La xifra de ADFGVX

Tipus	De substitució monoalfabètica y de transposició
Història	Durant la 1a Guerra Mundial (1914-1919) l'exèrcit alemany va fer servir aquesta xifra que era força pràctica per trametre-la per telègraf en codi Morse. Les lletres ADFGVX són prou diferents entre elles en Morse com per no donar peu a confusions.

Mètode

1a fase: substituir lletres

Es fa servir una taula de doble entrada, pactada entre els codificadors, i cada lletra es representa amb les que encapçalen la fila i la columna corresponents.

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

Exemple

Text clar	**d**	**i**	**n**	**o**	**s**	**a**	**u**	**r**	**e**
Text codificat	VX	FA	XV	AF	FX	FF	VF	XD	VD

2a fase: desordenar el missatge

Es tria una paraula clau i es fa una taula amb tantes columnes com lletres tingui la clau. A la primera fila s'escriu la paraula clau i, a sota, casella a casella cada parell de lletres de la 1a fase de la codificació. Mirem com quedaria si triem com a paraula clau: CALAIX

C	**A**	**L**	**A**	**I**	**X**
VX	FA	XV	AF	FX	FF
VF	XD	VD			

Si la taula no queda plena es completa amb un signe neutre. Per xemple podem triar el 2 (FG)

C	A	L	A	I	X
VX	FA	XV	AF	FX	FF
VF	XD	VD	FG	FG	FG

Les lletres de la paraula clau s'ordenen alfabèticament:

CALAIX --- AACILX

Es torna a copiar la taula anterior reordenant les columnes segons aquest ordre alfabètic de la clau:

A	A	C	I	L	X
FA	AF	VX	FX	XV	FF
XD	FG	VF	FG	VD	FG

Per acabar es copia el missatge per columnes d'esquerra a dreta

FA XD AF FG VX VF FX FG XV VD FF FG

Per descodificar un missatge es procedeix a la inversa.

Tasques

1) Codifica aquest missatge: "A les 8 al bosc" amb la paraula clau BROMA.

2) Descodifica aquest missatge: VFVXX DGXGA AAFFF FGFDG DVDVD

3) Intercanvia un missatge breu codificat amb una companya o company de la classe.