

ADGF(V)X

Linguistics 484

First World War

- Combination of three ideas, all good
 - Make it easy to send/receive in Morse
 - Digraph cipher
 - Columnar transposition

Idea 1: *Morse*

• *ADGFVX* easy to send, hard to confuse

Idea 2: Digraphs

- Use a Polybius square, 6 by 6

Polybius square

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

Hero = DX GG GA VX

Idea 3: transposition

O=5	R=6	A=1	N=4	G=3	E=2
D	X	G	G	G	V
X	D	V	F	F	D
V	F	G	A	A	A
V	X	D	G	A	A
V	D	A	G	G	V
D	D	D	D	D	D

Number the letters of the keyword alphabetically.

Result

O=5	R=6	A=1	N=4	G=3	E=2
D	X	G	G	G	V
X	D	V	F	F	D
V	F	G	A	A	A
V	X	D	G	A	A
V	D	A	G	G	V
D	D	D	D	D	D

G V G D A D V D A A V D G F A A G D G F A G G D D

X V V V D X D F X D D

Number the letters of the keyword alphabetically.

ADFGX and ADFGVX

- Original version was a 5x5, no digits used

-

Plus points

- Digraphs broken up by transposition
- 2 keys each day, changed fairly regularly
- specific purpose, protect 1918 spring offensive, worked.

Negatives

- Somewhat error-prone
- Digraph nature easy to guess from very restricted symbol set (6 different symbols)
- ADFGX was broken by Painvin a few weeks after introduction, by heroic cross-checking.