15 JUN 1972

387293

SECCION TECNICA
CLASIFICACION I. P. C.
CLASE G 06
SUBCLASE F

MEMORIA DESCRIPTIVA PARA SOLICITAR PATENTE DE INVENCION EN ESPAÑA POR: "METODO DE CIFRADO DE TEXTOS ESCRITOS EN TELEIMPRESOR", A NOMBRE DE STANDARD ELECTRICA, S.A., CON DOMICILIO EN MADRID, CALLE DE RAMIREZ DE PRADO Nº 5.

Este invento se refiere a un método relacionado con el equipo de teleimpresor para cifrar y descifrar un texto normal, que, de acuerdo con los procedimientos, comprende a intervalos una combinación de dos caracteres de RETORNO DE CARRO y uno de CAMBIO DE RENGLON, en el que el texto claro se transfiere desde un teclado de teleimpresor, o desde un transmisor automático para cinta perforada, dispuesto en el extremo transmisor, en el que cada caracter de texto claro se procesa normalmente con un material clave tal que de la salida del equipo de cifrado se deriva un carácter de texto cifrado para cada carácter de texto claro, y en el que el texto cifrado se transfiere por medios convencionales a un equipo de descifrado en el extremo receptor en el que cada carácter de texto cifrado se procesa con un material de clave correspondiente

al material de clave utilizado por dicho carácter en el extremo transmisor para recuperar el texto claro del carácter original.

Cuando se utiliza un código aleatorio para cifrar mensajes de teleimpresor, la salida cifrada es también aleatoria, lo que quiere decir que hay sobreimpresiones en los teleimpresores de impresión en página a no ser que se tomen precauciones para evitarlo. Normalmente esto no es un inconveniente del sistema porque tales mensajes cifrados se transmiten normalmente por líneas fijas o circuitos alquilados, pero en algunas redes conmutadas con supervisión automática, la sobreimpresión puede ser reconocida como una condición no permisible y caracteres extra insertos, destruyendo así el sincronismo de la clave de cifrado. El presente invento se refiere a un método para evitar las sobreimpresiones en el extremo de las líneas de teleimpresor de teleimpresores de página.

Actualmente se utilizan ya cifradores de formato. Normalmente estos tratan los mensajes cifrados como grupos de palabras de cinco letras, dispuestos ordenadamente en líneas y versículos. El sistema necesita una lógica muy complicada para realizar su tarea, el texto cifrado será mucho más largo que el texto claro actual y es necesario que el sistema comprenda algún método para detener la lectura de texto normal mientras se insertan los caracteres extra.

El presente sistema tiene por objeto evitar la sobreimpresión al final de las líneas de teleimpresor. Esto se hace en una forma sencilla con una lógica muy simple, y el texto cifrado tiene exactamente la misma longitud que el mensaje en texto claro. De esta forma se evi-

ta también la parada del texto claro.

La característica principal del presente invento es que el primero de los tres caracteres de procedimiento (dos RETORNOS DE CARRO y un CAMBIO DE RENGLON) que se incluyen a intervalos en el texto claro en el extremo transmisor se detectan en un dispositivo detector que controla el equipo de cifrado en el extremo transmisor tal que dicho primer carácter se cifra de forma normal mientras que los dos caracteres de procedimiento siguientes no se cifran, con lo que el texto cifrado comprende a intervalos dos de los caracteres do procedimiento del texto normal.

Otra característica del invento consiste en que el primero de los tres caracteres de procedimiento, el cual carácter existe en el modo cifrado en el texto cifrado, se descifra en forma normal en el extremo receptor en el que se recupera en el texto claro y se detecta simultáneamente en un dispositivo detector que controla el equipo de descifrado del extremo receptor tal que los dos caracteres siguientes son tratados como caracteres de texto claro y por lo tanto aparecen junto con el primero de los tres caracteres de procedimiento.

El método utiliza la propiedad de que la mayoría de los mensajes de teleimpresor contienen el carácter CAMBIO DE RENGLON casi siempre precedido por el RETROCESO DE CARRO, e incluso en muchos casos con otro RETORNO DE CARRO también para cubrir el retardo del movimiento del carro. En el sistema elegido, el operador que escribe el mensaje en texto claro tendrá que imprimir RETORNO DE CARRO, RETORNO DE CARRO, CAMBIO DE RENGLON, siem

pre que haya una nueva línea en el telegrama. Durante la operación de cifrado, el primer RETORNO DE CARRO se cifra como normal pero también es detectado en tal forma que deja que los dos caracteres siguientes pasen en el texto claro. Durante el descifrado, el primer RETORNO DE CARRO es considerado como normal, y la detección produce de nuevo que pasen los dos caracteres siguientes de texto claro. La señal cifrada puede ser recibida por lo tanto por un impresor de página normal sin producir sobreimpresión al final de las líneas impresas.

Las antes mencionadas y otras características y objetos del invento quedarán claras como consecuencia de la siguiente descripción detallada de una realización del invento, dada junto con los dibujos que se acompañan en los que:

Las figuras 1 y 2 muestran un esquemático de bloque de los extremos transmisor y receptor respectivamente;

Las figuras 3 y 4 muestran los símbolos lógicos utilizados en el diagrama detallado;

La figura 5 muestra las formas de onda de control que aparecen en el diagrama detallado y la figura 6 muestra la lógica detallada del sistema de un circuito utilizado de ambos extremos, transmisor y receptor.

En la figura 1 se ha representado un esquemático de bloques del extremo o transmisor en el que aparece la señal de texto claro en la salida de un bloque 1 que representa un teclado de teleimpresor o un transmisor automático. La señal de texto claro se aplica a un circuito de cifrado 2 en el que es procesada con un material de clave

de acuerdo con una regla predeterminada. El texto claro se aplica también a un circuito detector 3 para detectar el carácter de procedimiento RETORNO DE CARRO. Al detectar un RETORNO DE CARRO, el circuito detector 3 controla el circuito de cifrado 2 de forma que los dos caracteres siguientes, que de acuerdo con los procedimientos normales deben ser un segundo RETORNO DE CARRO y un carácter de CAMBIO DE RENGLON, no son tratados con material de clave. Los dos caracteres finalmente mencionados son pasados por lo tanto a través del circuito de cifrado 2 en el texto claro. La señal que sale del circuito de cifrado 2 puede ser, en el caso de trabajar fuera de línea, llevada a un dispositivo de escritura o de perforación 4 para producir una cinta perforada 5, o en el caso de funcionamiento en línea (no representado), ser transmitida directamente a través de una línea de transmisión no representada al extremo receptor.

En la figura 2 se ha representado un esquemático de bloques del extremo receptor en el que se recibe y se descifra una señal cifrada. En el caso de equipo fuera de línea, la señal cifrada se recibe en un dispositivo de impresión o de perforación normal (no representado) en el que se produce una cinta perforada 6 que contiene el mensaje cifrado. La cinta perforada 6 se lee en un circuito de lectura 7, cuya salida está aplicada a un equipo de descifrado 8. En el caso de recepción en línea (no representado), la señal cifrada recibida en la línea se aplica directamente a un equipo de descifrado 8.

En el equipo de descifrado 8, la señal cifrada se procesa con un material de clave idéntico al utilizado

387293

en el extremo transmisor tal que permita recuperar el texto original claro. Cuando hay un carácter de RETORNO DE CARRO en la salida del bloque 8, este carácter es detectado por un circuito detector 9 que controla el equipo de descifrado 8 de tal forma que los dos carácteres siguientes no son procesados con material de clave. Estos dos caracteres siguientes son, como se ha mencionado previamente, los dos últimos de los tres caracteres de procedimiento. La señal que aparece así en la salida del equipo de descifrado 8 es idéntica a la señal de texto claro original y está aplicada a un teleimpresor de recepción 10.

Ahora es obvio que la señal de cifrado que aparece en el canal de transmisión puede ser supervisada e impresa en un teleimpresor de página sin sobreimpresión al final de una línea, puesto que el segundo caracter de retorno de carro y el cambio de renglón se dejan en texto claro en la señal cifrada.

Los circuitos lógicos utilizados en el diagrama de bloques detallado se han representado en las figuras 3 y 4. La figura 3 muestra un circuito NAND normal para lógica positiva. La lógica "0" en una o ambas entradas se convierte en un "1" en la salida, mientras que la lógica "1" de ambas entradas produce un "0" en la salida como se ha representado en la tabla de combinaciones. La figura 4 muestra un flip-flop maestro arrastrado JK, cuyo funcionamiento se ha representado en la tabla. J y K son las entradas de señal normal y C la entrada de reloj mientras que R es una entrada de reposición. Q y $\overline{Q}$ son las salidas "verdadera" y "falsa". Una lógica "0" en la entrada de reposición R anula a todas las otras señales de entrada y mantie-

ne el flip-flop en el estado "0" ($Q = 0$, $\overline{Q} = 1$).

La figura 6 muestra un diagrama de bloques detallado do una realización del invento on la quo se utiliza el método fuera de línea. Un generador de clave 11, un teleimpresor 12 con una unidad de lectura 13 y una unidad de escritura 14, y un generador de control de formas de onda 15 se han representado como bloques porque sus detalles no son esenciales para compnender el presente invento. Las formas de onda de control necesarias C1-C4 se han representado en la figura 5.

La figura 6 muestra el equipo que tiene que utilizarse en el extremo transmisor y en el extremo receptor debiendo trazarse mediante la figura 6 la circulación de señal simpre representada en las figuras 1 y 2.

En el cifrado, el texto claro se escribe en un teleimpresor normal 12, o cuando el texto claro aparece como una cinta perforada, se lee mediante la unidad de lectura 13. Los caracteres de texto claro que ahora aparecen en forma serie (impulso de arranque - cinco bits de información - impulso de parada) se pasan directamente a través de una puerta no activa de descifrado 16 y un registrador de cambio 17 a una puerta de cifrado 18 en la que es tratado con material de clave suministrado por el generador de clave 11. Un carácter de RETORNO DE CARRO que aparece en el texto claro es detectado por una puerta 19 la cual a través de un contador 20 controla la puerta de cifrado 18 a través de una puerta 21 para prevenir el cifrado de los dos caracteres siguientes. La señal cifrada que sale por la puerta de cifrado 18 se transfiere a través de puertas 22 y 23 a la unidad de escritura y/o perforación 14 en este circuito

fuera de línea representado.

Al descifrar en el circuito fuera de línea representado, una cinta perforada cifrada es leída por la unidad de lectura 13 y se pasa directamente a la puerta de descifrado 16 en la que es tratado con material de clave suministrado por el generador de clave 11. La señal de salida de la puerta de descifrado 16 es alimentada a través del registrador de cambio 17 a través de una puerta de cifrado no activa 18 y las puertas 22 y 23 al circuito de escritura 14 del teleimpresor 12. Sin embargo, la señal descifrada que deja la puerta de cifrado 16 es supervisada por la puerta de detector 19 para la detección de un carácter de RETORNO DE CARRO. En cuanto se ha detectado este carácter, el contador 20 a través de la puerta 24 controla la puerta de descifrado 16 para dejar los dos caracteres siguientes sin ser tratados por el material de clave.

Por medio de la forma de onda del reloj C2, el generador de clave 11 es capaz de suministrar caracteres de clave aleatorios en los mismos momentos en que el teleimpresor presenta los cinco bits de información.

La unidad de lectura del teleimpresor 13 transforma las "Marcas" del teleimpresor en "unos" lógicos y los "Espacios" en ceros lógicos. El impulso de arranque de un caracter de teleimpresor se transmite a través de la unidad de lectura 13 al circuito de control 15 e inicia la generación de formas de onda de control C1-C4. La línea superior de la figura 5 muestra la ocurrencia de los impulsos de ARRANQUE y de PARADA y los bits de información de caracteres de teleimpresor, todos ellos referidos al contacto de emisión del teleimpresor. Cuando la forma de onda C1

es en lógica "0", la salida de la puerta 23 sigue en lógica "1", manteniendo así a la unidad de escritura del teleimpresor 14 en condición de Marca durante el impulso de PARADA, que es un bit retardado con relación a la señal del contacto de emisor. La forma de onda C2 temporiza los bits de información del teleimpresor al registrador de cambio 17 (X1-X6) en la figura 5 en tiempos a, b, c, d y e tales que en el tiempo "e", los cinco bits de información están presentes de Xo a X5. La forma de onda C3 es una señal de control que es lógica "1" cuando los cinco bits de información del primer caracter tienen que leerse de la etapa X6 del registrador de cambio. La forma de onda C4 es un solo impulso de detección que está presente cuando el contenido de información de un carácter de teleimpresor aparece en las etapas X1 - X5 del registrador de cambio.

Volviendo a la figura 6, el funcionamiento del circuito es el siguiente:

Un conmutador de tres posiciones 25 controla si el equipo va a cifrar o a descifrar un mensaje. En la posición 1, la señal EMISION es lógica "1" y se hace el cifrado. En la posición 2, la variable CLARO es lógica "1", y el relé del teleimpresor simplemente repite las señales del contacto de emisión. En la posición 3, la señal REC es lógica "1" y se hace el descifrado.

Supongamos que EMISION = "1". Cuando se pulsa una tecla del teclado del teleimpresor, se lee el caracter correspondiente en X1 - X5. Al mismo tiempo se extrae el primer caracter de X6 a través de las puertas 18, 22 y 23. Si la variable $\overline{Y2}$ es lógica "1", se transfiere un caracter de clave a la puerta 18 a través de la puerta 21. Este es el

funcionamiento normal y significa que el caracter de texto claro y el caracter de clave tienen añadido el módulo 2 bit a bit en la puerta 18, esto es el proceso normal de cifrado. Si es detectado un RETORNO DE CARRO en $X_1 - X_5$ como texto claro, el contador 20 (Y1Y2) empieza a contar, porque la entrada J a Y1 se hace alta a través de la puerta de detector 19. La secuencia de recuento es 00 - 10 - 11 - 01 - 00 normalmente ó 00 - 10 - 11 - 11 - 10 si el tercer caracter despues del primer RETORNO DE CARRO es otro RETORNO DE CARRO. Esto significa que $\overline{Y2}$ es lógica cero durante dos caracteres con lo que el cifrado no se hace durante estos dos caracteres. Depende del operador hacer uso de esta característica en un procedimiento de formato pulsando justamente los botones RETORNO DE CARRO, RETORNO DE CARRO, CAMBIO DE RENGLON, con lo que el primer RETORNO DE CARRO será cifrado normalmente mientras que los otros dos caracteres se escribirán en forma clara.

Supongamos que REC = "1". El objeto es ahora descifrar un mensaje, presentado normalmente al sistema como una cinta perforada, que tiene que ser leída por la unidad de lectura del teleimpresor 13. En el modo de recepción, el descifrado se hace en la puerta 16 antes de que el carácter entre en el registrador de cambio 17. El caracter de clave es presentado a la puerta 16 a través de la puerta 24 cuando la variable $\overline{Y1}$ es lógica "1". La detección de un RETORNO DE CARRO en $X_1 - X_5$ se hace como antes y la secuencia de recuento en Y1Y2 es exactamente la misma. Esto significa que los dos caracteres siguientes después de un RETORNO DE CARRO son tratados como caractores de texto claro porque la variable $\overline{Y1}$ es lógica cero para estos caracteres.

Debe señalarse que el equipo está diseñado de tal forma que los dos caracteres cualesquiera siguientes que aparezcan después de un RETORNO DE CARRO en el mensaje en texto claro se dejarán en texto claro en el texto cifrado. Esto significa que si el operador acciona inintencionadamente la tecla de RETORNO DE CARRO, los dos caracteres siguientes no se cifrarán. La seguridad no está disminuida por esta característica, porque una tercera parte que intervenga en la línea no tiene medios para detectar donde están presentes los dos caracteres en texto claro.

Este invento corresponde a una solicitud de patente formulada en Noruega el 16 de enero de 1970, señalada con el número 151/70 y se acoge por lo tanto a los beneficios que otorgan los convenios 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 método de cifrado de textos escritos en teleimpresor, para cifrar y descifrar un texto claro que de acuerdo con los procedimientos, comprende a intervalos una combinación de dos RETORNO DE CARRO y un CAMBIO DE RENGLON, en el que el texto claro se transfiere desde un teclado de teleimpresor o un transmisor automático para cinta perforada, dispuestos en el extremo transmisor, al equipo de cifrado del extremo transmisor en el que cada caracter de texto claro es procesado normalmente con un material de clave tal que se deriva de la salida del equipo de cifrado un caracter de texto cifrado para cada caracter de texto claro y en el que el texto cifrado se transfiere por proce-

dimientos convencionales al equipo de descifrado en el extremo receptor, en el que cada caracter de texto cifrado es procesado con un material de clave que corresponde al material de clave utilizado por dicho caracter en el extremo transmisor para recuperar el texto claro original, caracterizado en éste porque el primero de los tres caracteres de procedimiento (dos RETORNOS DE CARRO y un CAMBIO DE RENGLON) que están incluídos a intervalos en el texto claro del extremo detector se detectan en un dispositivo de detección (19) que controla el equipo de cifrado (18) del extremo transmisor de tal forma que el primero de dichos tres caracteres se cifra de una forma normal mientras que los dos caracteres siguientes de los tres caracteres de procedimiento no se cifran, con lo que el texto cifrado comprende a intervalos dos de los caracteres de procedimiento en texto claro.

2. Un método de cifrado para descifrar un texto claro cifrado de acuerdo con el método del punto 1 caracterizado en éste porque el primero de los tres caracteres de procedimiento, caracter que existe en el modo cifrado del texto cifrado, se descifra en la forma normal en el extremo receptor en el que se recupera como texto claro y simultáneamente se detecta en el dispositivo de detección (19) que controla el equipo de descifrado (18) en el extremo receptor de tal forma que los dos caracteres siguientes son tratados como caracteres de texto claro y con lo que aparecen juntos con el primero de los tres caracteres de procedimiento.

3. Un método de cifrado como el de los puntos 1 y 2 caracterizado porque el dispositivo de detección (19) del extremo transmisor (receptor) está asociado con un dispositivo de recuento (20) conectado de forma que de una

387293

señal de control a una puerta de control de cifrado (21) (puerta de control de descifrado (24) con lo que se detiene el proceso de cifrado (descifrado) para los dos caracteres que siguen a un caracter de RETORNO DE CARRO.

4. Un método de cifrado como el del punto 3 caracterizado en éste porque se utilizan equipos idénticos en los extremos transmisor y receptor, teniendo el equipo un conmutador (25) que tiene tres posiciones (EMISION, CLARO Y RECEPCION) por medio del cual, la puerta de control de cifrado (21) se permite, se bloquea el contador (20) y se permite la puerta de control de descifrado (24), respectivamente.

5. Un método de cifrado de textos escritos en teleimpresor.

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

Esta memoria consta de trece hojas escritas por una sola cara.

Madrid, 15 JUN. 1973

M. G. SANTAMARIA
VICE-SECRETARIO GENERAL

387293

STANDARD ELECTRICA, S. A.

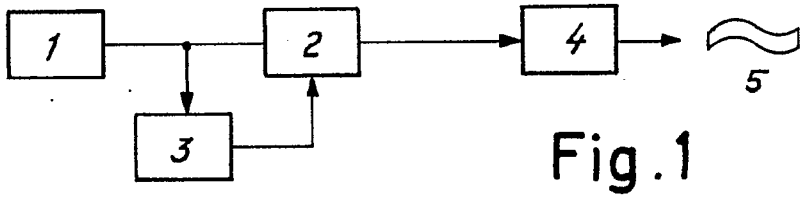


Fig. 1

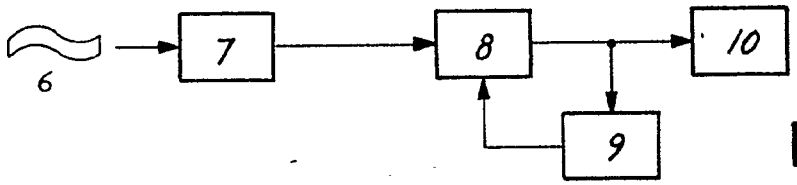
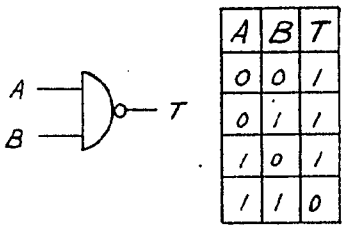


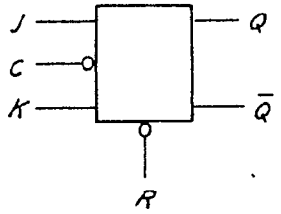
Fig. 2

15 ENE. 1971



A	B	T
0	0	1
0	1	1
1	0	1
1	1	0

Fig. 3



J^t	K^t	R^t	Q^{t+1}
0	0	0	0
0	1	0	0
1	0	0	0
1	1	0	0
0	0	1	Q^t
0	1	1	0
1	0	1	1
1	1	1	$\bar{Q}^t$

Fig. 4

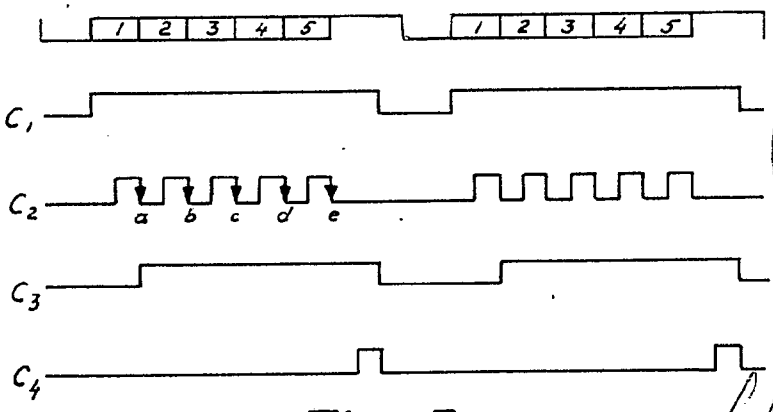


Fig. 5

EUGENIO BARROSO
Secretario General

387293

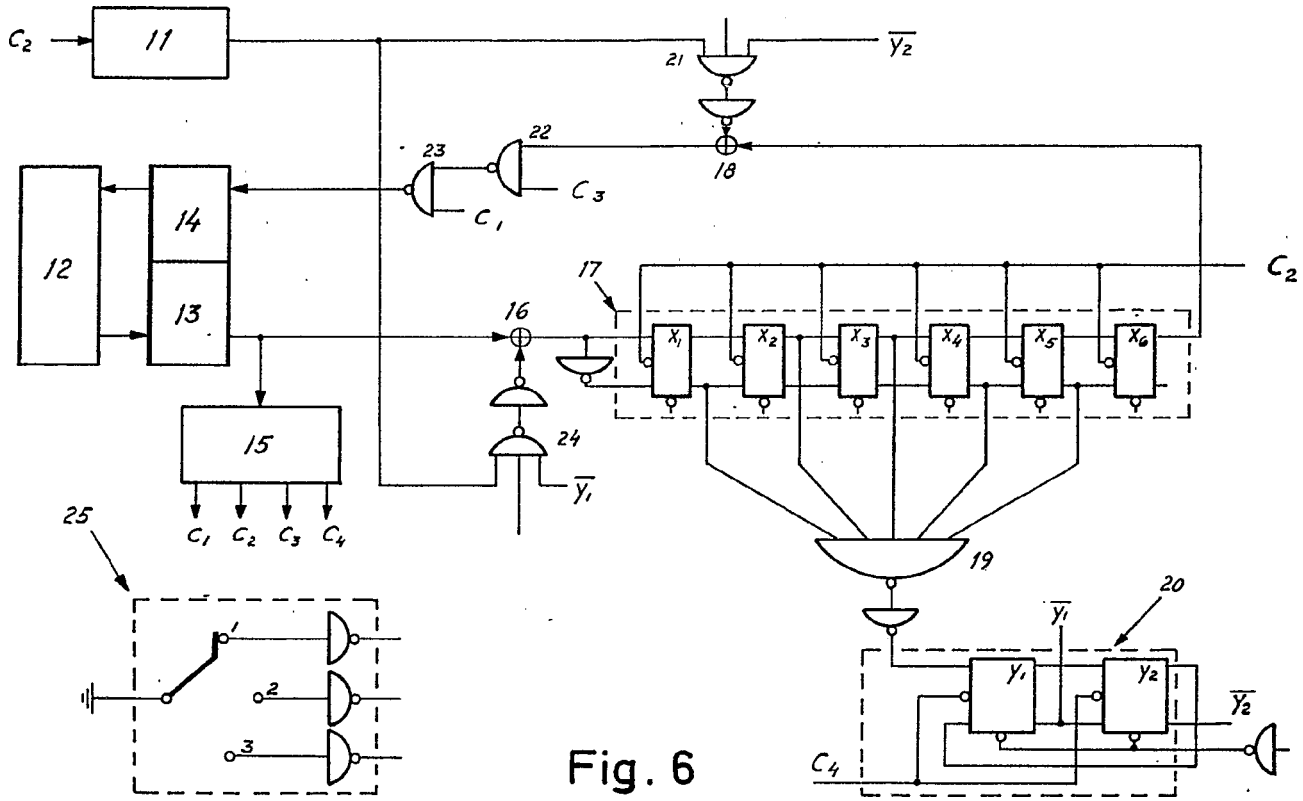


Fig. 6

15 ENE. 1971

EUGENIO BARROSO
Secretario General

387293

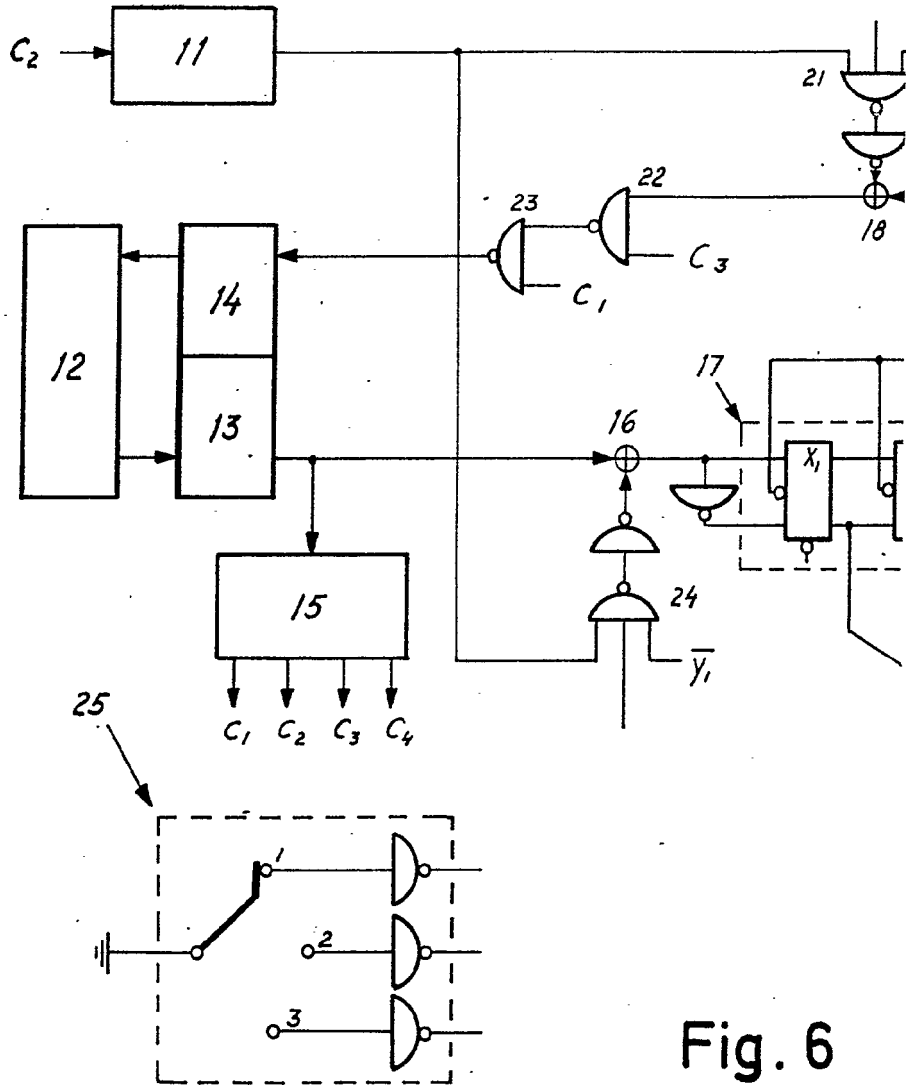
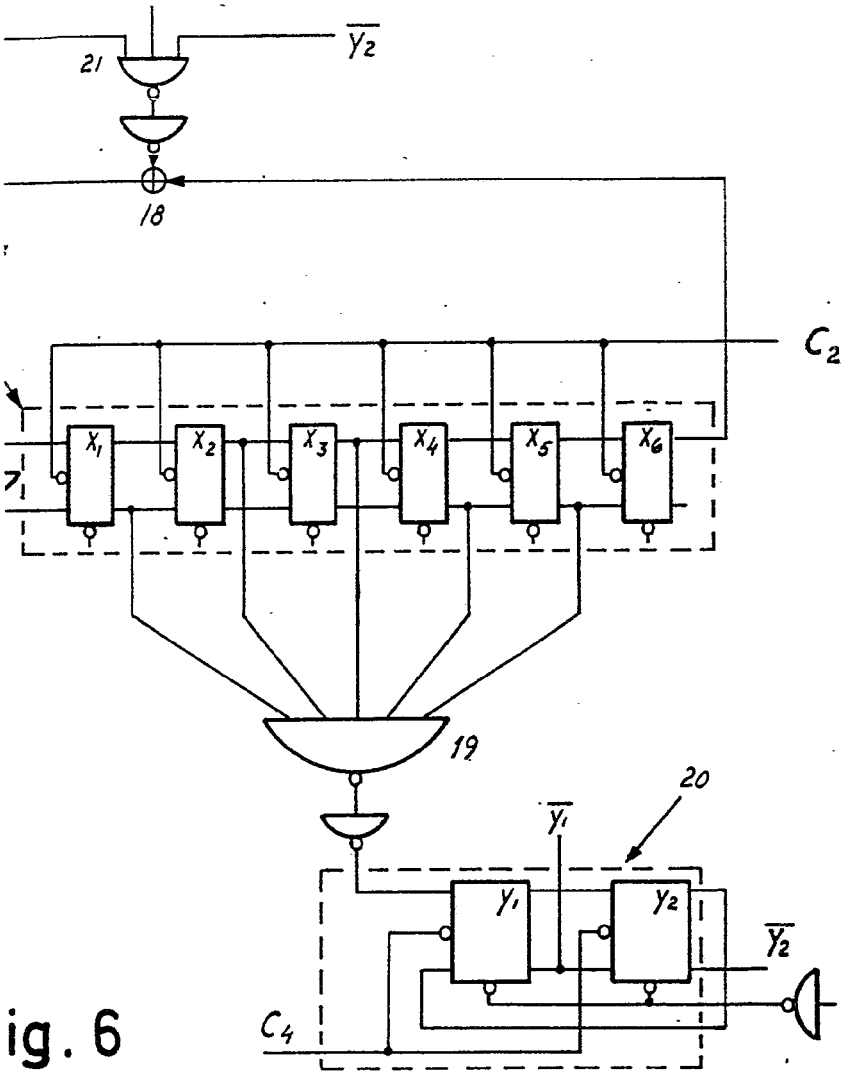

C2
11
21
22
23
18
C3
C1
14
12
13
17
16
X1
15
24
$\overline{y_1}$
C1 C2 C3 C4
25
1
2
3

Fig. 6

STANDARD ELECTRICA, S. A.

387293



ig. 6

15 ENE. 1971

EUGENIO BARROSO
Secretario General