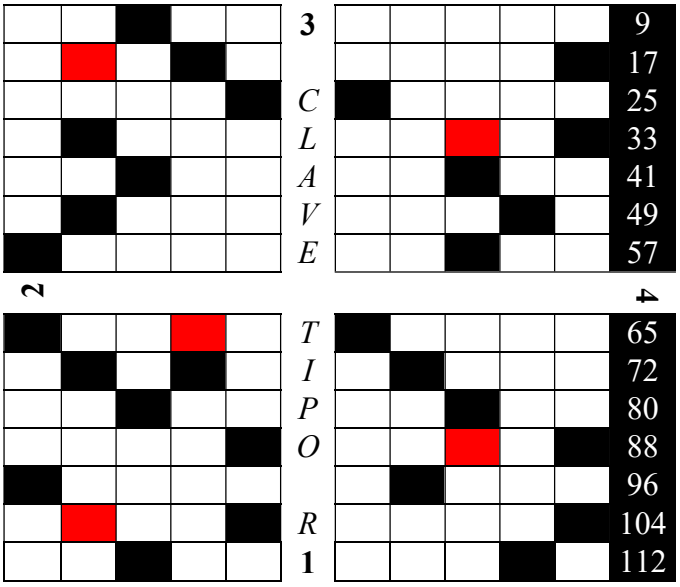
CIFRADOR R

No sabemos exactamente la fecha en que se usó, y aunque en un texto anterior lo databa en 1937 por error ya que coincidía el nombre con otra clave, hoy en día por lo que suponemos es de los años 40. La forma de cifrar con este cifrador es el típico de un cifrado de trasposición con nulos. Para cifrar ambos comunicantes deben disponer de unas hojas donde están dibujadas cuatro rejillas por cada cara, con lo que hay ocho maneras diferentes de escoger la rejilla inicial. El orden de la rejilla queda definido por un número que aparece en la parte superior una vez seleccionado el orden de la rejilla.



Una vez escogido el orden de colocación de la rejilla se comienza a escribir el mensaje de izquierda a derecha, en todas las rejillas, teniendo en cuenta que el número de letras debe ser un múltiplo de cinco. El número que aparece a la derecha de la tabla indica el número de celdas que hubiésemos rellenado en el caso de que el mensaje ocupase hasta el final de la línea. Por ejemplo, si hubiésemos rellenado hasta el final de la cuarta línea, nuestro mensaje tendría 33 caracteres, con lo que nos harían falta dos nulos para tener un mensaje con un número de letras múltiplo de cinco. La escritura del mensaje sigue unas reglas sencillas:

1) El número de letras inscritas ha de ser siempre un múltiplo de cinco.
2) El punto se representa por WW.
3) Los nombres extranjeros y las denominaciones geográficas van precedidas de XX, que también se colocarán al final. Por ejemplo para poner JUAN escribiríamos XXJUANXX.
4) Los números se obtienen de una tabla de equivalencias, denominada "*Criterio de equivalencias literales*", que convierte cada dígito en una letra. Para determinar que es un número vendrá precedido y terminado con ZZ.
5) Las casillas rojas son de control y en ellas se escribe el carácter que ocupa la posición anterior.

La tabla de equivalencias para los números está formada por dos filas, una con los números y dos más con sus equivalencias en letras. En el documento "*Instrucciones Generales para el uso de las claves tipo R*" nos aparece la siguiente tabla de equivalencias:

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
C	F	E	A	G	J	H	B	I	D
K	M	N	Q	R	O	S	P	T	L

Por ejemplo, si queremos cifrar el mensaje “ENVIAR A IBIZA 250 FUSILES. FUERZAS ENEMIGAS FUERTEMENTE ARMADAS.” Primeramente tendríamos que escribir el mensaje siguiendo las reglas anteriores, con lo que el mensaje quedaría convertido en “ENVIAR A XXIBIZAXX ZZEOCZZ FUSILESWW FUERZAS ENEMIGAS FUERTEMENTE ARMADASWW”.

Una vez acabada la transformación del mensaje, ponemos el mensaje en la rejilla escogiendo la posición 3, la misma que aparece en el gráfico anterior.

E	N	■	V	I	**3**	A	R	A	X	X	9
I	I	B	■	I		Z	A	X	X	■	17
Z	Z	E	O	■	*C*	■	C	Z	Z	F	25
U	■	S	I	L	*L*	E	S	S	W	■	33
W	F	■	U	E	*A*	R	Z	■	A	S	41
E	■	N	E	M	*V*	I	G	A	■	S	49
■	F	U	E	R	*E*	T	E	■	M	E	57
2											**4**
■	N	T	T	E	*T*	■	A	R	M	A	65
D	■	A	■	S	*I*	W	■	W	W		72
		■			*P*			■			80
				■	*O*			■		■	88
■							■				96
	■			■	*R*					■	104
		■			**1**				■		112

El orden por el cual se tratarán las columnas viene dado por una tabla complementaria, en realidad un conjunto de tres. No hemos podido obtener las tablas originales, pero, por la descripción que se encuentra en las instrucciones generales, debe ser más o menos como la que se muestra a continuación.

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
A	2	5	14	9	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3
B	5	14	9	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1
C	14	9	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1	8
D	9	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1	8	11
E	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1	8	11	7
F	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1	8	11	7	4
G	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1	8	11	7	4	10
H	8	11	7	4	10	6	13	2	5	14	9	12	3	1	8	11	7	4	10	6
I	11	7	4	10	6	13	2	5	14	9	12	3	1	8	11	7	4	10	6	13
J	7	4	10	6	13	2	5	14	9	12	3	1	8	11	7	4	10	6	13	2
K	4	10	6	13	2	5	14	9	12	3	1	8	11	7	4	10	6	13	2	5
L	10	6	13	2	5	14	9	12	3	1	8	11	7	4	10	6	13	2	5	14
M	6	13	2	5	14	9	12	3	1	8	11	7	4	10	6	13	2	5	14	9
N	13	2	5	14	9	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12
O	2	5	14	9	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3
P	5	14	9	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1
Q	14	9	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1	8
R	9	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1	8	11
S	12	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1	8	11	7
T	3	1	8	11	7	4	10	6	13	2	5	14	9	12	3	1	8	11	7	4

Si nos fijamos bien veremos que no hay el mismo número de columnas en la rejilla en función de la orientación escogida, diez en un caso o catorce en el otro. Debe escogerse pues una serie que contemple el caso con el que estemos trabajando. Por ejemplo, si escogemos la posición 2 de la rejilla y la serie de catorce números que vienen identificados por la intersección de la línea O, columna A. Estos son 2-5-14-9-12-3-1-8-11-7-4-10-6-13. De estos escogeríamos

los números menores de 10, en nuestro caso 2-5-4-9-3-1-8-7-10-6, con lo que el orden de cifrado sería tal como marcan los números de la serie escogida seleccionando las letras por columnas y en grupos de cinco.

El mensaje resultante sería pues:

AZERITW EIZUWED IILEMRES BESNUTA NIZFFN XFSSEA AXZSARW RACSZGEA VOIUEET XXZWAMMW.

Para enviar el mensaje, éste se agrupa en bloques de cinco letras a los que se añaden dos grupos más, uno indicador y otro de comprobación que se colocaban en la posición que indica la instrucción particular de la clave. Al final del mensaje se añade una referencia del registro del telegrama y del número de grupos, incluyendo los dos comentados anteriormente. Los grupos añadidos se generan de la siguiente manera:
Grupo Indicador, formado por cinco letras.

Letra	**Descripción**
Primera	Posición de la rejilla. El número se convierte en una letra mediante la tabla de equivalencias.
Segunda	Número de la tabla de donde se elige la serie. El número se convierte en una letra mediante la tabla de equivalencias.
Tercera	Línea de la serie.
Cuarta	Columna de la serie.
Quinta	Criterio seguido en la obtención del cifrado.

El criterio seguido para la obtención del cifrado se obtiene de otra tabla en la que a cada letra del alfabeto se le asigna una orientación y una forma de lectura. Por ejemplo:

Criterio de lectura	**Orden de lectura**	**Equivalencias**
Por filas	De derecha a izquierda	I, J, K, L, M, N
	De izquierda a derecha	C, D, E, F, G, H
Por columnas	De arriba abajo	O, P, Q, R, S, T
	De abajo a arriba	U, V, W, X, Y, Z

En este caso si la rejilla está en la posición 3, suponiendo que hayamos escogido los

valores de la tabla 2, y teniendo en cuenta que hemos leído el texto cifrado por columnas y de arriba abajo obtendríamos un grupo de control como el siguiente:

AEOAO

El grupo de comprobación es igual al indicador, pero escogiendo las letras que no hemos usado en la tabla de equivalencias. Es decir, usamos la letra no utilizada que está en la misma columna que la que aparece en el grupo indicador. En nuestro caso el grupo de comprobación sería,

QNJQJ

Con lo que, añadiendo la referencia del registro, que siempre viene precedida de una R y a la que siguen el registro del telegrama (el número de orden de emisión), y el número de grupos de cinco letras que lo forman, quedaría como el siguiente, suponiendo que el grupo indicador y el de control fuesen los dos primeros y que el número de registro fuese el 20:

AEOAO QNJQJ AZERIT WEIZU WEDII LEMRE SBESN UTANI ZFFNX FSSEA AXZSA RWRAC SZGEA VOIUE ETXXZ WAMMW RECFH