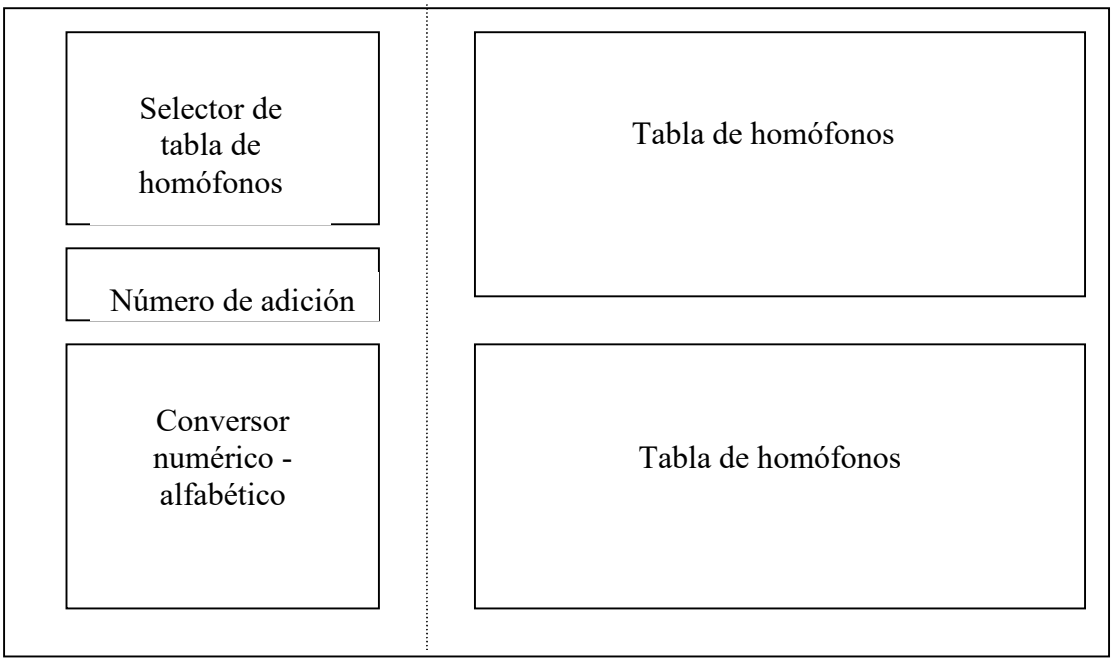
Como diseñar un cifrador táctico seguro. El Cifrador Homofónico Multiple "HomofoniX".

Se tiene la falsa creencia de que un cifrado manual es siempre fácil de romper. Esta creencia es totalmente falsa y la historia nos ha dado varios ejemplos de documentos cifrados que hoy en día siguen guardando sus secretos. Si el mensaje no tiene una longitud mínima, y sobre todo en determinados cifrados, como los homofónicos, hay demasiada inconcreción y ambigüedad lo que no permite hacer un criptoanálisis que nos dé un resultado correcto. La fortaleza de un cifrado depende de varios factores, entre ellos la frecuencia de cambio de claves, el tráfico generado con cada clave y, evidentemente, la fortaleza del propio algoritmo de cifra. En este texto vamos a ver como diseñar un cifrador táctico de lápiz y papel al que hemos dado un nombre que suena a personaje de Asterix, y que aunque no lo sea pretendemos acercarnos a la invencibilidad que caracteriza al pequeño galo. Entenderemos como cifrador táctico aquel cuyas necesidades de seguridad se alargan a unas semanas como máximo y que debe poder hacerse en condiciones en las cuales no se pueden utilizar medios electrónicos. Su característica básica es que los mensajes son cortos y están siempre formados por letras o números. Pretendemos con un ejemplo dar las pautas para hacer un cifrador con suficiente seguridad. No se trata de una nueva técnica para hacer un cifrador, sino de aplicar las técnicas clásicas para diseñar un sistema lo suficientemente seguro.

Si estudiamos la historia el mejor método de cifrado, utilizado en condiciones ideales, es sin duda el código. Al no haber ninguna relación entre el texto fuente y el cifrado es muy difícil la reconstrucción de éste si tiene suficientes términos. Sin embargo, los códigos tienen, en general, el problema de su poca versatilidad. El método más parecido a un código, desde el punto de vista de los sistemas de cifra, es quizás la tabla de homófonos. Partiremos de éste método, pero, para reducir el riesgo de un ataque de texto conocido utilizaremos un sistema homofónico múltiple que sea fácil de intercambiar. Para ello se pueden utilizar unas carpetas pequeñas, con capacidad para 5 hojas, que pueden contener las tablas (2 en cada hoja) dentro de apartados con plástico transparente.

Se podría alegar que con una tabla de homófonos de 1000 términos se conseguiría lo mismo. Sin embargo, eso no es del todo cierto. En primer lugar una tabla de homófonos nos generaría tantos homófonos como en el caso que nosotros hemos escogido, pero cada número representaría una sola letra. En nuestro caso, el mismo número puede representar diferentes letras en función de la tabla escogida, aumentando de esta manera la confusión. Por otra parte siempre es más fácil manejar una tabla de cien homófonos que una de mil. Ésta última podría acabar haciendo que el conjunto de elementos escogidos por cifrador fuese siempre el mismo, haciendo que la seguridad del sistema bajase. Esto es una consecuencia de la tendencia humana a la repetición, no de la debilidad del sistema en sí.

Un esquema de las hojas individuales, tal como las hemos planteado podría ser el siguiente. Nótese que la parte izquierda es fija, habiendo solo un elemento. La parte en la que tendrían que haber diez hojas, que podrían moverse hacia arriba y desplazarse a la parte de atrás con un simple canutillo o espiral es la de la derecha:

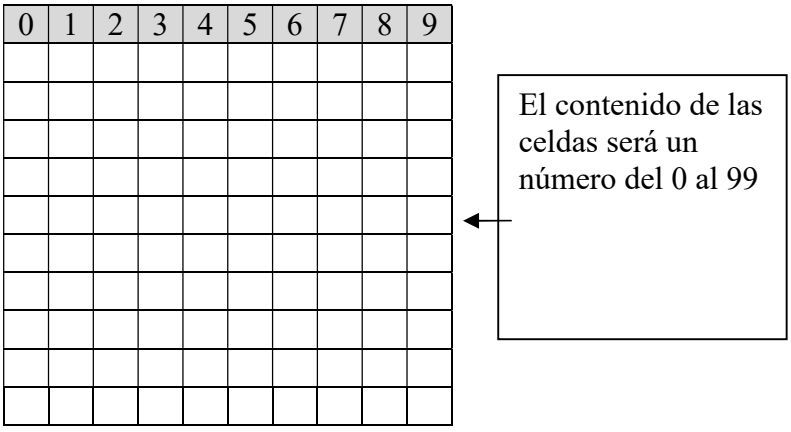


El cambio de clave afectaría a los cuatro componentes de la clave:

1. Selector de tabla de homófonos.
2. Conversor número-letra.
3. Número de adición.
4. Diez tablas de homófonos.

Cada uno de estos apartados sería como los siguientes:

1. **Selector de tabla de homófonos.** Nos permitirá seleccionar la tabla de homófonos a utilizar en ese momento, pero enmascarándolo de manera que no haya una relación directa con ésta. Las tablas vienen identificadas por un número del 0 al 9. Para seleccionar una tabla determinada escogemos un número cualquiera de la columna que identifica a la tabla de homófonos.



Un ejemplo de tabla selectora, que utilizaremos a continuación en los ejemplos, podría ser la siguiente. Nótese que para hacer más fácil la identificación los números de cada columna están ordenados ascendentemente:

0	1	2	3	4	5	6	7	8	9
07	06	00	09	01	08	02	03	05	11
14	15	22	13	18	12	30	19	04	17
25	23	37	16	28	21	31	20	10	26
32	33	39	24	29	37	35	42	27	38
50	34	41	40	48	54	55	46	44	47
59	43	51	52	49	56	63	57	60	65
69	45	68	62	53	66	74	64	75	67
71	58	73	70	61	78	79	77	81	76
72	83	82	85	86	88	80	89	91	87
97	84	96	95	98	99	90	94	93	92

2. **Conversor número – letra.** Esta tabla nos permite hacer una conversión de letra a número y viceversa. El hecho de que las filas de cada número de la tabla estén duplicadas es simplemente para poder buscar más fácilmente, ya que cada número de la izquierda representa la decena del número, y evitar el problema de que no pueda haber dos números de la misma decena representando la misma letra.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0
0																																					
1																																					
2																																					
3																																					
4																																					
5																																					
6																																					
7																																					
8																																					
9																																					

El contenido de la tabla son números del 00 al 99 que están puestos en sus filas para poder identificarlos mejor. Para utilizarla en los próximos ejemplos usaremos la siguiente tabla:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0
0	01			08				02			07		03				04			06									09				00				
	05																																				
1		10			11				19					18	17						13		14		15		16	12									
2	22			23	26				21	20		24	25			27		28	29																	
3			31	32	39	33	35					36	37								38	30				34											
4			42			48	47		40			41		46		45						43		49				44									
5	50		51		52		53		54					57		58		59											56						55		
6		65		66		67		68		69										61		62								60		63		64			
7	79		70			71			72			73		74			75		76			77								78							
8	87	80	88			81		89		82			83				84			85																86
9					99							90	91		92		93			95		96				98				94						97	

3. **Número de adición sin acarreo.** Un número *n* de entre cuatro y doce dígitos. En los ejemplos utilizaremos el 7340, aunque recomendamos utilizar un número de ocho dígitos mínimo.
4. **Tabla de homófonos.** (Hay entre 6 y 10 tablas identificadas con el dígito 0 al 9).

Numero tabla									Nulos			Cambio de tabla								
	2	7	3	6	5	0	4	1	8	7	1	..								3
	G	R	N	P	Z	A	Q	K	LL	S	C	..								RR
0																				
1																				
2																				
3																				
4																				
5																				
6																				
7																				
8																				
9																				

La tabla tiene 30 columnas con dos filas por cada número. Esto permite evitar un problema de las implementaciones de tablas de homófonos, que en general solo tenían una fila. Si una letra cualquiera, pongamos la *e*, estaba representada por el grupo 05, podíamos inferir que ningún grupo empezando por el 0 podía representar a su vez a esa letra. En la columna superior se ponen los números del 0 al 9 repetidos y desordenados por si hubiera que poner un número. Hay dos valores máximo para indicar el inicio y final de grupos de nulos (puede utilizarse cualquiera de los dos como inicio o final) y tres como máximo para indicar el cambio de tabla de homófonos.

Para nuestros ejemplos utilizaremos únicamente las dos siguientes tablas. Como vemos identificamos la tabla con un número entre los valores nulos y los de cambio de tabla:

Número tabla									Nulos			Camb. tabla																		
0									17	37		07	11	13																
	2	7	3	6	5	0	4	1	8	7	1	0	2	3	1	1	9	2	0	6	3	9	7	4	8	2	5	7	4	6
	A	B	C	D	E	F	G	H	I	J	K	L	LL	M	N	Ñ	O	P	Q	QU	R	RR	S	T	U	V	W	X	Y	Z
0	06										09		01					02				03			04			05		
	08																													
1				18					10			16		15			12									14			19	
2	21		20		22		23												24				25	27			28			29
																							26							
3				30		38		31		32					33	35	39			34					36					
4	40		41		42		43		44		45		46		47		48		49											
5																					50		51		52		53		54	
6	60		61		62		63		64		65		69		68		67		66											
7		76		77		78		79												75		74		73		72		71		70
8										80		81		82		83		84			85		89		88		87		86	
9	90				91				92				93				94				95		99		96		98		97	

Número tabla								Nulos		Camb. tabla			
1								23	43		17	19	53

	2	7	3	6	5	0	4	1	8	7	1	0	2	3	1	1	9	2	0	6	3	9	7	4	8	2	5	7	4	6
	A	B	C	D	E	F	G	H	I	J	K	L	LL	M	N	Ñ	O	P	Q	QU	R	RR	S	T	U	V	W	X	Y	Z
0							08		06		04		02		01		03		05		07		09							
1		15	18	13		11																			10		12		14	16
2							20	24		25	21	26	22	27		29		28												
3	39		38			37			36			35								30		31		32		33		34		
4			44		40		48		41		49		42				45				47				46					
5	56				59							57				50		52			55			51			54			55
	58																													
6		60		67			66		61		68			65			62			69			63					64		
7	73				77		72			74			71			70		79		75				78			76			
8	87				80			81			86			82			85					83		88			84			89
9			93				90			97				91	96			94			99		92				95		98	

Formas de funcionamiento.

En primer lugar tendremos que hablar del funcionamiento de una tabla de homófonos estándar. Se trata tan solo de sustituir cada elemento del mensaje en claro por uno de los grupos numéricos que aparece en la columna identificada por esa letra o grupo de letras. Es importante destacar que la sustitución debe ser aleatoria, *nunca cifre cíclicamente*, es decir, si miramos la tabla **1** veremos que la letra A puede representarse por los grupos 39, 56, 58, 73, 87. Uno podría pensar que una buena estrategia sería ir cambiando cada A que apareciese en el texto por cada uno de esos grupos en secuencia. Eso sería un grave error. Existe un método de criptoanálisis que es capaz de romper el cifrado en el caso de utilizarse las tablas de homófonos de esa manera[1].

Por ejemplo, utilizando la tabla 1, si queremos cifrar la frase "MANDEN 15 TANQUES AL FRENTE", obtendríamos:

M	A	N	D	E	N	1	5	T	A	N	QU	E	S	A	L	F	R	E	N	T	E
65	58	01	13	40	01	29	12	78	39	96	69	80	09	73	35	11	99	59	01	32	80

Aunque el cifrado también podría ser:

M	A	N	D	E	N	1	5	T	A	N	Q	U	E	S	A	L	F	R	E	N	T	E
27	87	96	67	59	96	04	59	78	58	01	05	46	59	92	39	26	37	47	80	96	51	40

[1] Puede verse un ejemplo de criptoanálisis de este método, desarrollado por Luis Alberto Benthin, en el apartado *Sobre las tablas de homófonos y su criptoanálisis* del capítulo III de nuestro libro "Mensajes secretos".

Como vemos el cifrado no tiene por qué ser único, aunque sí el descifrado que no debe dar lugar a ambigüedad. Véase además que no hemos utilizado nulos, generalmente no usados en las tablas de homófonos, en cuyo caso las variaciones en el cifrado podrían ser mucho mayores.

Vamos a ver ahora como cifraríamos usando nuestro algoritmo de cifrado. En realidad éste es bastante versátil y nos permite utilizarlo de diferentes maneras. Veremos seis de ellas de menor a mayor fortaleza de cifrado. Es de destacar que se podría usar la forma de cifrar como una parte de la clave. En este caso tendríamos que identificarla en el mensaje simplemente sustituyendo el número que identifica a la forma de cifrado (1, 2, 3, 4 o 5) por uno de los grupos que identifica ese número en la tabla selectora (tabla 1) e incluyéndolo en el mensaje cifrado en una determinada posición acordada de antemano.

Cifrado Básico (1)

El procedimiento es el siguiente:

1. Seleccionar la tabla de cifrado.
2. Escoger un número de la columna que coincida con ese número en el selector de tabla de homófonos (1).
3. Incluirlo como primer grupo cifrado.
4. Empezar a cifrar el mensaje con la tabla de homófonos seleccionada. Ir cambiando de tabla frecuentemente (cifrar entre 10 y 35 letras con cada tabla de homófonos). Incluir de vez en cuando nulos tal como se indica en el paso 6.
5. Cambio de clave.
    a. Poner el indicativo de cambio de cambio de clave (uno de los tres).
    b. Poner un número del selector de tabla de homófonos (1) igual que en el paso 2.
    c. Poner el indicativo de cambio de cambio de clave (uno de los tres).
    d. Empezar a cifrar con la nueva tabla.
6. Inclusión de nulos.
    a. Poner indicativo de nulos (uno de los dos).
    b. Incluir tantos grupos del cuerpo de la tabla de homófonos como se quiera.
    c. Poner indicativo de nulos (uno de los dos).

Veamos un ejemplo. Supongamos que queremos cifrar el mensaje “SE ESPERA ATAQUE INFANTERIA PRECEDIDO FUERTE PREPARACION ARTILLERA”.

En primer lugar dividiremos el mensaje en tantas partes como queramos para cifrar cada una de ellas con una tabla de homófonos diferente. En nuestro caso cifraremos SE ESPERA ATAQUE INFANTERIA PRECEDIDO” con la tabla **1** y el resto con la tabla **0**. Para más seguridad incluiremos un par de nulos después de la primera A de INFANTERIA. El cifrado quedaría así:

1	S	E	E	S	P	E	R	A	A	T	A	QU	E	I	N	F	nulo	nulo	nulo
34	63	59	40	63	52	40	55	56	58	51	39	69	80	36	96	37	23	12	35
nulo	A	N	T	E	R	I	A	P	R	E	C	E	D	I	D	O			
23	73	01	32	77	55	61	87	28	47	59	38	80	13	41	67	45			

Cambio tabla	**0**	F	U	E	R	T	E	P	R	E	P	A	R	A	C	I	O	N	A
19	59	38	36	42	85	73	22	84	50	62	02	08	85	21	20	44	12	68	06
R	T	I	LL	E	R	A													
85	27	64	01	42	95	60													

Como vemos el sistema tiene una desventaja, aumenta el tamaño del mensaje. Por el contrario presenta dos ventajas muy interesantes. En primer lugar el mismo grupo puede representar a varias letras, lo que hace más difícil la labor del posible criptoanalista. Por otra parte su posibilidad de variación del tamaño reduce la posibilidad de comparación del mensaje enviado desde diferentes estaciones, al poder tener estos diferentes tamaños.

Cifrado con enmascaramiento (2)

Se trata de una variante del primero con la intención de ocultar el tipo de cifrado real que se está utilizando. Consiste básicamente en, una vez realizado el cifrado en la forma básica, sustituir cada grupo por una de las letras correspondientes obtenidas de la tabla de conversión número-letra (tabla 2).

Si cogemos el resultado del cifrado anterior el nuevo texto cifrado quedaría:

34	**63**	**59**	**40**	**63**	**52**	**40**	**55**	**56**	**58**	**51**	**39**	**69**	**80**	**36**	**96**	**37**	**23**	**12**	**35**
Y	5	Q	I	5	E	I	8	2	O	C	E	J	B	L	U	M	D	1	G
23	**73**	**01**	**32**	**77**	**55**	**61**	**87**	**28**	**47**	**59**	**38**	**80**	**13**	**41**	**67**	**45**	**19**	**59**	**38**
D	L	A	D	U	8	S	A	Q	G	Q	T	B	T	L	F	O	I	Q	T
36	**42**	**85**	**73**	**22**	**84**	**50**	**62**	**02**	**08**	**85**	**21**	**20**	**44**	**12**	**68**	**06**	**85**	**27**	**64**
L	C	S	L	A	P	A	U	H	D	S	I	J	1	1	H	S	S	O	7
01	**42**	**95**	**60**																
A	C	S	3																

Con lo que nuestro mensaje sería:

YWQIWEIKLLOCEJBLUMDQUGDLADUKSAQGQTBTLFOIQTACSRR

Cifrado con suma sin acarreo (3)

En esta forma de cifrar vamos a utilizar un método ampliamente utilizado en los códigos para hacer variar sus valores, la suma sin acarreo de un número o grupo de ellos. Para ello, cogemos el número *n* de cuatro dígitos del que hemos hablado anteriormente. Los pasos a seguir serían:

1. Cifrar el mensaje en la forma básica.
2. Agrupar el mensaje en grupos de *x* dígitos, siendo *x* el número de dígitos de *n*. Si falta un grupo de dos dígitos incluir uno al azar como relleno. En nuestro caso *x* es 4.
3. Sumar sin acarreo el primer grupo el número de adición que forma parte de la clave.
4. Sumar el resultado obtenido con los equivalentes del grupo cifrado obtenido en el paso anterior.
5. Seguir con lo especificado en el punto anterior hasta el final.

Como ya hemos dicho anteriormente el número *n* que vamos a utilizar es 7340. Veamos el proceso:

3463	5940	6352	4055	5658	5139	6980	3696	3723	1235
7340	*0703*	*5643*	*1995*	*5940*	*0598*	*5627*	*1507*	*4193*	*7816*
0703	**5643**	**1995**	**5940**	**0598**	**5627**	**1507**	**4193**	**7816**	**8041**
2373	0132	7755	6187	2847	5938	8013	4167	4519	5938
8041	*0314*	*0446*	*7191*	*3278*	*5015*	*0943*	*8956*	*2013*	*6522*
0314	**0446**	**7191**	**3278**	**5015**	**0943**	**8956**	**2013**	**6522**	**1450**
3642	8573	2284	5062	0208	8521	2044	1268	0685	2764
1450	*4092*	*2565*	*4749*	*9701*	*9909*	*7420*	*9464*	*0622*	*0207*
4092	**2565**	**4749**	**9701**	**9909**	**7420**	**9464**	**0622**	**0207**	**2961**
0142	9560								
2961	*2003*								
2003	**1563**								

El resultado sería:

07035643199559400598562715074193781680410314044671913278501509438956201365221450409225654749970199097420946406220207296120031563

Evidentemente esta solución no es demasiado útil si el enemigo conoce las tablas de homófonos. Lógicamente la seguridad sigue dependiendo de que las tablas sean secretas. Sin embargo sí que será muy útil para evitar que pueda obtenerlas por medios analíticos. Aparte de que elimina la posibilidad de un descifrado rápido con lápiz y papel, ya que tenemos aproximadamente $10^x - 1$ posibilidades para del número resultado de la suma inicial.

Para descifrar simplemente hay que restar sin acarreo al mensaje cifrado el número utilizado como clave y a partir de aquí ir sacando el resto de números. Haciéndolo solo con la primera fila de nuestro ejemplo tendríamos:

0703	5643	1995	5940	0598	5627	1507	4193	7816	8041
7340	*0703*	*5643*	*1995*	*5940*	*0598*	*5627*	*1507*	*4193*	*7816*
3463	**5940**	**6352**	**4055**	**5658**	**5139**	**6980**	**3696**	**3723**	**1235**

El principal problema de este sistema es que es un poco más laborioso, con lo que es recomendable disponer de una cierta tranquilidad para cifrar y descifrar correctamente. Es pues mas adecuado para una implementación por software. Sin embargo, hace el cifrado más robusto y más difícil de atacar por métodos estadísticos. Se podría hacer lo mismo repitiendo el número escogido como clave tantas veces como hiciera falta, al igual que se hace con los cifrados de Vigenère. Sin embargo, eso hace más vulnerable al cifrado a un ataque por palabra probable si alguna de las tablas es conocida por el enemigo.

Cifrado con suma sin acarreo y enmascaramiento (4)

Podemos ocultar el tipo de cifrado desviando la atención sobre él haciendo lo mismo que en el método (2). Tan solo consiste en:

1. Cifrar en el mensaje en el formato (3).
2. Sustituir cada grupo por una de las letras correspondientes obtenidas de la tabla conversora número-letra (2).

0703	5643	1995	5940	0598	5627	1507	4193	7816	8041
KM	**LLU**	**LS**	**QL**	**AY**	**LLO**	**XK**	**LP**	**XZ**	**BL**
0314	0446	7191	3278	5015	0943	8956	2013	6522	1450
MV	**PN**	**FM**	**DX**	**AX**	**LLU**	**HLL**	**JT**	**BA**	**VA**
4092	2565	4749	9701	9909	7420	9464	0622	0207	2961
IÑ	**MB**	**GW**	**WA**	**ELL**	**NJ**	**RRY**	**SA**	**HK**	**RS**
2003	1563								
JM	**XW**								

Con lo que el mensaje a enviar sería:

KMLLULSQLAYLLOXKLPXZBLMVPNFMDXAXLLUHLLJTBAVAIÑMBGWWAELL
NJRRYSAHKRSJMXW

Cifrado con suma sin acarreo con anagramación (5)

Podemos considerar este sistema como el más seguro de todos ya que rompe cualquier valor estadístico que pudiera quedar. El cifrado sería de la siguiente manera:

1. Cifrar en el mensaje en el formato (3).
2. Dividir el mensaje en líneas de 20 grupos cada línea.
3. Poner los grupos del mensaje de manera que el primer dígito del número esté en la primera fila y el segundo en la segunda. $D_1D_3D_5$
   $D_2D_4D_6$
4. Hacer la sustitución línea a línea en la tabla 2 cogiendo los grupos en la misma línea horizontal, es decir, D_1D_3, D_5D_7, etc.

En nuestro ejemplo:

3	6	5	4	6	5	4	5	5	5	5	3	6	8	3	9	3	2	1	3
4	3	9	0	3	2	0	5	6	8	1	9	9	0	6	6	7	3	2	5
2	7	0	3	7	5	6	8	2	4	5	3	8	1	4	6	4	1	5	3
3	3	1	2	7	5	1	7	8	7	9	8	0	3	1	7	5	9	9	8
3	4	8	7	2	8	5	6	0	0	8	2	2	4	1	6	0	8	2	6
6	2	5	3	2	4	0	2	2	8	5	1	0	4	2	8	6	5	7	4
0	4	9	6																
1	2	5	0																

El resultado final sería:

36	54	65	45	55	53	68	39	32	13	43	90	32	05	68	19	90	66	73	25
27	03	75	68	24	53	81	46	41	53	33	12	75	17	87	98	03	17	59	98
34	87	28	56	00	82	24	16	08	26	62	53	24	02	28	51	04	28	65	74
04	96	12	50																

Con lo que el mensaje a enviar seria:

365465455553683932134390320568199066732527037568245381464153331275178798031
759983487285600822416082662532402285104286574049612 50

Cifrado con suma sin acarreo y enmascaramiento con anagramación (6)

Al igual que en el cifrado tipo 2 haremos un paso suplementario para ocultar el tipo de cifrado real que se está utilizando. Simplemente ciframos con el método anterior y luego sustituimos cada grupo por una de las letras correspondientes obtenidas de la tabla de conversión número-letra (tabla 2).

Si cogemos el resultado del cifrado anterior el nuevo texto cifrado quedaría de la siguiente manera:

36	**54**	**65**	**45**	**55**	**53**	**68**	**39**	**32**	**13**	**43**	**90**	**32**	**05**	**68**	**19**	**90**	**66**	**73**	**25**
L	I	B	O	8	G	H	E	D	T	U	L	D	A	H	I	L	D	L	M
27	**03**	**75**	**68**	**24**	**53**	**81**	**46**	**41**	**53**	**33**	**12**	**75**	**17**	**87**	**98**	**03**	**17**	**59**	**98**
O	M	P	H	L	G	F	N	L	G	F	1	P	Ñ	A	Y	M	Ñ	Q	Y
34	**87**	**28**	**56**	**00**	**82**	**24**	**16**	**08**	**26**	**62**	**53**	**24**	**02**	**28**	**51**	**04**	**28**	**65**	**74**
Y	A	Q	2	6	J	L	Z	D	E	U	G	L	H	Q	C	P	Q	B	N
04	**96**	**12**	**50**																
P	U	1	A																

El resultado seria:
LIBO8GHEDTULDAHILDLMOMPHLGFNLGF1PÑAYMÑQYYAQ26JLZDEUGLHQCP QBNPU1A

Conclusión.

Como vemos podemos hacer un cifrado de lápiz y papel tan complejo como queramos utilizando las lecciones aprendidas a través de la historia. La seguridad del método reside fundamentalmente en las tablas de homófonos con lo que el sistema de distribución de claves y la frecuencia de cambio son fundamentales. Una posible complicación al cifrado para hacerle la vida un poco más difícil a un posible criptoanalista sería añadir una cinta móvil en las tablas (2) y (4). En este caso los dos primeros grupos serían las letras iniciales de colocación de las cintas. Sin embargo, creemos que utilizando cualquiera de los métodos anteriores ya se obtiene suficiente seguridad. Es más, se pueden combinar los métodos anteriores como medida suplementaria de seguridad. En ese caso, habría que incluir un grupo que indicase el formato de cifrado a utilizar.