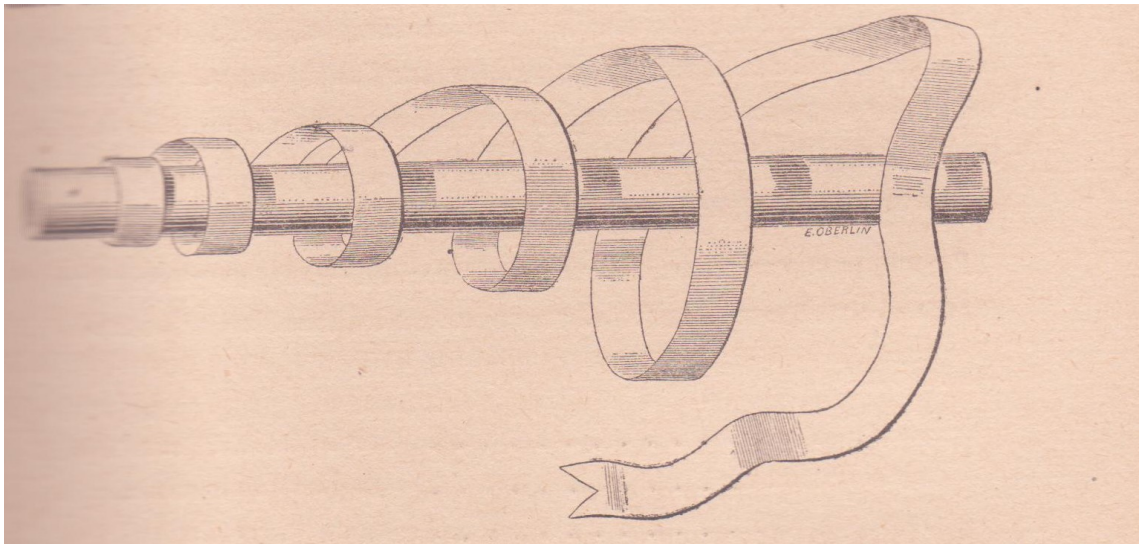
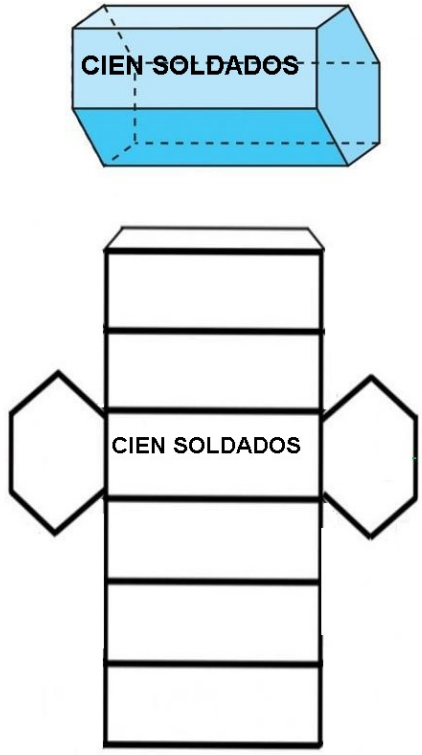
Sistemas de trasposición básicos.

Hablamos de un sistema de trasposición cuando en lugar de intercambiar un símbolo o letra por otro, lo que hacemos es intercambiar el orden de las letras según un patrón preestablecido, de manera que el mensaje resultante sea ininteligible. El cambiar el orden y no los hace que el análisis de la frecuencia de los caracteres no sea útil para el criptoanalizar a este tipo de cifrados, ya que no varía en el mensaje cifrado con respecto al mensaje original. Ese método de criptoanálisis solo es adecuado si se mantiene la posición, pero se cambian los símbolos, es decir, en un cifrado de sustitución.

Si pensamos en un sistema de este tipo, el primero del que tenemos conocimiento es la escítala lacedemonia.



La escítala era un bastón redondo, aunque en realidad debía ser un prisma de seis o más lados (intentad escribir en un bastón redondo y veréis que es sumamente incómodo). Para hacer más sencillo nuestra descripción consideraremos que se trata de un bastón hexagonal. Para cifrar se enrollaba una cinta alrededor del bastón y se escribía el mensaje sobre ella. Al desenrollar la cinta las letras cambiaban el orden con lo que ya no se podía leer el mensaje. En realidad con una simple tabla se puede simular una escítala. Veamos cómo se hace un prisma hexagonal en la imagen siguiente.



Como vemos es equivalente a utilizar una tabla de seis filas que se rellenarían horizontalmente y se enviaría el mensaje verticalmente. Es decir, si queremos cifrar la siguiente frase debemos poner diez letras en cada fila:

C	I	E	N	S	O	L	D	A	D
O	S	E	N	E	M	I	G	O	S
H	A	N	S	I	D	O	V	I	S
T	O	S	E	N	L	A	C	E	R
C	A	N	I	A	D	E	L	P	U
E	B	L	O	V	E	C	I	N	O

Ahora cogemos las letras por columnas y tenemos el mismo resultado que con la escítala:

COHTCEISAOABEENSNLNNSEIOSEINAVOMDLDELIOAECDGVCLIAOIEPNDSSRUO

Este método, el de la tabla, se utilizó, como mínimo, hasta la Segunda Guerra Mundial. Lo utilizaban nuestros compatriotas de la División Azul cuando se necesitaba enviar un mensaje rápido, con un cifrado no demasiado fuerte ya que en unos minutos la información, si era obtenida por el enemigo, ya no les serviría para nada (cifrado táctico).

Podemos también cambiar el orden de rellenado de la tabla y hacerlo por columnas, leyéndolo por filas. Si hiciéramos eso con dos o tres filas tendríamos el famoso método de la valla de ferrocarril o “rail fence”, utilizado en la guerra de Secesión en Norteamérica.

En realidad, podemos utilizar cualquier orden para rellenar la tabla (por columnas, por columnas alternando la dirección, en diagonal empezando por cualquier vértice de la tabla, en diagonal alternando el sentido, etc.), pero tanto el emisor como el receptor del mensaje deben saber tanto el tipo de tabla (filas y columnas), como el

orden de rellenado. Estas dos cosas son las que forman la clave del mensaje. Podemos añadir una tercera que sería una palabra o frase que nos indicaría el orden de lectura. Por ejemplo, utilizando la tabla anterior y leyendo por columnas, si utilizamos la clave “HIPOTENUSA” y el orden alfabético leeríamos las columnas de la siguiente manera, que hemos señalado poniendo un número encima:

3	4	7	6	9	2	5	10	8	1
H	I	P	O	T	E	N	U	S	A
C	I	E	N	S	O	L	D	A	D
O	S	E	N	E	M	I	G	O	S
H	A	N	S	I	D	O	V	I	S
T	O	S	E	N	L	A	C	E	R
C	A	N	I	A	D	E	L	P	U
E	B	L	O	V	E	C	I	N	O

Con lo que el mensaje cifrado sería:

DSSRUOOMDLDECOHTCEISAOABLIOAECNNSEIOEENSNLAOIEPNSEINAVDGVCLI

Una cuestión a tener en cuenta es el qué hacemos si el mensaje es más corto que el número de celdas y no rellenamos completamente la tabla. Hay dos opciones:

- Utilizar la tabla incompleta
- Rellenarla con nulos

Las dos tienen sus ventajas e inconvenientes. En el primer caso, dado que la tabla está incompleta, nos obligaría a hacer una operación matemática. Es decir, si el mensaje fuese “CIEN ENEMIGOS HAN SIDO VISTOS”, tendríamos la siguiente tabla:

C	I	E	N	S	O	L	D	A	D
O	S	E	N	E	M	I	G	O	S
H	A	N	S	I	D	O	V	I	S
T	O	S							

Simplemente dividiríamos el número de letras (33) por el número de columnas (10) con lo que nos daría 3 de resultado y un resto de 3. Con ello sabemos que las tres primeras columnas tendrán cuatro letras y el resto tres.

En el segundo caso, rellenaríamos con “nulos”, es decir, con letras aleatorias de manera que la tabla estuviese totalmente ocupada por letras o números. Al descifrar solo habría una parte con sentido que sería el mensaje y desecharíamos el resto. Esto nos evita hacer la operación del caso anterior haciendo más regular el cifrado y el descifrado. Sin embargo tiene un problema, el número de letras será siempre un múltiplo del número de filas por el número de columnas, con lo que el potencial criptoanalista pronto verá un patrón y podrá deducir fácilmente el número de filas y columnas.