El cifrado ADFGVX.

Se trata de una de las cifras más famosas de la historia, fundamentalmente por la importancia que tuvo su criptoanálisis. Utilizada por los alemanes en la I Guerra Mundial a partir de 1918, su primera versión, la ADFGX, realmente se denominaba GEDEFU 18, abreviatura de "cifra secreta de operadores de radio 18". El nombre por el que ha pasado a la historia le viene precisamente de las letras que se utilizaban para cifrar, dispuestas en una tabla de Polibio. Su historia es la de un sistema criptográfico que tuvo que adaptarse a las necesidades y restricciones que había en su momento. El coronel Fritz Nebel, su autor, necesitaba una cifra que fuese fácil de utilizar, resistente al criptoanálisis y, al mismo tiempo, que el resultado del cifrado pudiese ser transmitido por radio sin muchos errores, debido fundamentalmente a la falta de radiotelegrafistas expertos. La elección de las letras fue precisamente por este último tema. Las letras utilizadas, cinco o seis según el método, se representan de forma muy diferente en morse (la transmisión por radio en esa época se hacía siempre en morse, por eso se solía llamar telegrafía sin hilos, conocida generalmente por su abreviatura francés, TSF). Básicamente se trata de un supercifrado de trasposición sobre un cifrado de sustitución. El primer paso es cifrar usando una tabla de Polibio. Las tablas utilizadas podrían ser las siguientes en función de si utilizamos el ADFGX o el ADFGVX.

	A	D	F	G	X
A	q	w	e	r	t
D	a	s	d	g	h
F	f	k	l	z	x
G	c	v	b	n	m
X	y	u	i	o	p

	A	D	F	G	V	X
A	q	w	e	r	1	t
D	a	s	d	g	2	h
F	f	k	l	z	5	x
G	c	6	b	7	3	8
V	4	v	7	n	9	m
X	y	u	i	0	o	p

El primer paso consistiría en hacer el cifrado de sustitución con la tabla de Polibio cogiendo como primera letra la fila y como segunda la columna. Por ejemplo vamos a cifrar la frase CIEN FUSILES. El resultado sería:

Claro	**C**	**I**	**E**	**N**	**F**	**U**	**S**	**I**	**L**	**E**	**S**
ADFGX	GA	XF	AF	GG	FA	XD	DD	XF	FF	AF	DD
ADFGVX	GA	XF	AF	VG	FA	XD	DD	XF	FF	AF	DD

El siguiente proceso sería el de supercifrar con un método de trasposición. Escogemos por ejemplo la palabra ACHTUNG. En primer lugar disponemos el mensaje cifrado en una tabla con tantas columnas como letras tenga la palabra clave, en nuestro caso siete. Posteriormente colocamos el mensaje por filas, tal como se muestra en la tabla siguiente:

	1	**2**	**4**	**6**	**7**	**5**	**3**
ADFGX	**A**	**C**	**H**	**T**	**U**	**N**	**G**
	G	A	X	F	A	F	G
	G	F	A	X	D	D	D
	X	F	F	F	A	F	D
	D						

	1	**2**	**4**	**6**	**7**	**5**	**3**
ADFGVX	**A**	**C**	**H**	**T**	**U**	**N**	**G**
	G	A	X	F	A	F	V
	G	F	A	X	D	D	D
	X	F	F	F	A	F	D
	D						

El último paso sería coger las letras en columnas según el orden establecido por la palabra clave y que nosotros hemos señalado con un número encima de la letra. Con lo que el mensaje cifrado sería:

Claro	CIEN FUSILES
ADFGX	GGXDAFFGDDXAFFDFFXFADA
ADFGVX	GGXDAFFVDDXAFFDFFXFADA