ADFGX - ADFGVX

Jedná se o dvě velmi podobné německé polní šifry z konce první světové války. Luštění speciálních případů těchto systémů (se znalostí části otevřeného textu (Know-plaintext attack) nalezl v roce 1918 francouzský důstojník kryptoanalytik Georges- Jean Painvin Obecné řešení těchto šifer nalezl až roku 1933 známý americký kryptolog ruského původu William Friedman.

Ze systémového hlediska se jedná o digrafickou substituci realizovanou pomocí Polybiova čtverce a následnou sloupcovou transpozici. Souřadnice Polybiova čtverce tvořila písmena ADFGX nebo ADFGVX. Šifrová abeceda je tedy v těchto systémech tvořena pouze pěti resp. šesti znaky. Souřadnice ADFGX se používaly pro případ čtverce 5x5, který obsahoval znaky mezinárodní abecedy; souřadnice ADFGVX pro případ čtverce 6x6, který mimo znaků mezinárodní abecedy obsahoval i deset číslic. Důvod, proč byly vybrány právě jako znaky šifrové abecedy písmena ADFGVX je v tom, že šifrový text byl přenášen rádiem a kódy těchto písmen v Morseově abecedě trénovaný radista i při špatném příjmu dobře rozezná (A .-, D -.., F ..-., G --., V ...-, X -..-.). Při šifrování se používaly dva různé klíče. První klíč tzv. substituční určoval obsah převodové tabulky a druhý klíč tzv. permutační, určoval velikost transpoziční tabulky do které se vepisoval šifrový text a pořadí vypisování sloupců z této tabulky.

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

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

Příklady substitučních tabulek používaných při šifrování systémem ADFGX - ADFGVX

Vzhledem k tomu, že tabulka pro ADFGX má pouze 25 znaků, je třeba při použití mezinárodní abecedy jednu „buňku“ tabulky využít pro dva znaky. Nejběžnějšími spojeními jsou: J/I , U/V, Q/W nebo se nahrazuje W znaky VV.

Příklad – postup při šifrování pomocí šifrového systému ADFGX

První klíč tzv. substituční určoval obsah převodové tabulky
Substituční klíč : NASE VEC MUSI ZVITEZIT
Substituční klíč : NASE VC MUI ZT (po vypuštění opakujících se písmen)

Tabulka 25 znaků: A-Z, W --> nahrazeno za V V.

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

Pomocí substitučního hesla se vytvoří převodová tabulka. Heslo se vepisuje do tabulky zleva doprava, pokud již nějaké písmeno hesla bylo do tabulky jednou vepsáno, tak se při dalších výskytech vynechá. Tabulka se doplní písmeny, které v hesle nejsou obsaženy. Zvolené substituční heslo vede na výše uvedenou převodovou tabulku.

Druhý klíč tzv. permutační, určoval po permutačním vyčíslení příslušnou transpozici
Permutační klíč : UKAZKA
Permutační vyčíslení: 531642
Permutační klíč v originální šifře byl dlouhý přes dvacet znaků. Klíč a jeho permutační vyčíslení určuje velikost transpoziční tabulky (v našem případě to bude 6 sloupců).

Nyní si připravíme otevřený text (přepsaný do mezinárodní abecedy) :
SKAKAL PES PRES OVES

Otevřený text se nejdříve zašifroval pomocí digrafické substituce, určené převodovou tabulkou:

S	K	A	K	A	L		P	E	S		P	R	E	S	O	V	E	S
AF	GF	AD	GF	AD	GG		XA	AG	AF		XA	XF	AG	AF	GX	AX	AG	AF

Následovala transpozice. Předšifrovaná zpráva se vepsala do tabulky pod permutační klíč. Text se vepisuje do tabulky po řádcích zleva doprava..

U	K	A	Z	K	A
5	3	1	6	4	2
A	F	**G**	F	A	D
G	F	**A**	D	G	G
X	A	**A**	G	A	F
X	A	**X**	F	A	G
A	F	**G**	X	A	X
A	G	**A**	F		

Konečný šifrový text se získá vypsáním sloupků této tabulky do jednoho řádku. Sloupky se vypisují v pořadí permutačního vyjádření.

G A A X G A D G F G X F F A A F G A G A A A A G X X A A F D G F X F

Výsledný šifrový text se získá rozdělením šifrových znaků do skupin po pěti znacích.
G A A X G A D G F G X F F A A F G A G A A A A G X X A A F D G F X F+