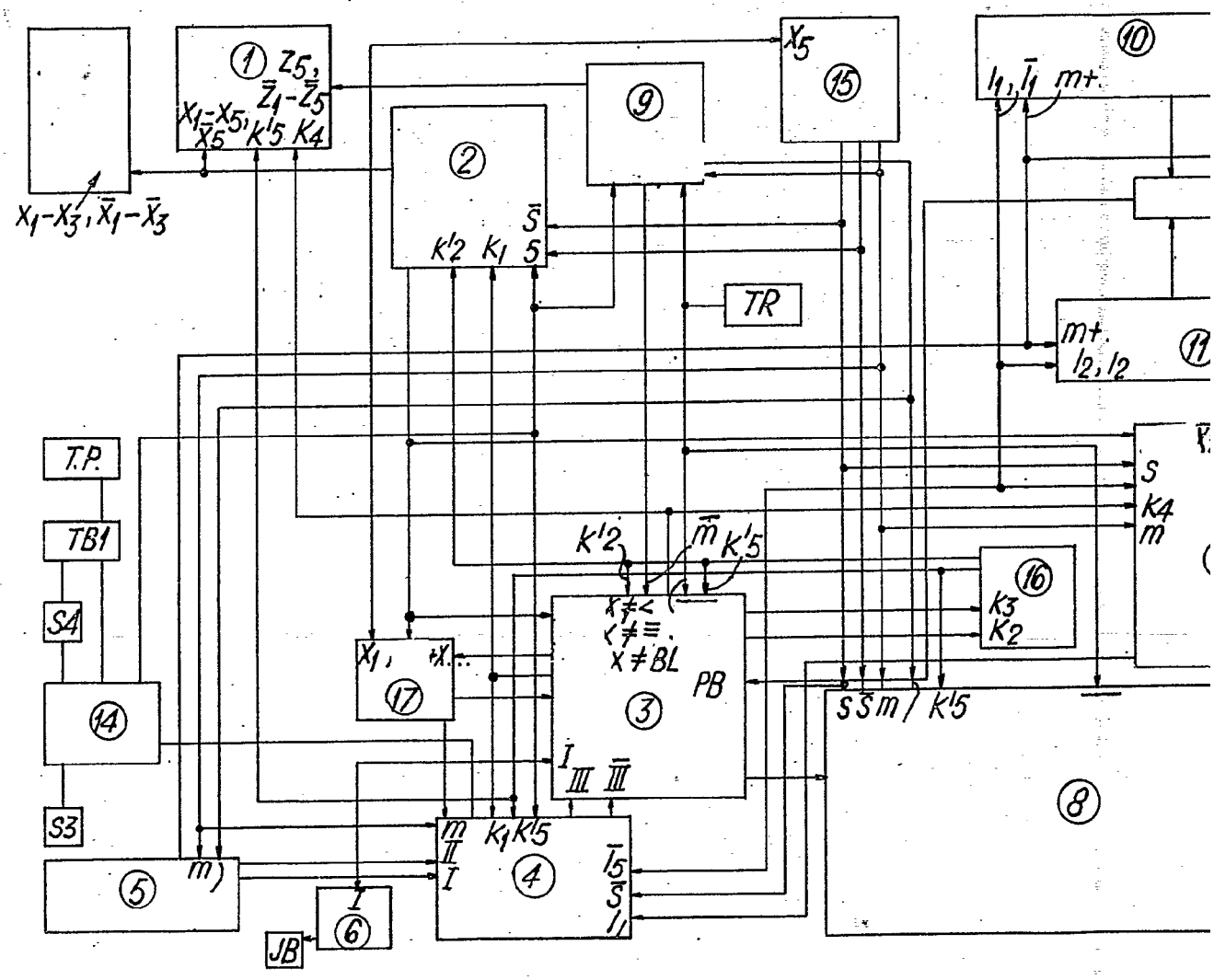


Fig. 1b.

Fig. 2a.

341955



341955

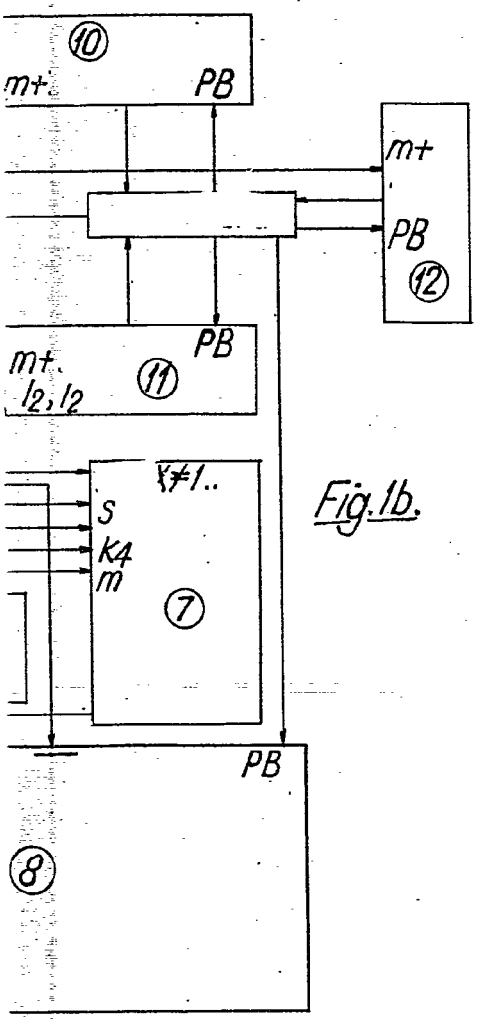
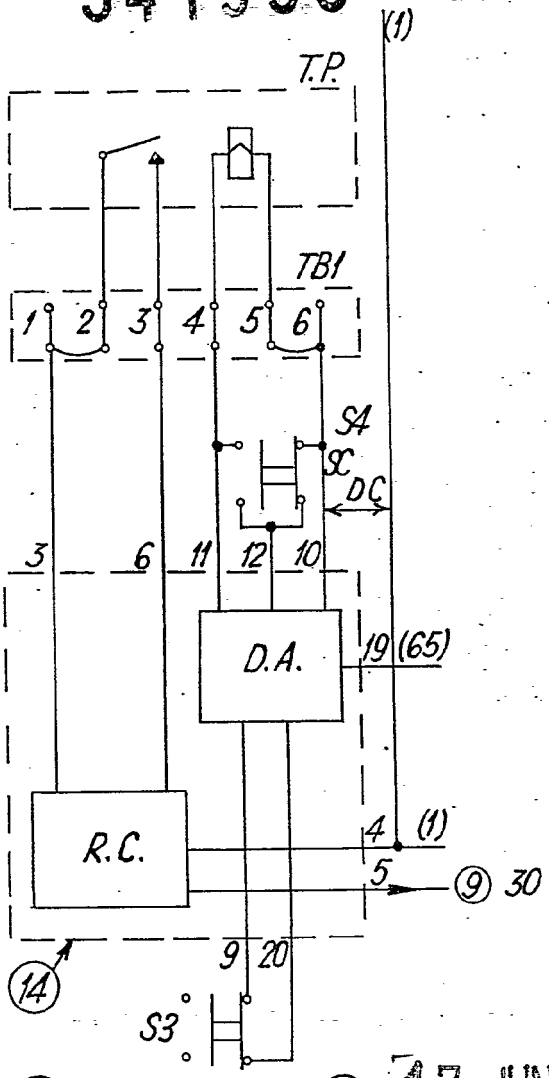


Fig. 1b.



17 JUN. 1967

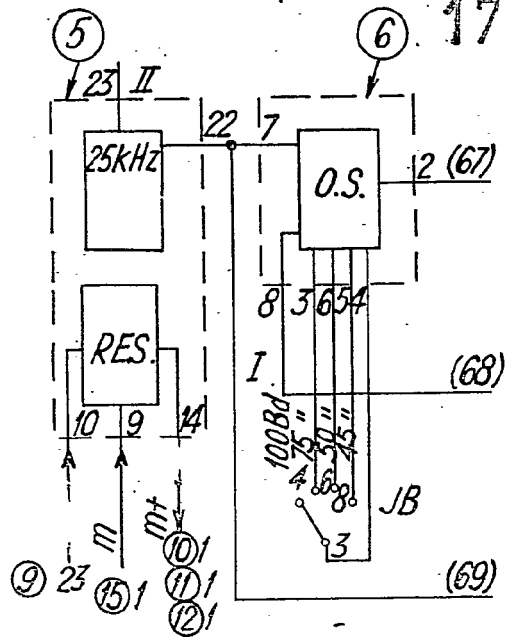


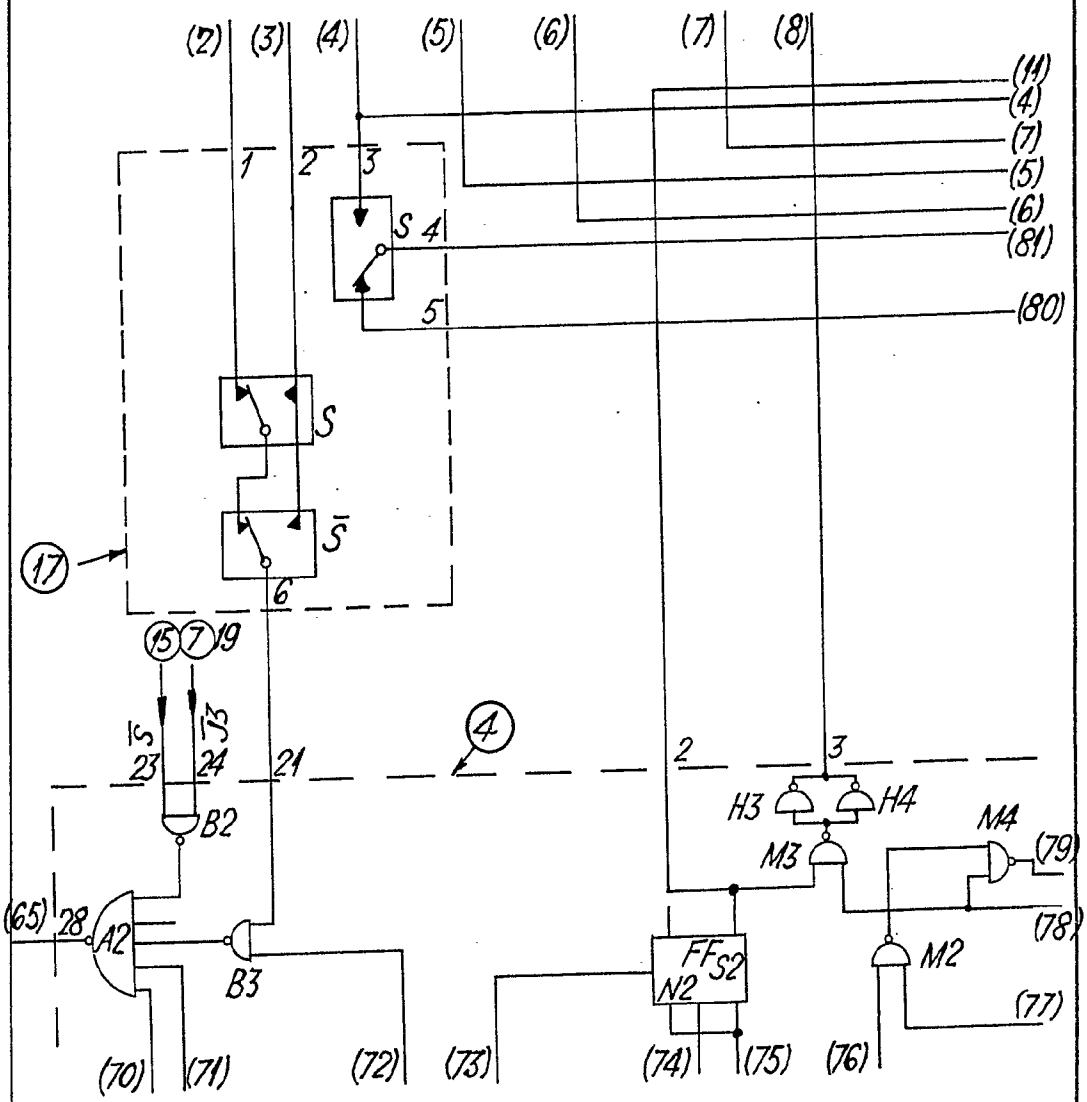
Fig. 2a.

STANDARD ELECTRICA, S. A.

(6:

Fig. 2b.

341955



17 JUN 1967

Telefonos Standard Cables

EUGENIO BARROS
Secretario General

341955

341955

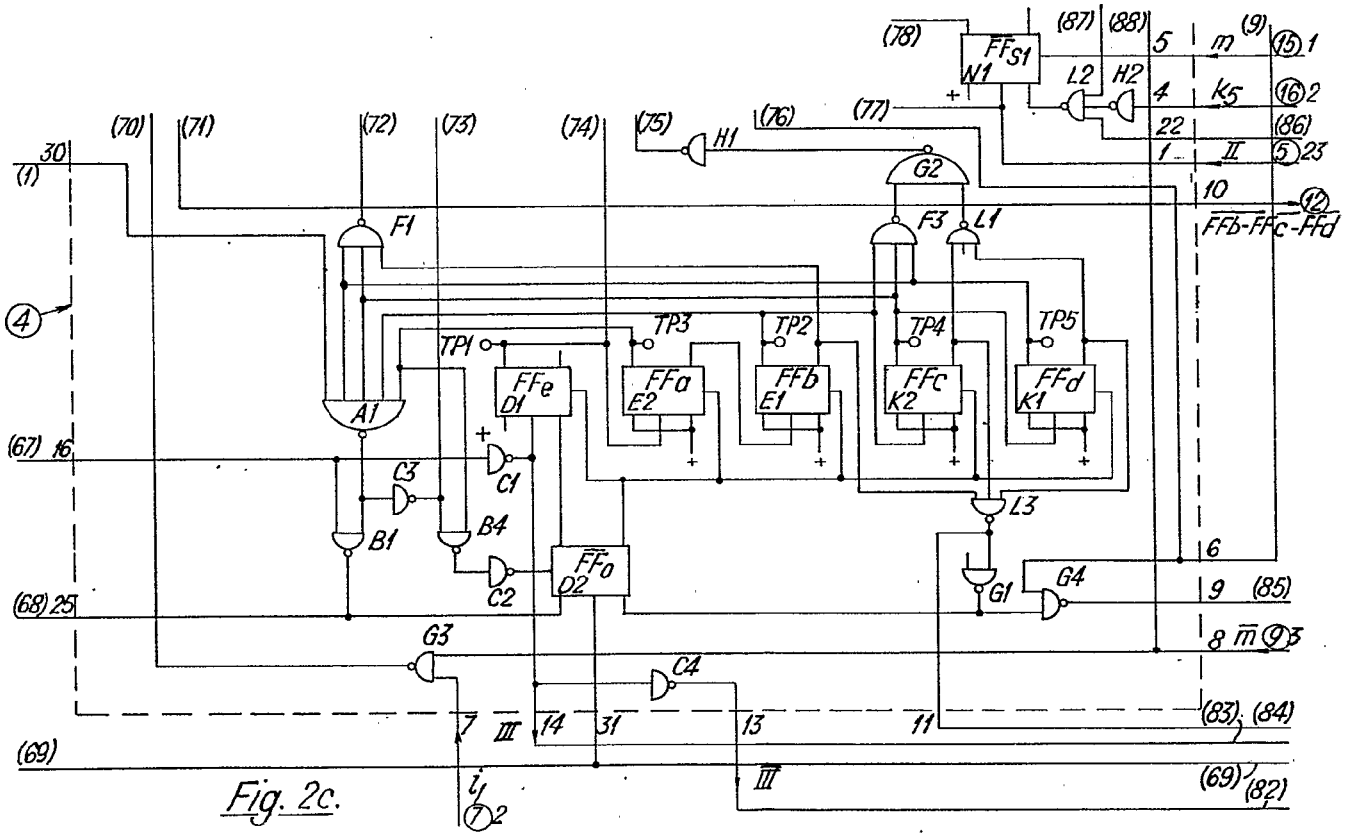


Fig. 2c.

17 JUIN 1967

341955

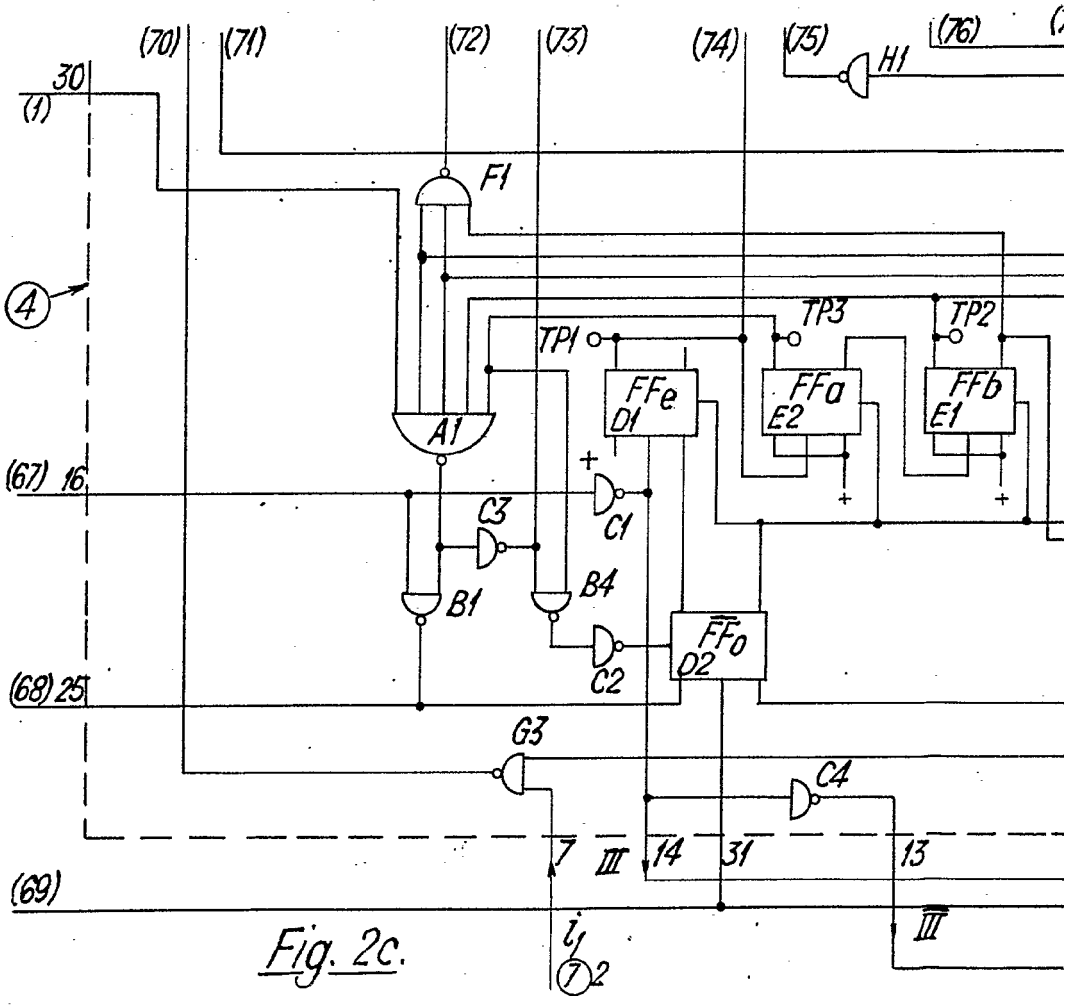
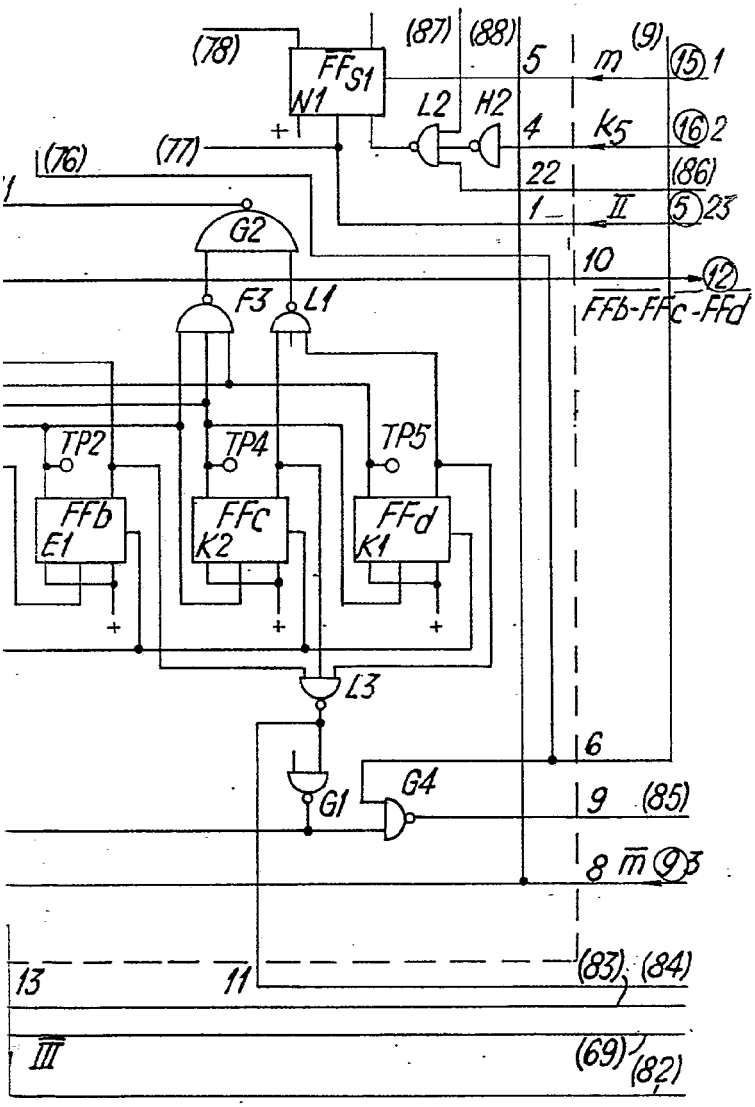


Fig. 2c.

341955



17 JUN. 1967

341955

341955

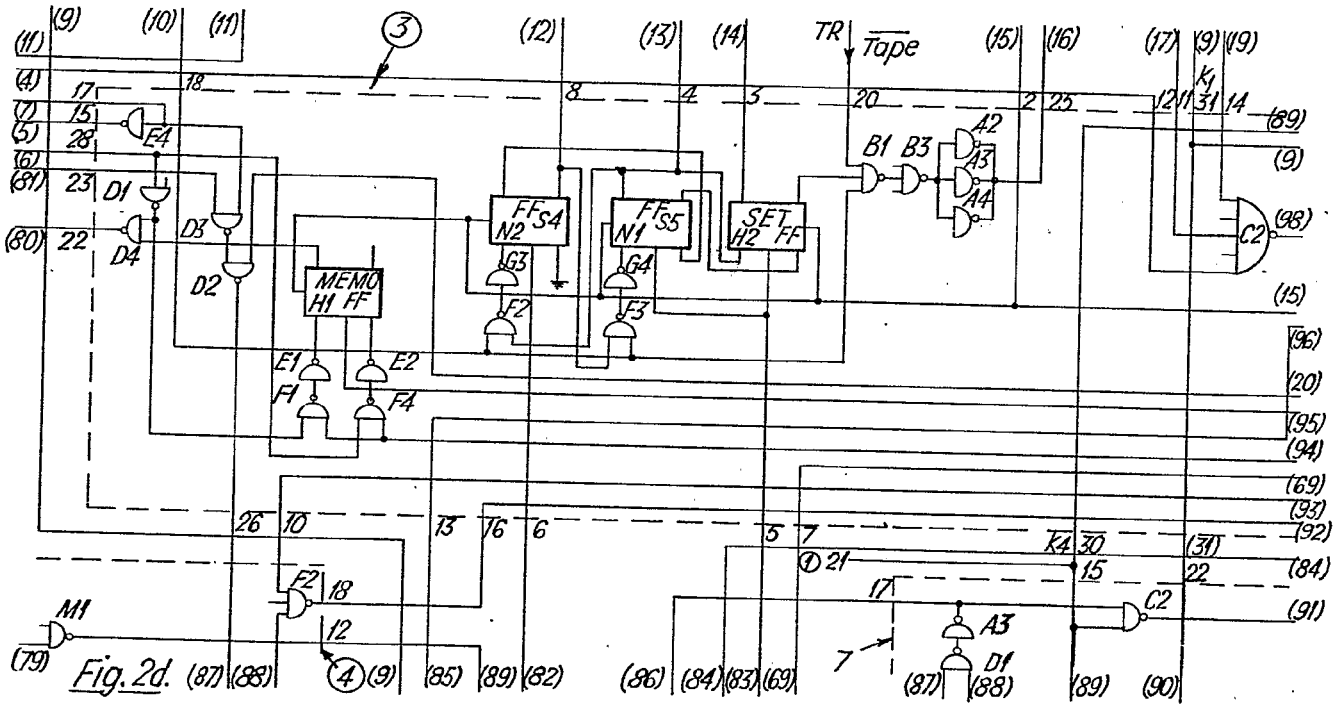


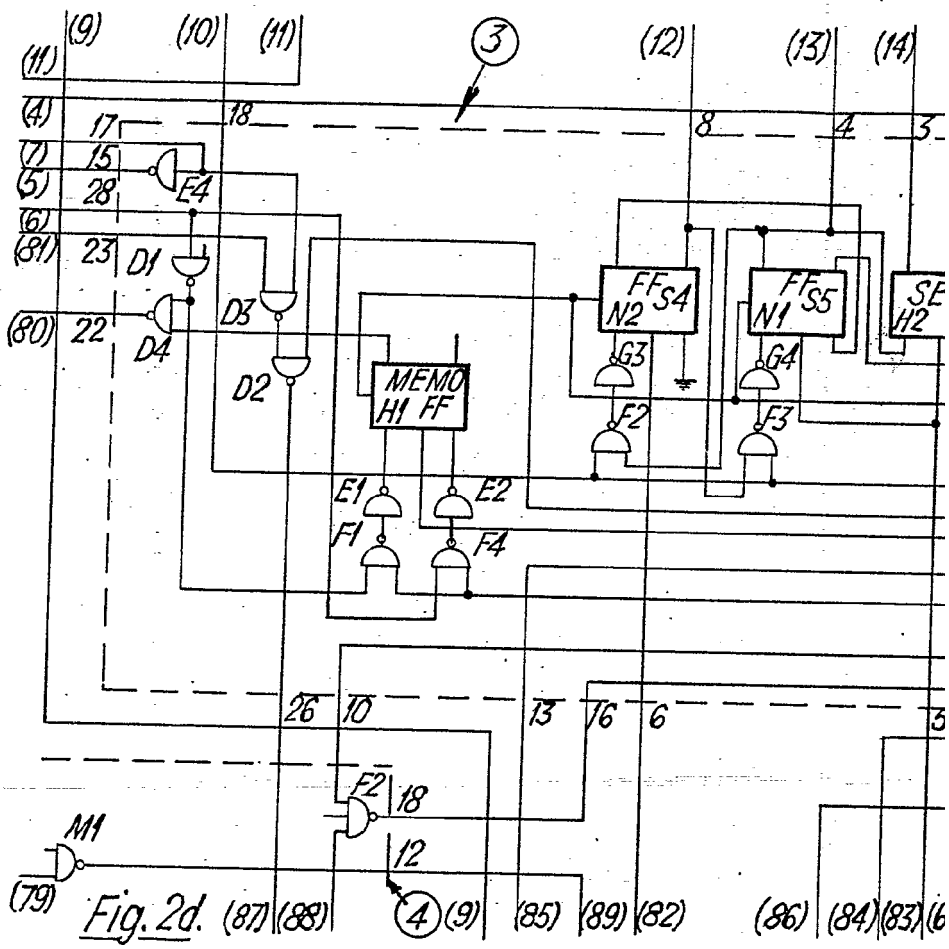
Fig. 2d.

1 JUN. 1967

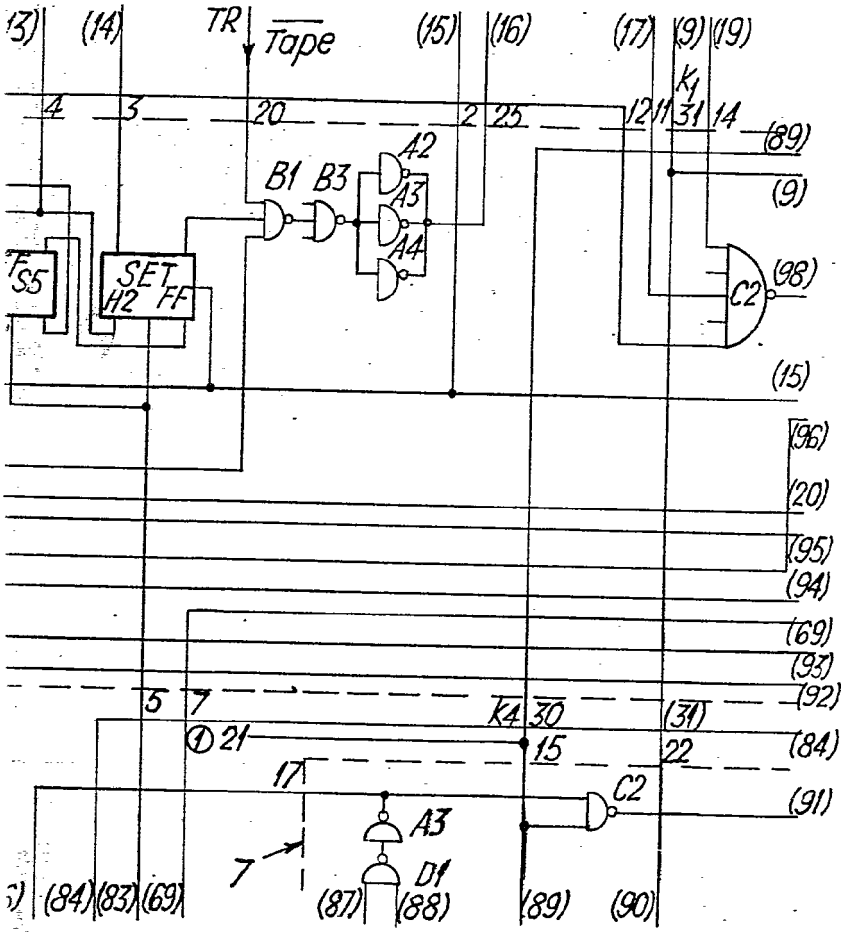
Telefonos Standard Cables

EUGENIO [illegible]
Secretario General

341955


(9)
(10)
(11)
3
(12)
(13)
(14)
(11)
(4)
17
18
8
4
3
(7)
15
E4
(5)
28
(6)
(81)
23
D1
D3
(80)
22
D4
D2
MEMO
H1 FF
FF S4
N2
FF S5
N1
SE
H2
G3
G4
F2
F3
E1
E2
F1
F4
26
10
13
16
6
F2
18
M1
12
(79)
Fig. 2d.
(87)
(88)
4
(9)
(85)
(89)
(82)
(86)
(84)
(83)

341955



18 JUN. 1967

Telefonos Standard Cables

EUGENIO BARROSO
Secretario General

STANDARD ELECTRICA, S. A.

341955

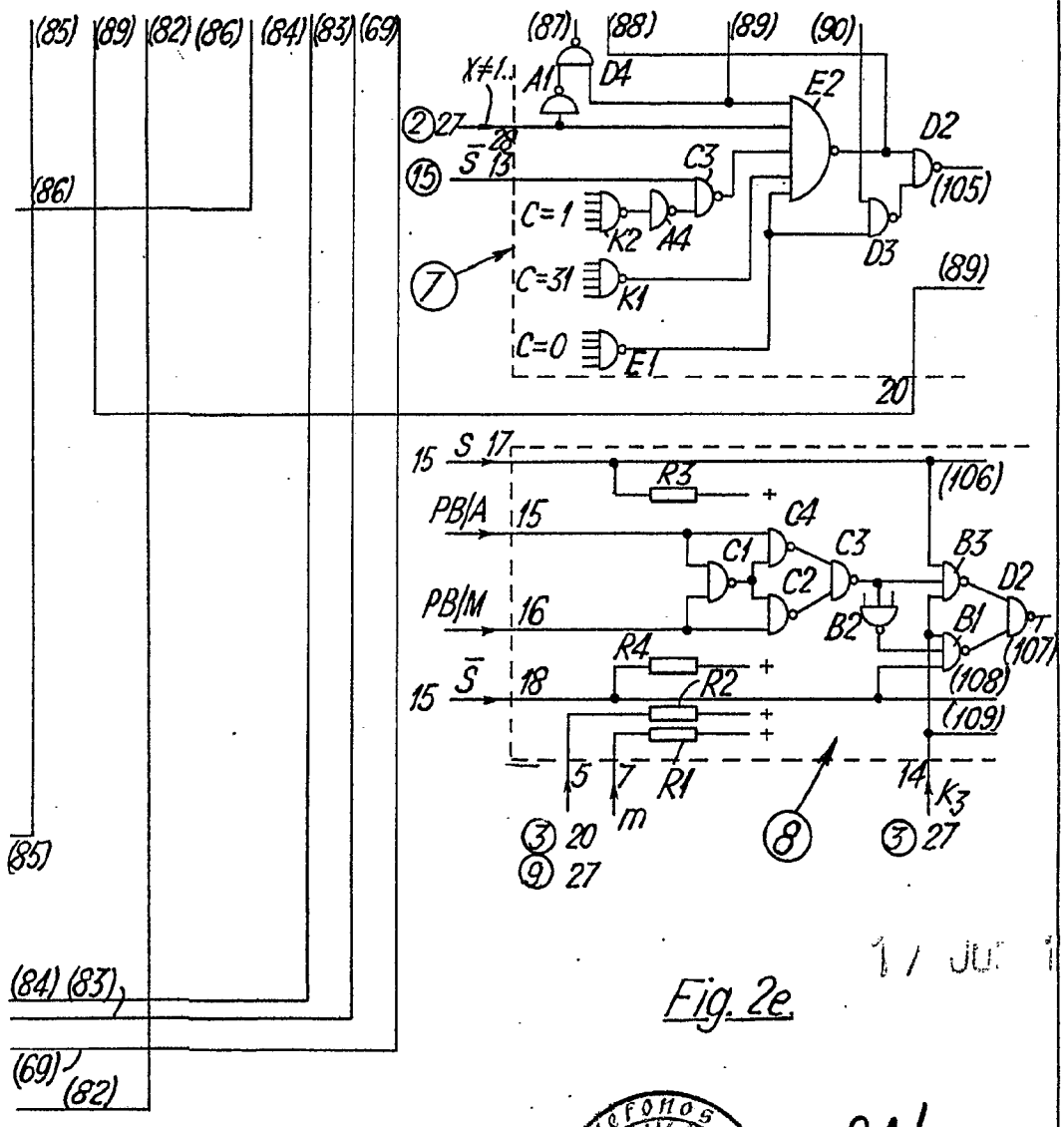


Fig. 2e

341955

341955

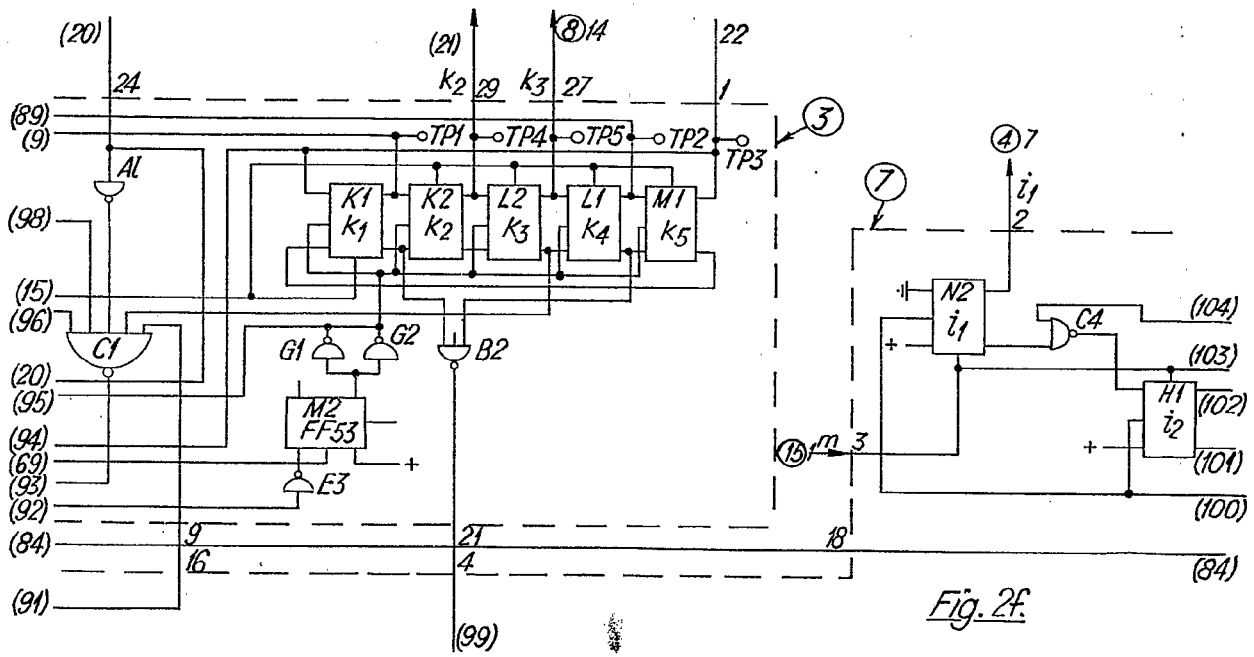
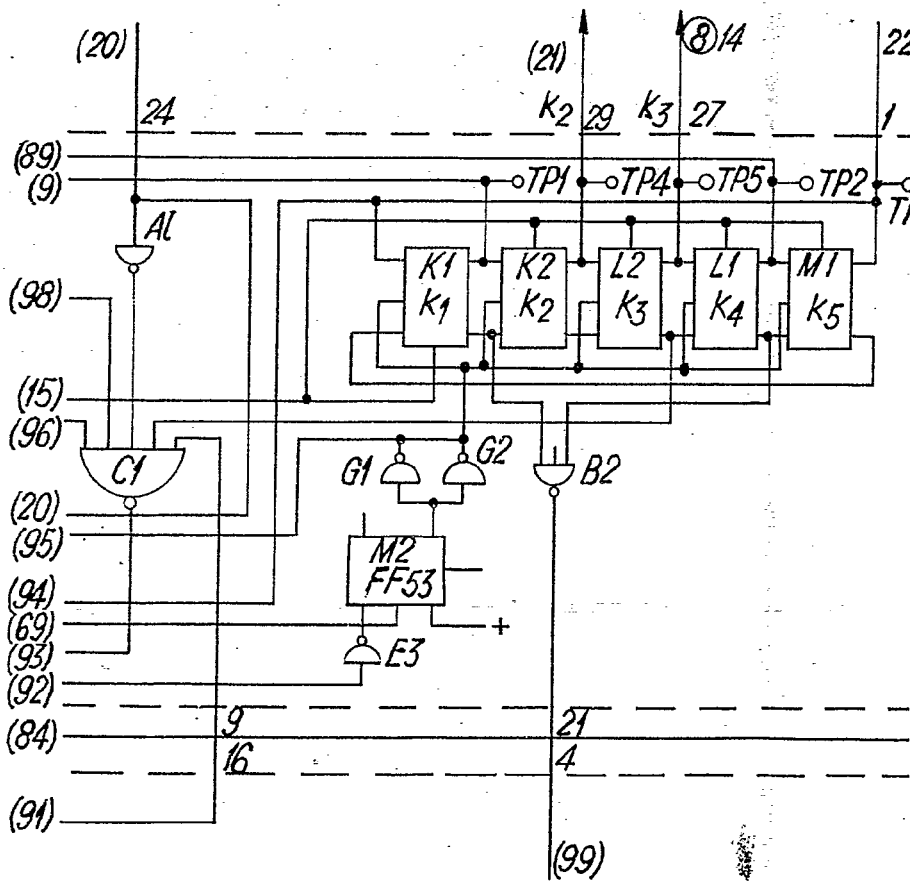


Fig. 2f.

17 JUN 1967

EUGENIO BARROSO
Secretario General

341955


(20)
(21)
⑧14
24
K2 29
K3 27
(89)
(9)
TP1
TP4
TP5
TP2
A1
K1 K1
K2 K2
L2 K3
L1 K4
M1 K5
(98)
(15)
(96)
C1
G1
G2
B2
(20)
(95)
M2 FF53
(94)
(69)
(93)
E3
(92)
(84)
9
16
21
4
(91)
(99)

341955

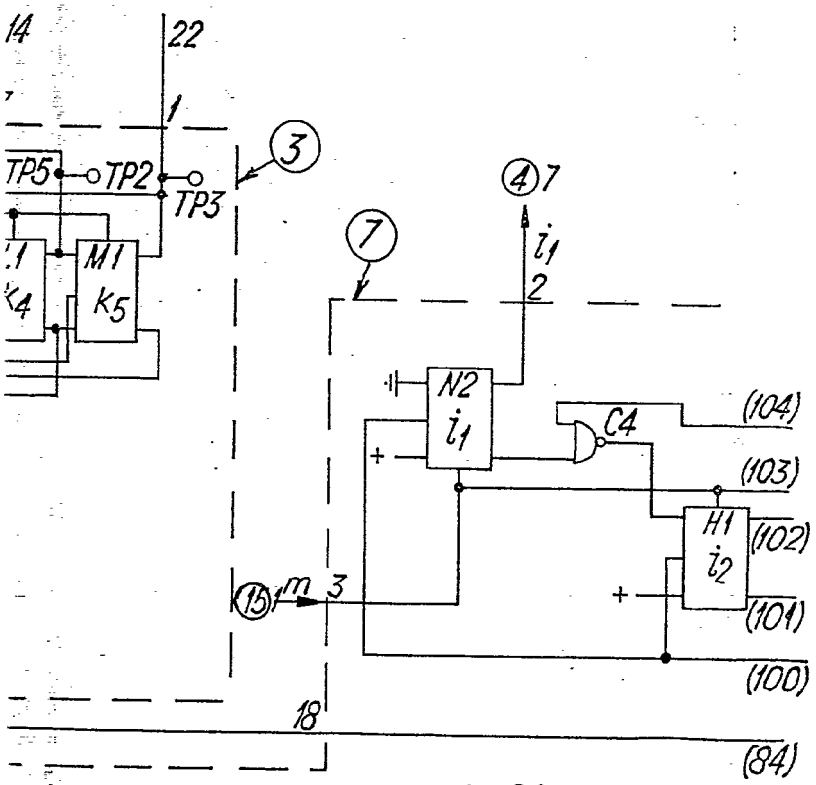


Fig. 2f.

17 JUN 1967

EUGENIO BARROSO
Secretario General

341955

341955

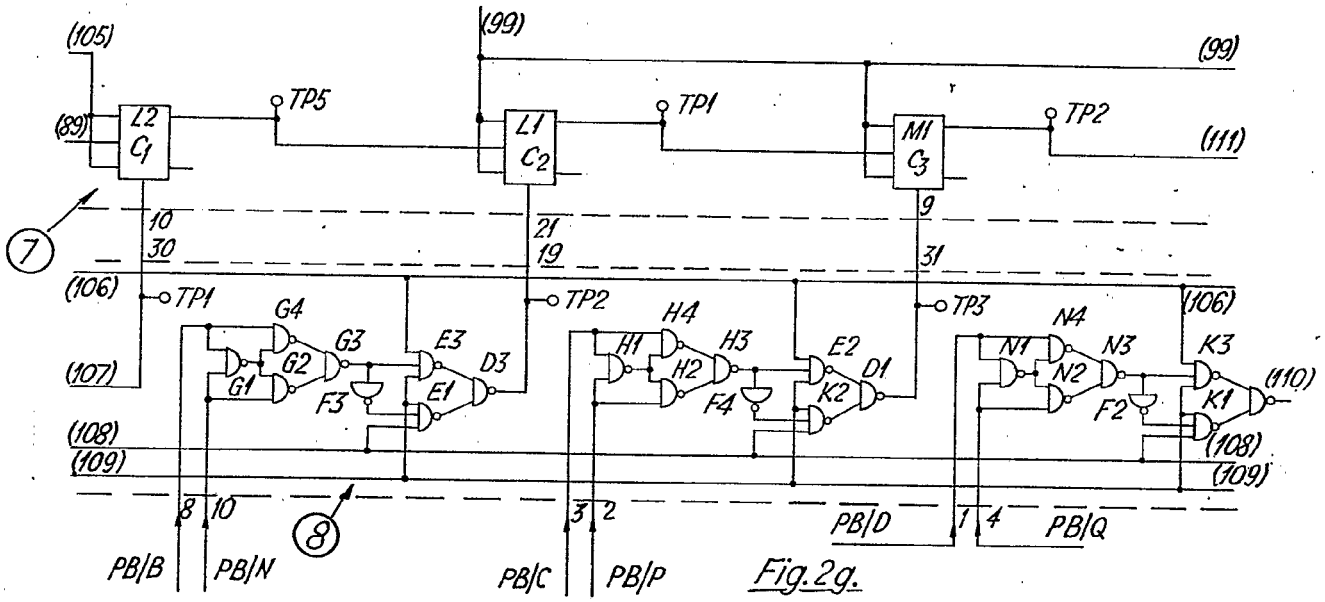
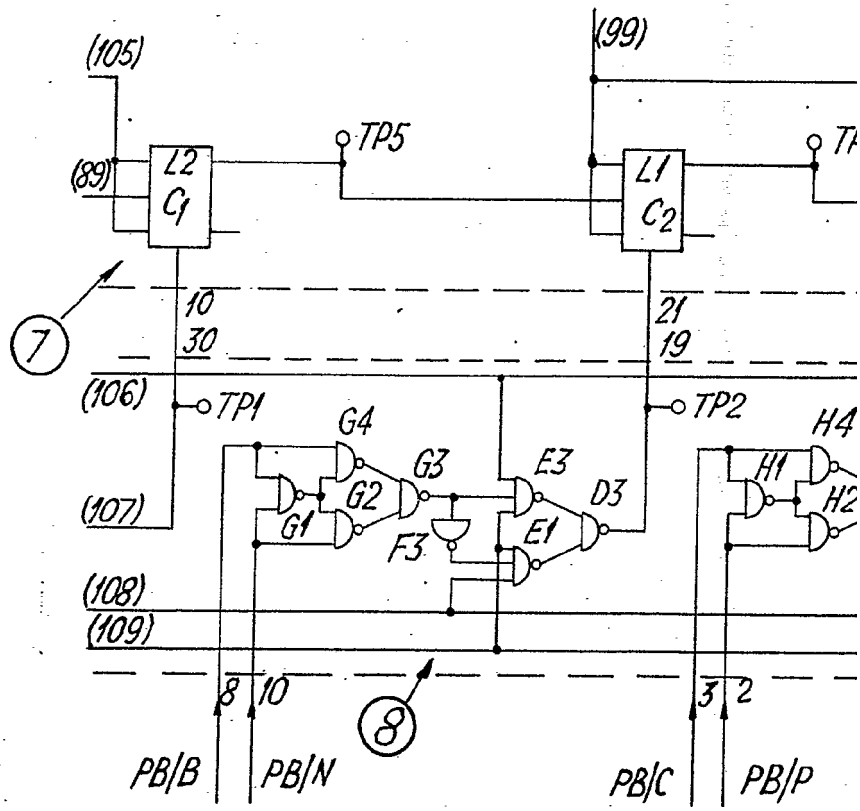


Fig. 2g.

17 JUN 1967

EUGENIO BARROSO
Secretario General

341955


(105)
(99)
(89)
L2
C1
TP5
L1
C2
7
10
30
21
19
(106)
TP1
TP2
(107)
G4
G3
G2
G1
F3
E3
E1
D3
H4
H1
(108)
(109)
8
10
3
2
8
PB/B
PB/N
PB/C
PB/P

341955

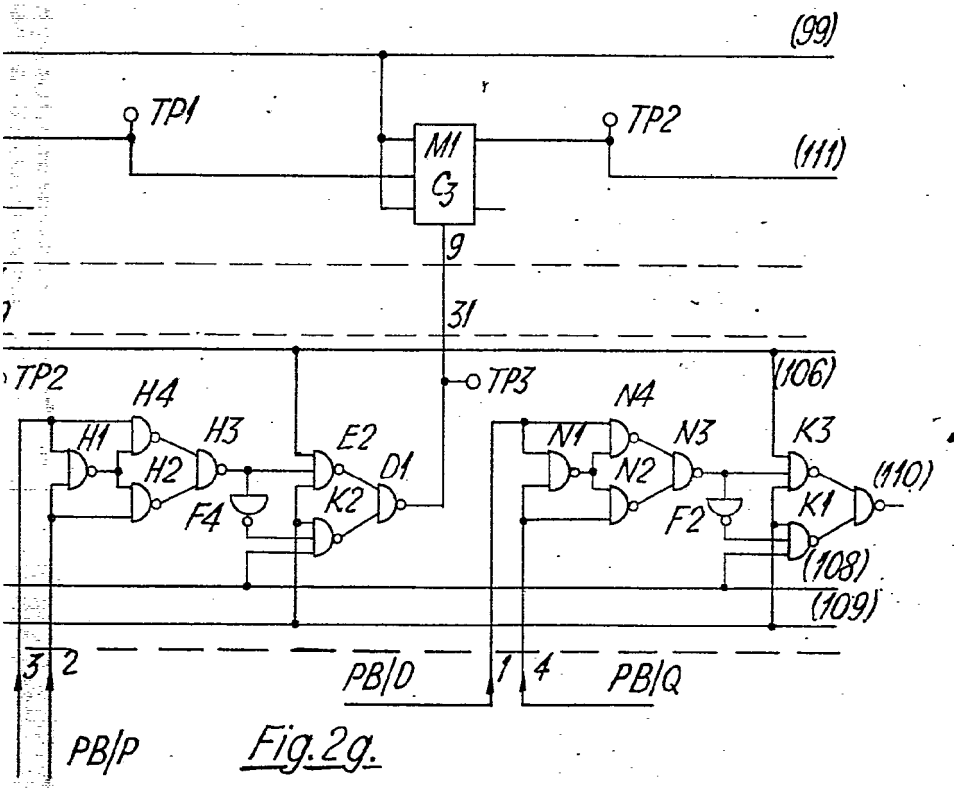


Fig. 2g.

17 JUN 1967

Telefonos Standard Cables

EUGENIO BARROSO
Secretario General

STANDARD ELECTRICA, S. A.

341955

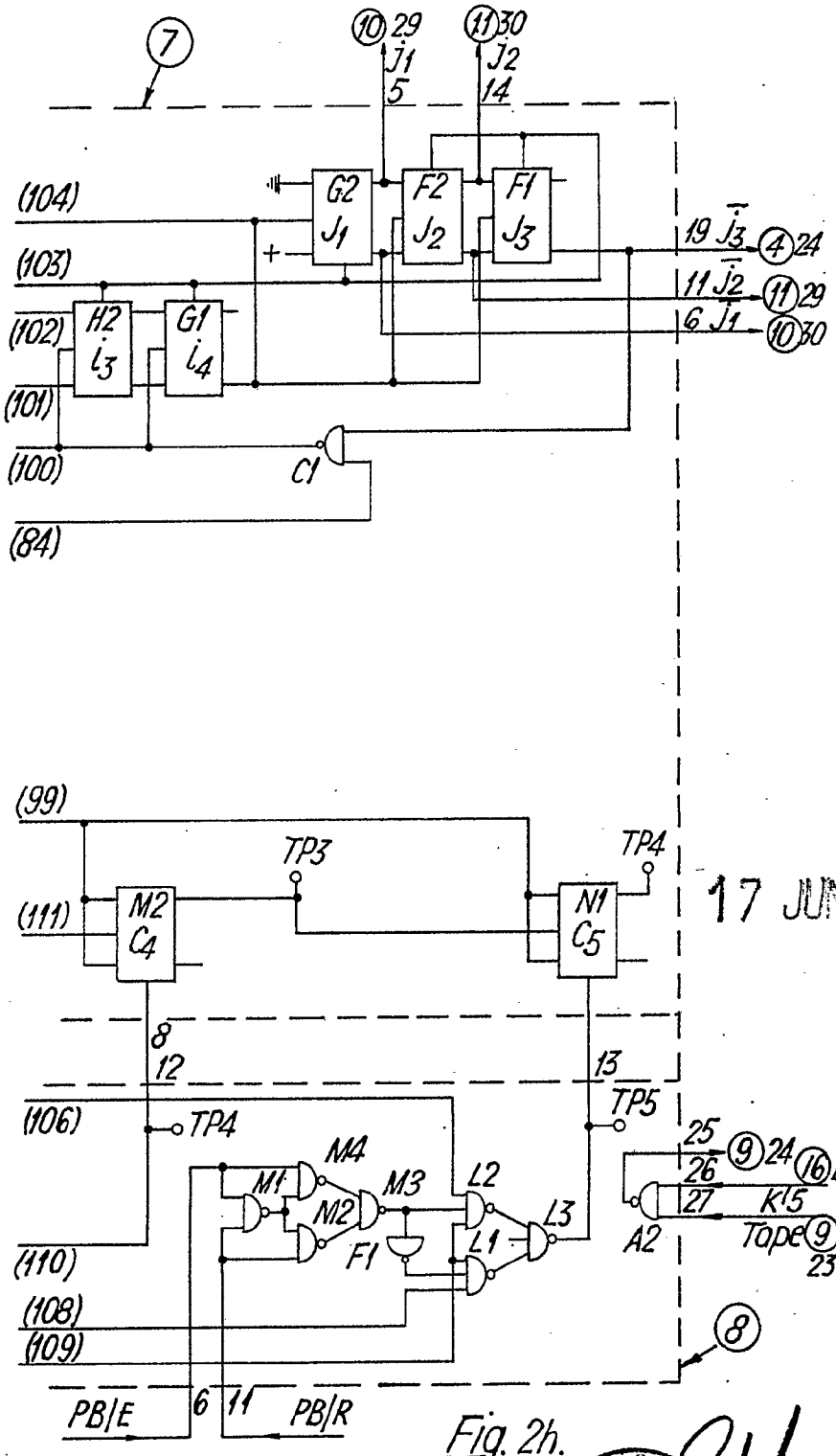
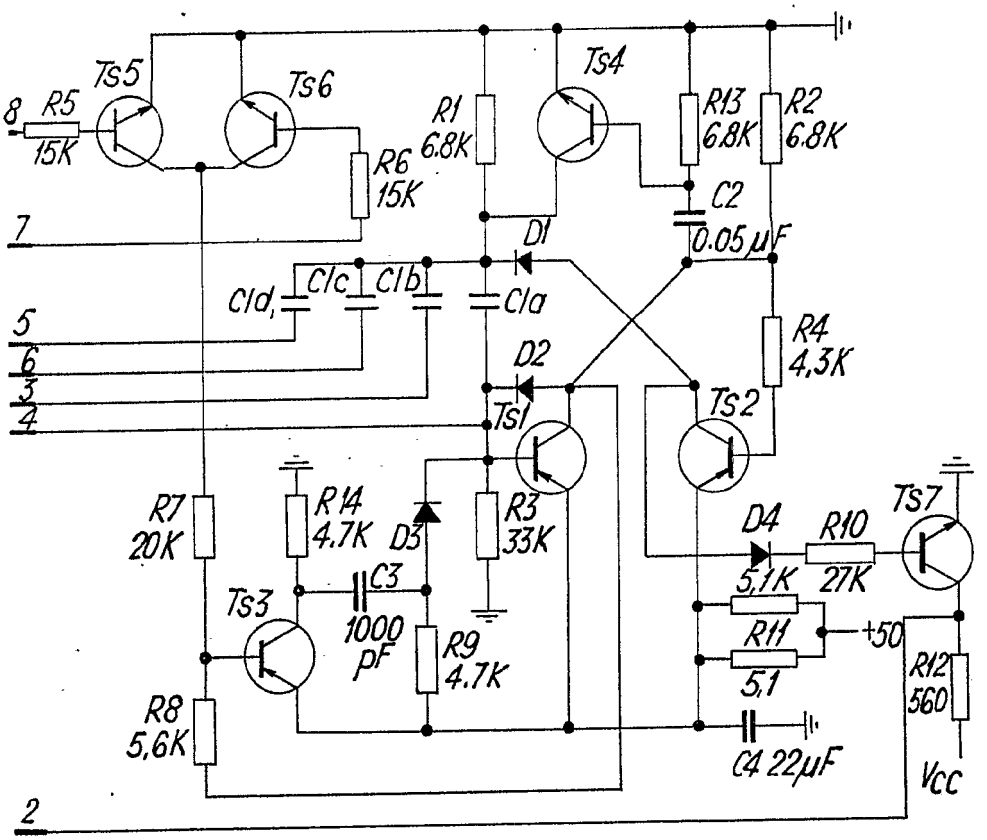


Fig. 2h.

17 JUN. 1967

EUGENIO BARROSO
Secretario General

341955



17 JUN. 57

O.S.

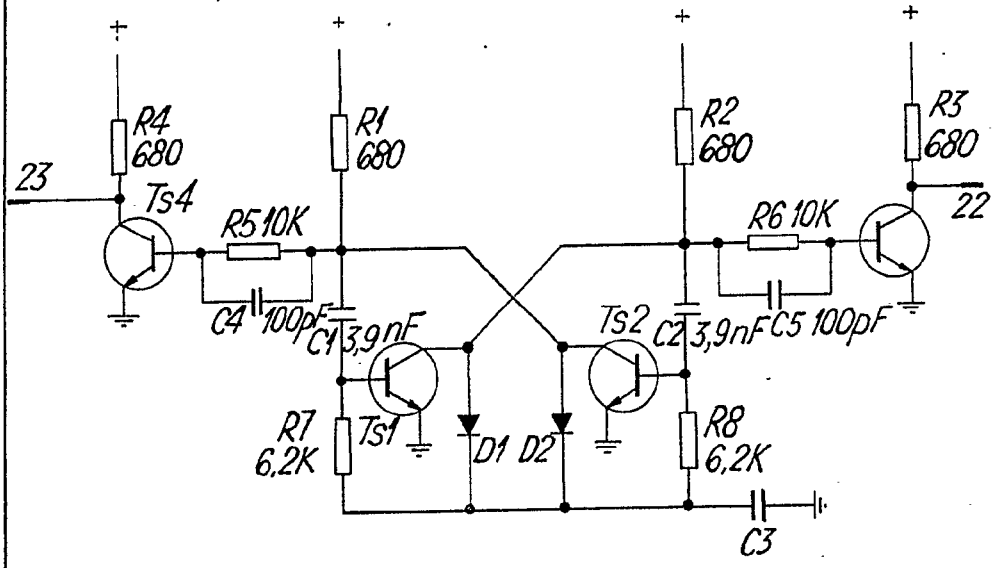
Fig.3.

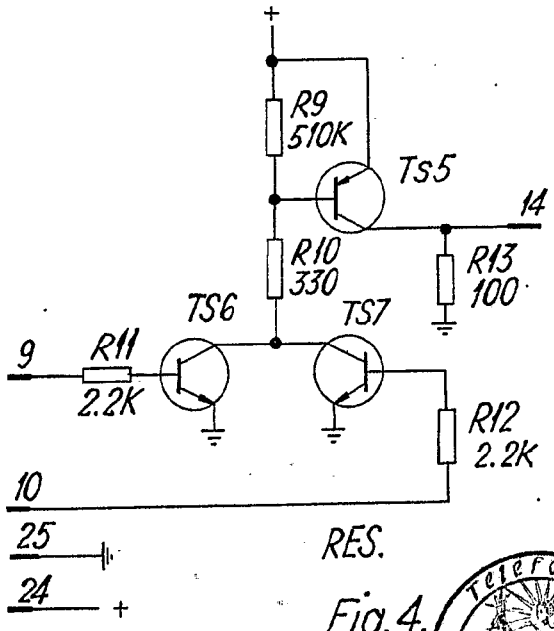
(6)

EUGENIO BARROSO
Secretario General

STANDARD ELECTRICA, S. A.

341955





17 JUN. 1967

Fig. 4.

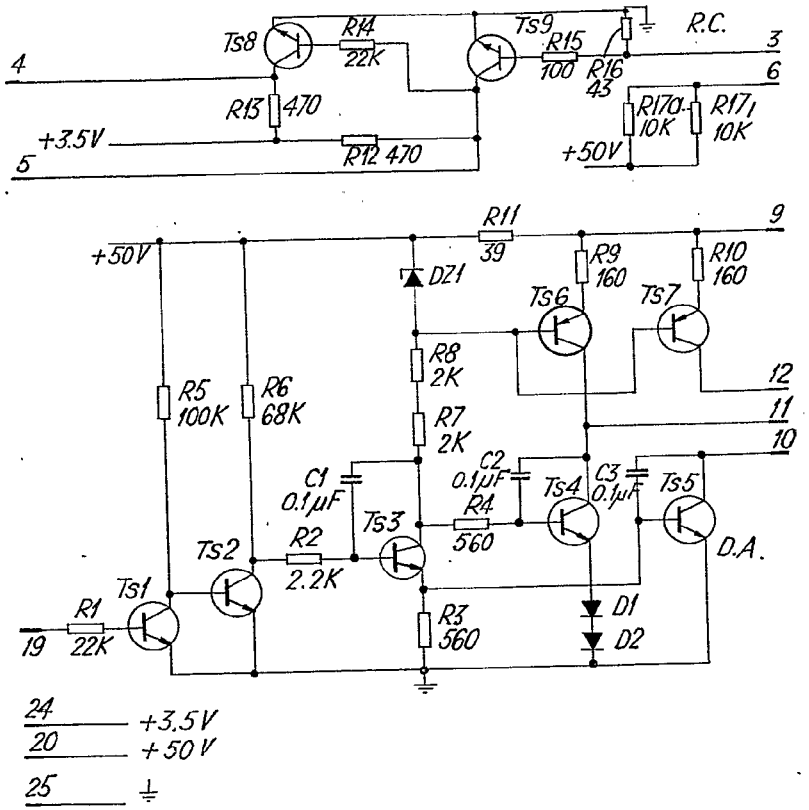
⑤

Teléfonos Standard cables

EUGENIO BARROSO
Secretario General

341955

341955



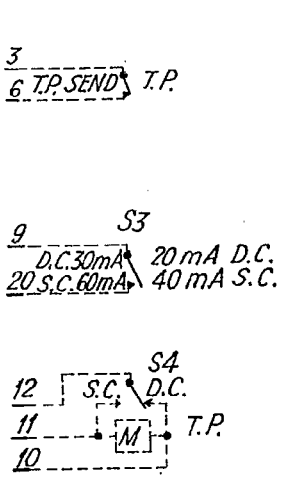


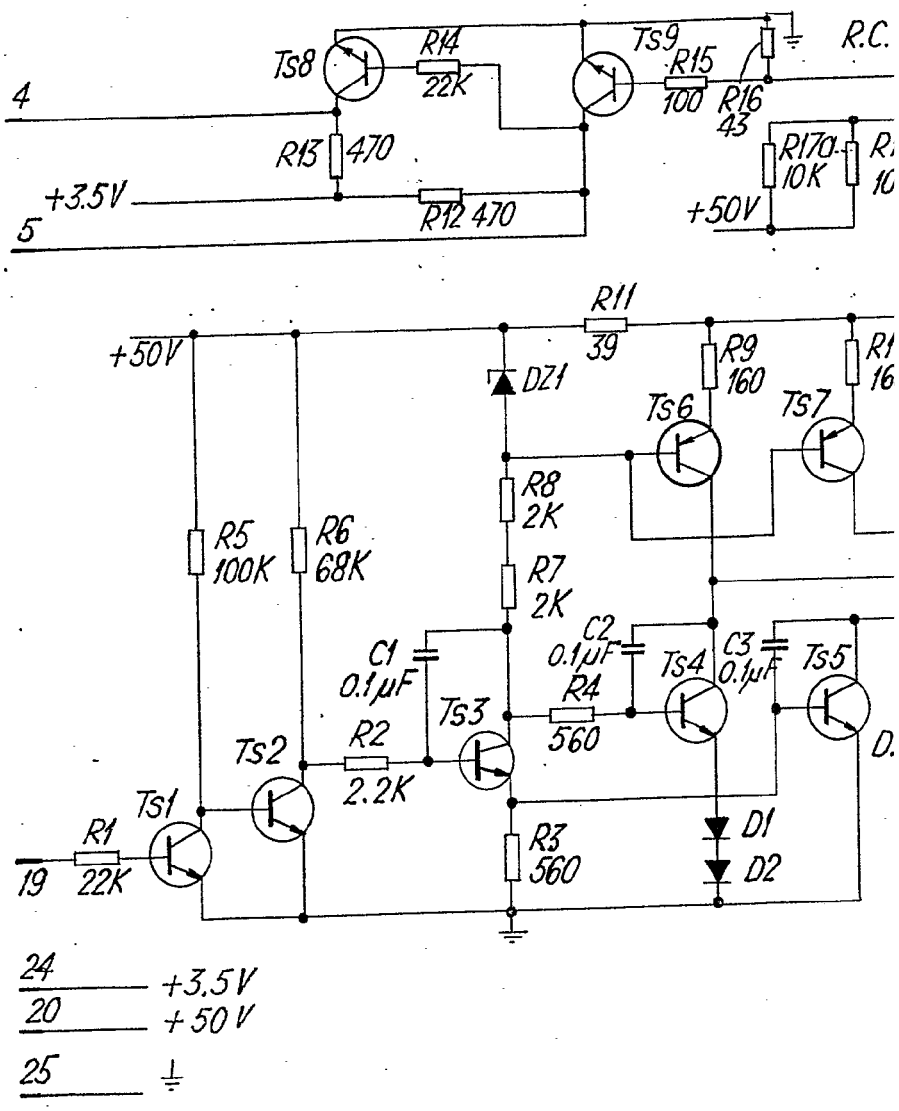
Fig. 5.

(14)

17 JUN 1967

EUGENIO BARROSO
Secretario General

341955


4
5
+3.5V
Ts8
R14
22K
R13
470
R12 470
Ts9
R15
100
R16
43
R.C.
R17a
10K
+50V
R11
39
+50V
DZ1
R9
160
Ts6
Ts7
R8
2K
R7
2K
R5
100K
R6
68K
C1
0.1µF
C2
0.1µF
C3
0.1µF
Ts4
Ts5
R4
560
Ts3
R2
2.2K
Ts2
Ts1
R1
22K
19
R3
560
D1
D2
24
+3.5V
20
+50V
25

341955

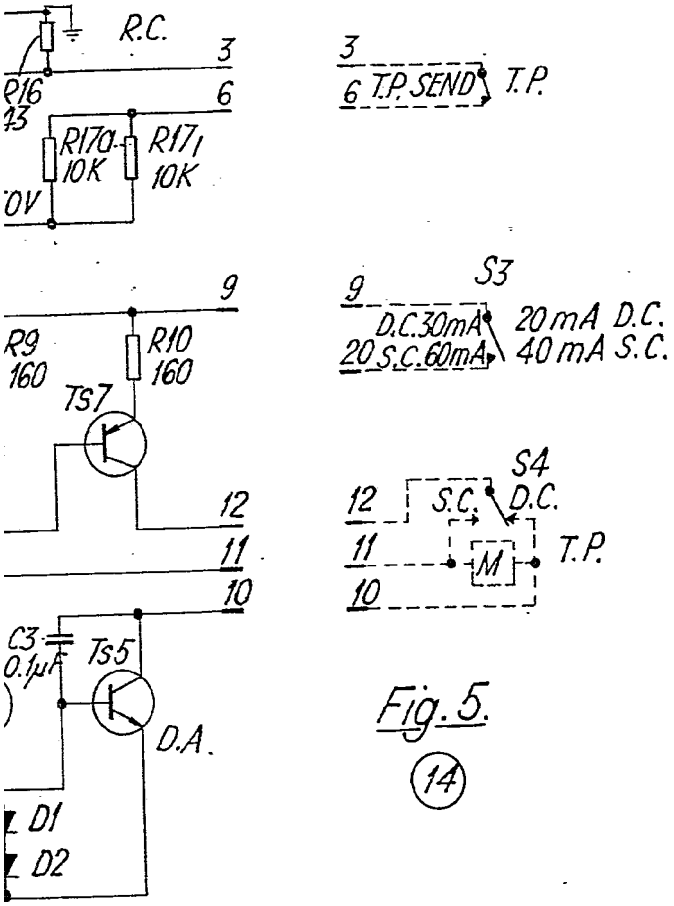


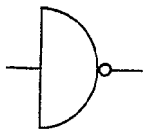
Fig. 5.

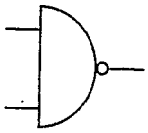
(14)

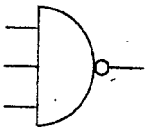
17 JUN. 1967

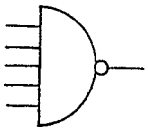
EUGENIO BARROSO
Secretario General

341955

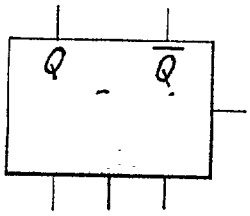


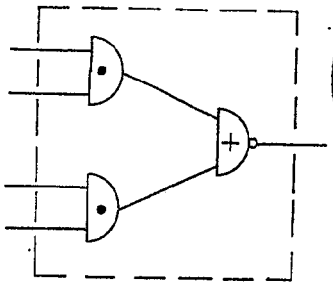






17 JUN 1967





EUGENIO BARROSO
Secretario General

Fig. 6.

21/21

STANDARD ELECTRICA, S. A.

341955

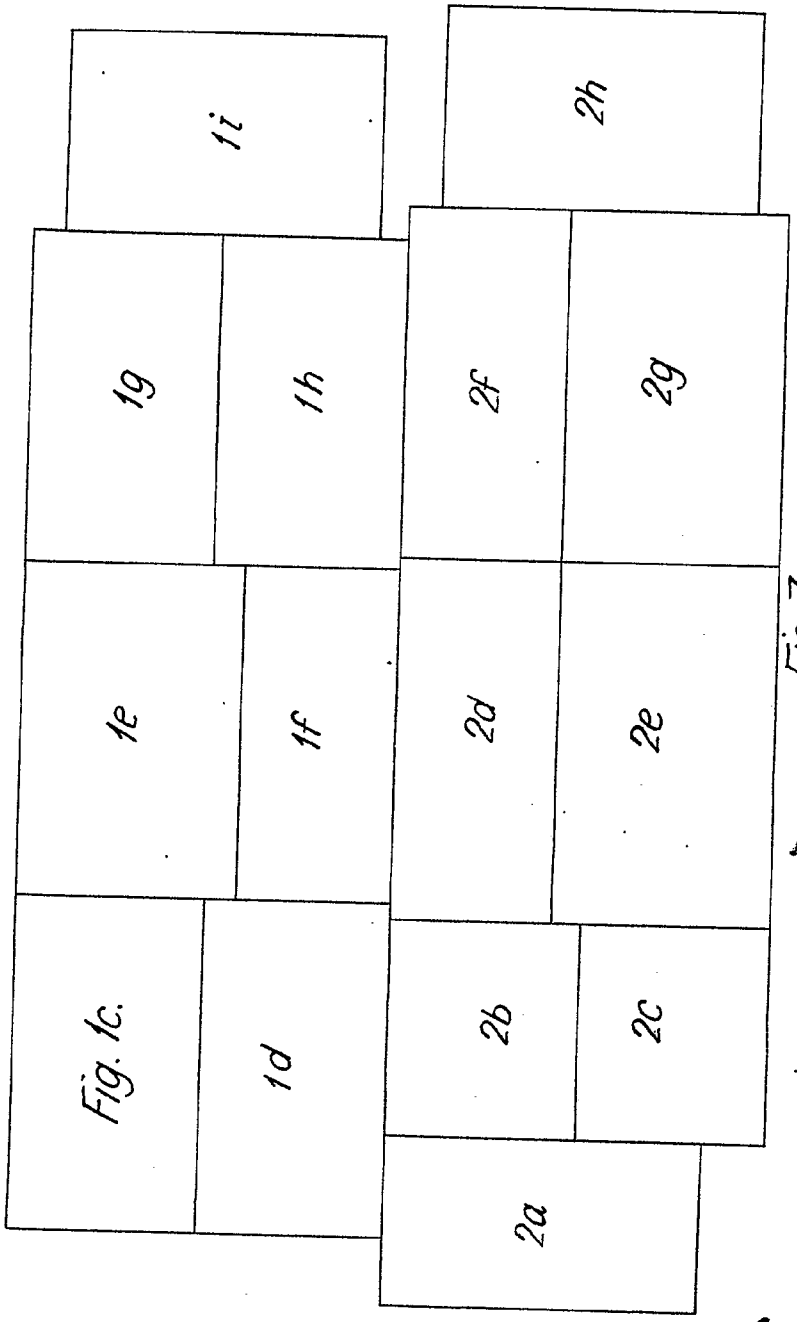


Fig. 1

17 JUN. 1957

Teléfonos Standard Cable

EUGENIO D[illegible]
Secretario General

341955

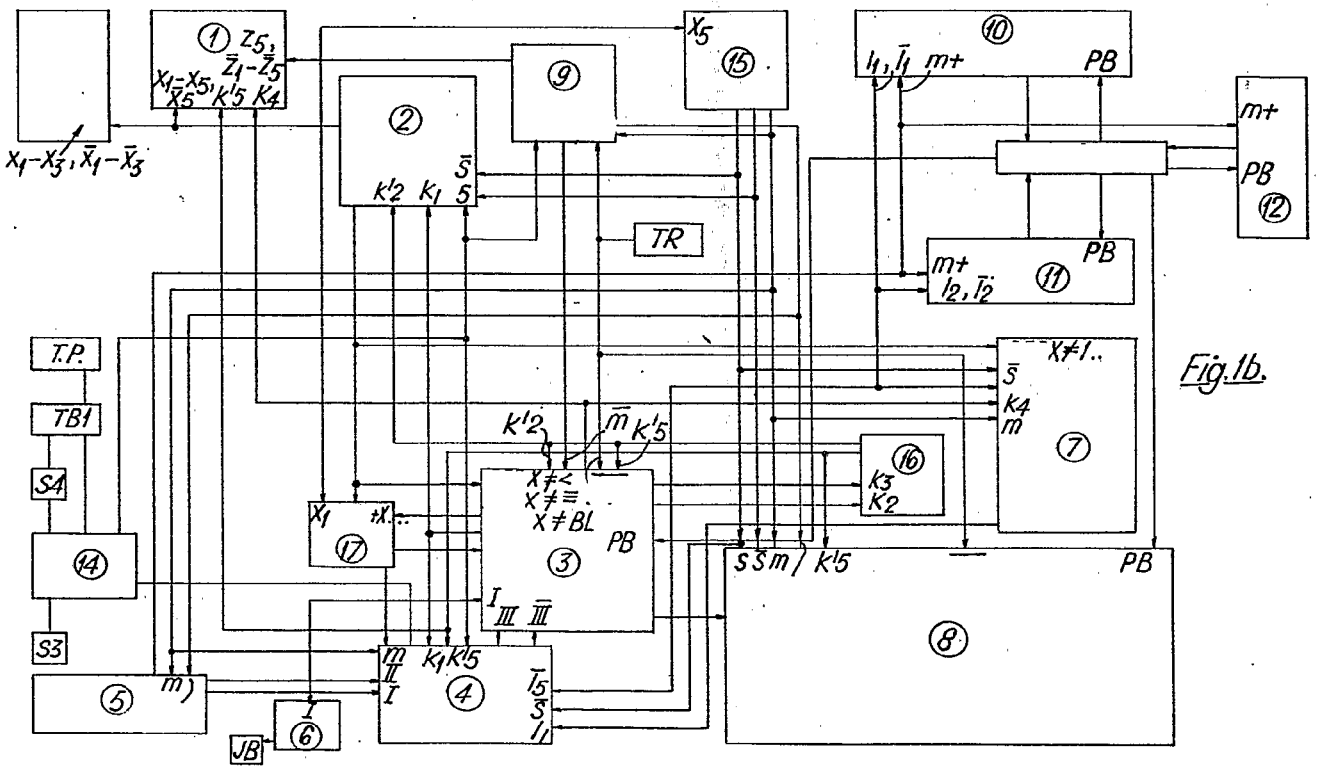
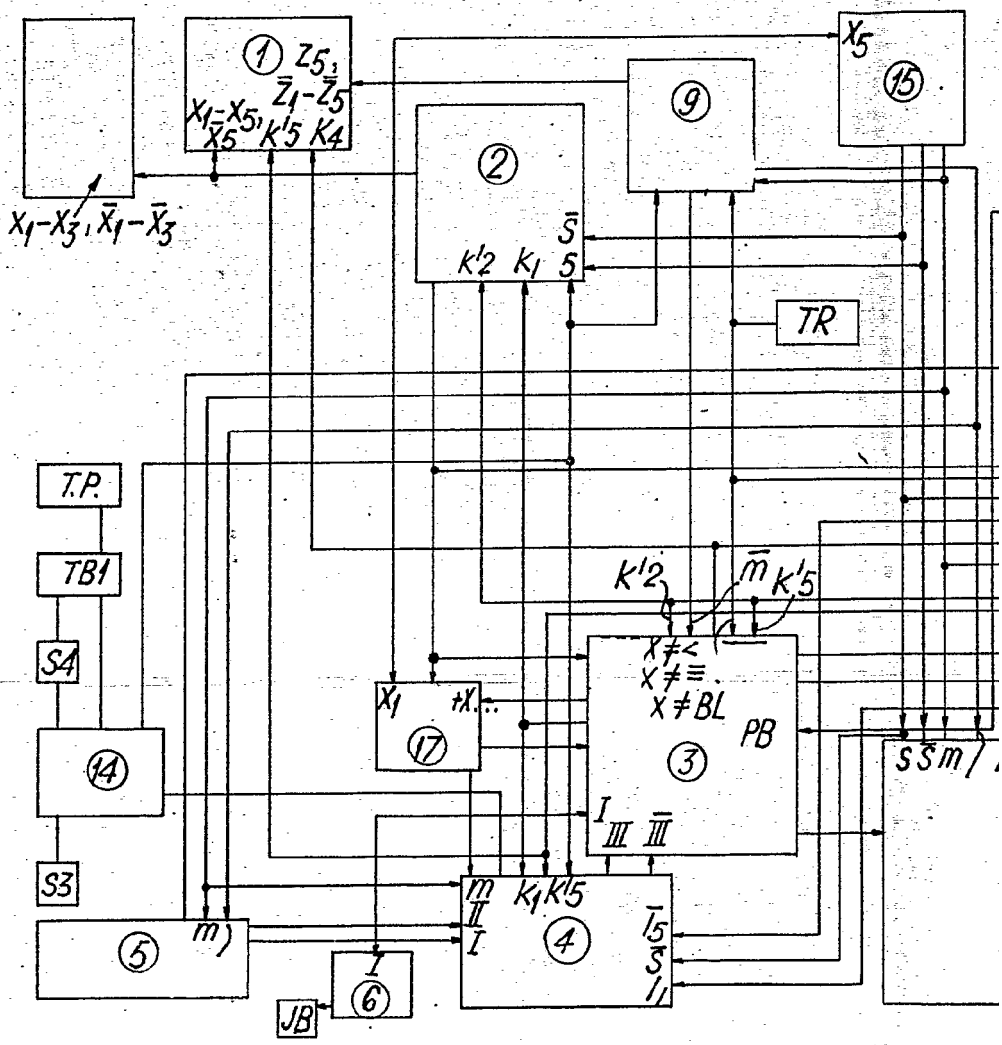


Fig.1b.

7 SEP. 1967

M. G. SANTAMARIA
VICE-SECRETARIO GENERAL

341955


1
Z_5
$\bar{Z}_1-\bar{Z}_5$
X_1-X_5
$\bar{X}_5$
k'_5
K_4
X_1-X_3, $\bar{X}_1-\bar{X}_3$
2
$\bar{S}$
k'_2
k_1
5
9
X_5
15
TR
T.P.
TB1
S4
14
S3
5
m)
JB
6
I
$\bar{X}_1$
+X...
17
k'_2
$\bar{m}$
k'_5
X≠<
X≠≡
X≠BL
PB
3
I_{III} $\bar{III}$
m
II
I
k_1
k'_5
4
$\bar{I}_5$
$\bar{S}$
$\bar{I}_1$
S $\bar{S}$ m)

STANDARD ELECTRICA, S. A.

21/1bis

341955

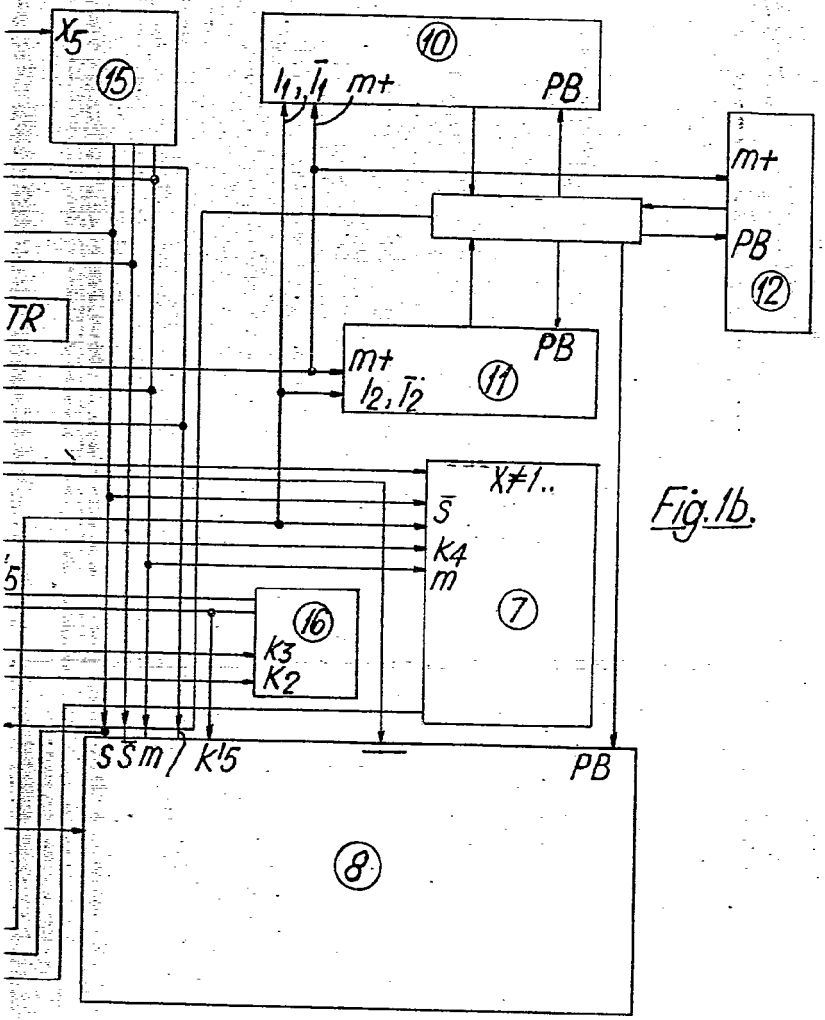


Fig. 1b.

7 SEP. 1967

M. G. SANTAMARIA
VICE-SECRETARIO GENERAL