Tablas de homófonos.

Denominamos así a todos aquellos sistemas en los que se sustituye un símbolo o letra por más de un símbolo cifrado. Es decir se trata de una relación de uno a muchos. Básicamente, lo que se pretende es acabar con el patrón de frecuencias del alfabeto original. Al igual que en los sistemas de sustitución simples tenemos dos alfabetos que utilizaremos para cifrar o descifrar. La diferencia básica está en que en este tipo de cifrados lo que se suele utilizar para estas operaciones es una tabla en la que cada elemento puede tener como contrapartida más de un grupo de símbolos como cifrado. Hay que recalcar que, aunque en general el alfabeto cifrado suele ser multilateral, no tiene por qué serlo y, sobre todo en las tablas del siglo XVI, nos podemos encontrar con que se utilizan varios símbolos extraños y cabalísticos para representar una letra.
El siguiente es un ejemplo de lo que podría ser una tabla de homófonos:

Claro	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
Cifrado	22	28	34	10	23	09	24	07	14	15	06	32	25	58	05	40	20	03	26	04	19	17	31	36	18	33	27
	30	12	11		29	47	56		21	08		16	39	01		02	54		38	41	42	37					
	48				35				45			44	52	46		50			43	55		51					
	13				49									53					57	60		59					

Como vemos, a las letras que aparecen más frecuentemente en los textos se les asignan más valores. En este caso la palabra CIEN se podría transmitir de varias maneras, entre otras como: 34142358, 34452946, 11212953, etc.

Sin embargo, la forma más típica de representar una tabla de homófonos, simplemente porque facilita la tarea de cifrar y descifrar, es mediante una tabla en la que hay varias filas, generalmente nueve o diez y en el que el número de la fila señala a los homófonos que empiezan por ese número. También se pueden dejar algunos números para representar puntos, separaciones o cambio de letras a numeración o viceversa. También, en algunos casos podían incluir un pequeño código con palabras de uso muy habitual. Un ejemplo podría ser el siguiente:

Claro		8				3				5			1	6	2		7			4	9		0					,	.	NL
		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			
Cifrado	0			05			06		02			08	07			01					04				09	03					
	1		10		11						12		13		14			15	19			16		18			17					
	2	27				20		21		25				26	29		22			23	28							24				
	3	38	36	30	35		34			37		33					31						32	39								
	4	41		44		43		49			48			42				46		47	45						40					
	5		59	51					50		58		56		55	57			52	54		53										
	6	67			68	63		66		65			69		64		69				61		62				60					
	7	77				76	72			75				71			74			79			78	73				70				
	8	85		81		84			82	80			83					88					89									
	9	99				92				94							90						92						95	91	93
Código		86	aviones			87	tropas			88	socorro					96	tanques			97	ofensiva				98	retirada						

En este caso la palabra CIEN se podría transmitir de varias maneras, entre otras como: 30652014, 05807655, etc.

Se trata de un sistema relativamente seguro si no hay mucho tráfico. Al igual que el resto de los cifrados de sustitución es vulnerable al ataque de palabra probable.
Otro método que puede utilizarse para generar una tabla de homófonos es utilizar un cuadrado de polibio en el que cada fila y cada columna vienen representadas por dos números o dos letras. La única limitación es que con números tiene que ser un cuadrado de 5x5, ya que si ampliamos la tabla habrá filas o columnas con solo una representación, aunque también se puede jugar con ellas de manera que si solo hay una representación en las filas haya más de una en las columnas y viceversa. En general con números se utiliza la de 5x5, aunque también podría utilizarse la de 6x6 e incluso 7x7 sin problemas. Con letras tenemos muchas más posibilidades.
Para el ejemplo utilizaremos una de 5x5 como la siguiente:

	73	90	62	54	81
37	N	M	E	F	G
81	T	A	O	S	H
25	B	L	D	P	V
94	U	J	C	X	I
60	Z	K	R	Q	Y

Si queremos cifrar la palabra CIEN, en este caso podría representarse de varias maneras diferentes, entre otras: 92913233, 96983637, 42417273, 46487677.

Cifrado de Cinta móvil o método español.

Se trata básicamente de una tabla de homófonos en el que los valores de cada letra cambian en función de la posición marcada por una cinta móvil que se colocaba debajo del alfabeto ordenado, con otro alfabeto en forma aleatoria duplicado o triplicado. Fue muy utilizado en España desde finales del XIX y hasta la segunda mitad del siglo XX (la clave 99 de la Guardia Civil que aparece en el apartado de criptografía real es un ejemplo de este tipo de cifra). Al igual que la tabla de homófonos es relativamente segura si no hay mucho tráfico cifrado. Para romper la cifra, simplemente hay que agrupar los cifrados en grupos. Cada grupo con la misma posición de cinta. Posteriormente tratar cada grupo como una tabla de homófonos. Una vez descubierta la tabla de homófonos, se procede a recuperar la cinta.
Al igual que en el caso anterior, se le podían añadir pequeños códigos, signos de puntuación, etc. Incluso, en la guerra civil, había algunas claves de este tipo con más de una cinta. Un ejemplo, utilizando la tabla de homófonos anterior, podría ser la siguiente:

Claro		8				3				5			1	6	2		7			4	9		0							
		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			
U	G	V	W	D	R	Ñ	N	Q	C	V	K	P	Y	A	L	Z	E	O	T	I	B	S	M	J	F	H	U	G	V	W	D	R	Ñ
Cifrado	0			05			06		02			08	07			01						04				09	03					
	1		10		11						12		13		14			15	19				16		18			17				

	2	27				20		21		25				26	29		22			23	28						24				
	3	38	36	30	35		34			37		33					31						32	39							
	4	41		44		43		49			48			42				46		47	45						40				
	5		59	51					50		58		56		55	57			52	54		53									
	6	67			68	63		66		65			69		64		69				61		62				60				
	7	77				76	72			75				71			74			79			78	73				70			
	8	85		81		84			82	80			83					88					89								
	9	99				92				94							90						92						95	91	93
Código		86	aviones			87	tropas			88	socorro						96	tanques				97	ofensiva			98	Retirada				
Signos		95	,			91	.			93	NL																				

La teoría es que, de esta manera, tendríamos tantas tablas de homófonos como letras tendría el alfabeto. Para identificarlas solo hay que indicar una combinación de dos letras que nos indique la posición de la cinta, por ejemplo la P en la I o la A en la D. Es importante ir cambiando el par de letras que señalan la posición y no utilizar siempre la misma como referencia (por ejemplo la A que es la más evidente) para dificultar la labor del posible criptoanalista. Como vemos es un método sencillo que, en caso de poco tráfico, puede dar suficiente seguridad. Sin embargo, como todos, no es seguro cien por cien. Podemos ver en el libro de García Carmona (en realidad se llamaba Cesáreo Huecas Carmona), un ejemplo de criptoanálisis de este método.

Hemos dicho la parte buena, un sistema que nos permite utilizar con una sola tabla varias tablas de homófonos. Empezamos con las malas noticias. Las tablas de homófonos están hechas de manera que se intenta acabar con la frecuencia del texto original. En este tipo de cifrado no pasa exactamente lo mismo. Si ponemos la W en la A en el sistema de cinta de ejemplo tendríamos un solo símbolo, el 09, para representar la A, lo que sería una locura criptográficamente hablando. Para hacerlo bien, en este método todas las letras tienen que tener entre tres y cinco símbolos cifrados. No debemos hacer tampoco que todos tengan la misma cantidad de símbolos ya que también daríamos pistas a un posible criptoanalista. Para señalar el par de letras de colocación de la cinta, se indica como ya hemos dicho al principio del mensaje, o, mucho mejor, se pueden cambiar las letras por un par de números que indiquen esa posición situados en una posición fija del mensaje (los pares 10 y 3 por ejemplo). Los números se pueden obtener de la columna de cada letra utilizando el alfabeto fijo como referencia (por ejemplo la W en la A podría representarse en el ejemplo como 09 27 o 09 41 entre otros pares). Como vemos un método relativamente seguro si se usa con precaución y con un volumen moderado de tráfico.