2.6. Szyfr ADFGVX

Bardziej złożoną odmianą szyfru Polibiusza jest szyfr ADFGVX. Szyfrowanie tą metodą odbywa się w dwóch krokach i wykorzystuje ona operacje podstawiania i przestawiania.

W metodzie tej wpisywane są litery (również cyfry) do kwadratu o wymiarach 6 × 6. Dla utrudnienia złamania szyfru wpisuje się je w przypadkowej kolejności.

Pierwszy krok polega na odczytaniu indeksów znakowych kolumn i wierszy. Z tablicy otrzymany zostaje wstępnie zaszyfrowany tekst.

Kolejny etap polega na utworzeniu tablicy z uzyskanego kryptogramu, gdzie w pierwszym wierszu wpisane zostaje słowo kluczowe. Tak skonstruowana tablica zostaje uporządkowana poprzez przestawienie kolumn zgodnie z porządkiem alfabetycznym na podstawie słowa kluczowego.

Ostateczny tekst zaszyfrowany otrzymany zostaje po odczytaniu tablicy kolumnami.

Tekst zaszyfrowany w ten sposób przesyłany był przy pomocy alfabetu Morse'a. W szyfrze tym wykorzystano litery A, D, F, G, V, X z przyczyn bardzo praktycznych. Litery te w alfabecie Morse'a bardzo się różnią, dzięki czemu zminimalizowano prawdopodobieństwo błędu podczas przesyłania wiadomości.[1, 12]

Przykład 2.6.1.

Tekst jawny: ALGORYTM Klucz: ADAM

Krok 1

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

Tablica 2.6. Tablica z tekstem jawnym.

Po poprawnym odczytaniu otrzymany zostanie kryptogram: DA XA GX FA DD GA VF VD

Krok 2

A	D	A	M
D	A	X	A
G	X	F	A
D	D	G	A
V	F	V	D

Tablica 2.7. Tablica z wpisanym kluczem i kryptogramem.

A	A	D	M
D	X	A	A
G	F	X	A
D	G	D	A
V	V	F	D

Tablica 2.8. Tablica z kryptogramem po przestawieniu.

Poprawnie odczytany tekst z tablicy:

DG DV XF GV AX DF AA AD