Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
им. В.И. Ульянова (Ленина)

Лабораторная работа №1+2+3

ИЗУЧЕНИЕ КЛАССИЧЕСКИХ ШИФРОВ

Студент: _____ Выонг В.З, группа 1362

Руководитель: _____ Племянников А.К., доцент каф. ИБ

Санкт-Петербург 2025

Цель работы

Цель: Повышение компетенции в области криптографии

Задачи: Исследовать классические шифры: Rail Fence, Scytale, Caesar, Substitution, Permutation/transposition, vigenere, Hill, adfgvx, playfair.

Получить общее представление о работе шифров и возможных атаках на них.

Визуализация алгоритма зашифрования Rail Fence в инфографике

Открытый текст: Vuong Van Duy

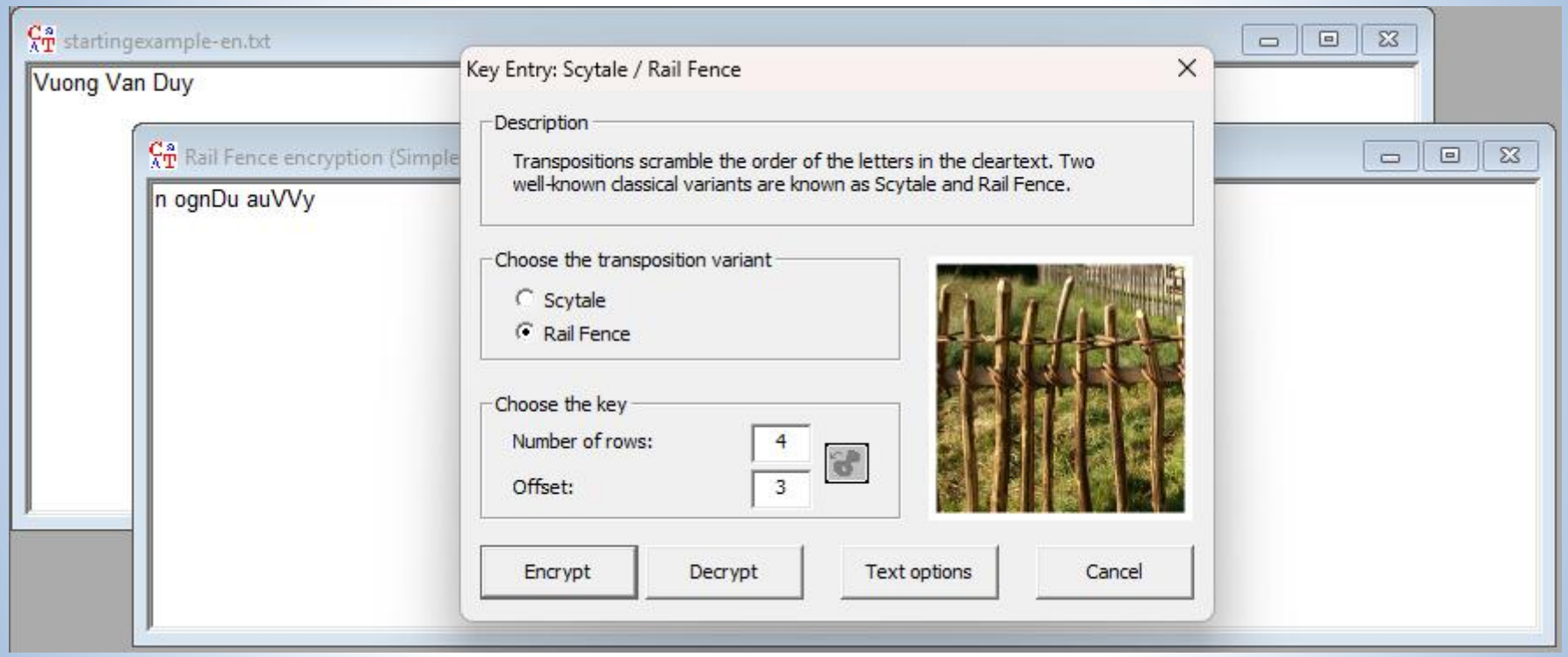
Количество строк: 4

Offset: 3

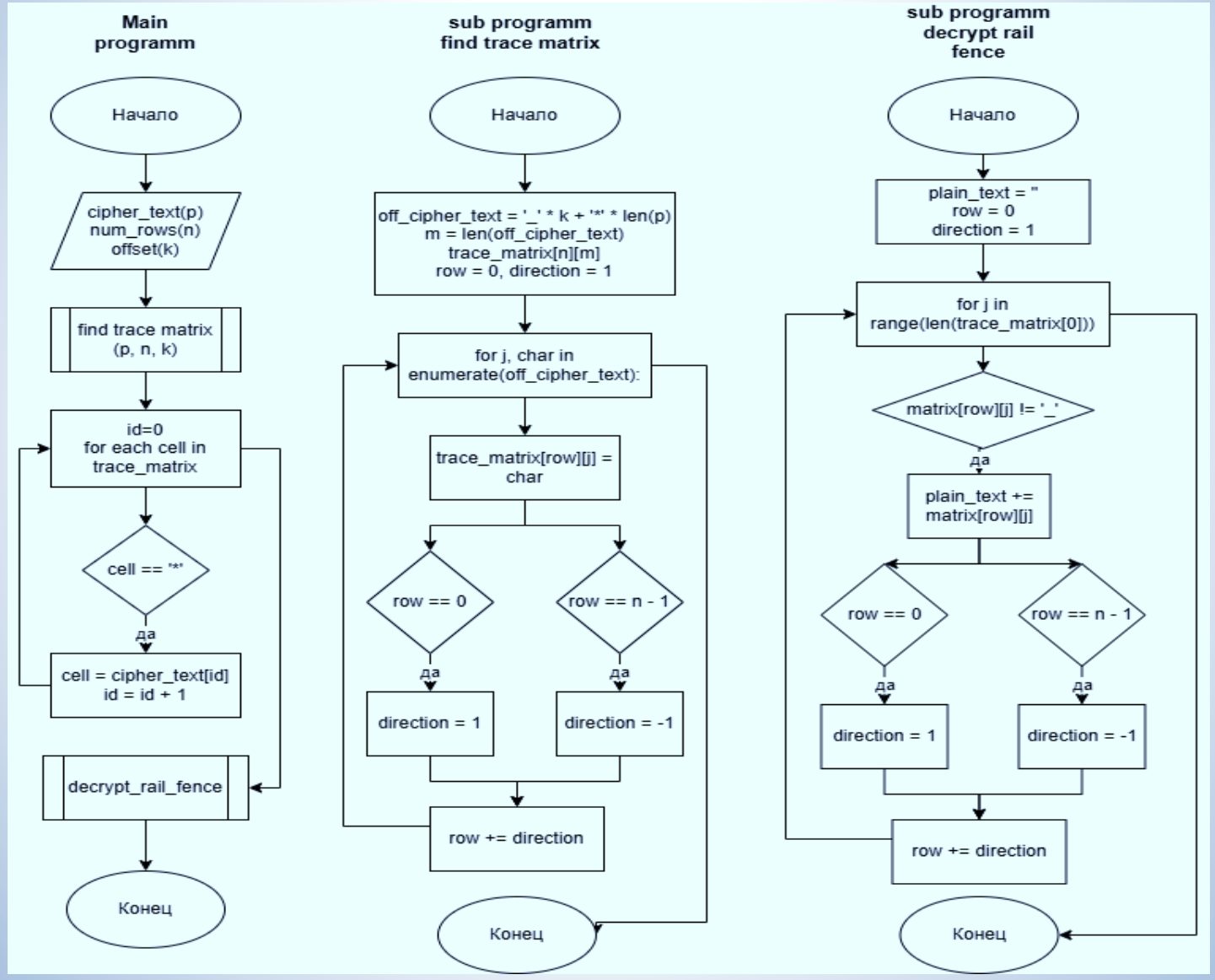
-						n									
	-				o		g				n		D		
		-		u						a				u	
			V						V						y

Шифровка: n ognDu auVVy

Схему инструмента CrypTool 1 для исследования протокола зашифрования и расшифрования сообщения



Блок-схему алгоритма расшифрования сообщения



Визуализация алгоритма зашифрования Scytale в инфографике

Открытый текст: Vuong Van Duy

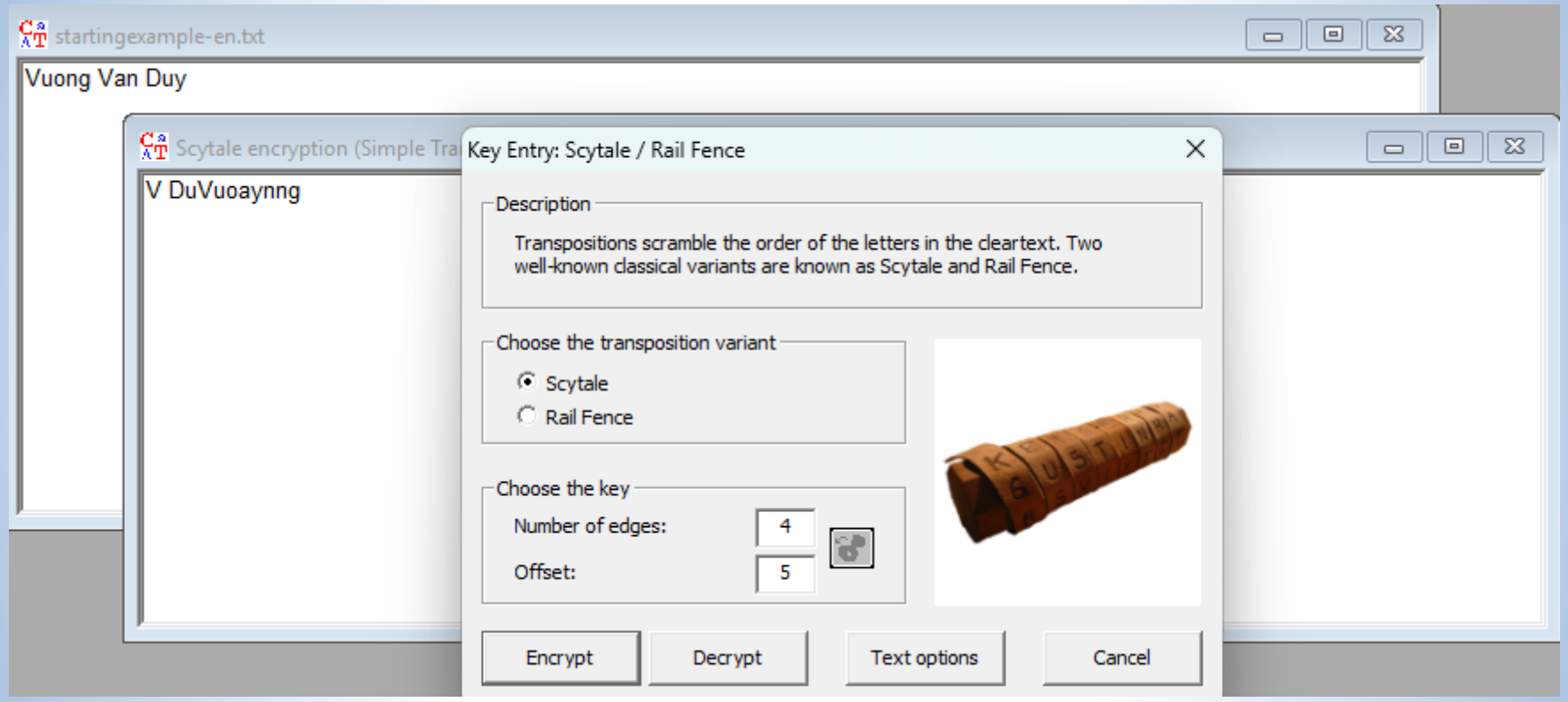
Количество ребер: 4

Offset: 5

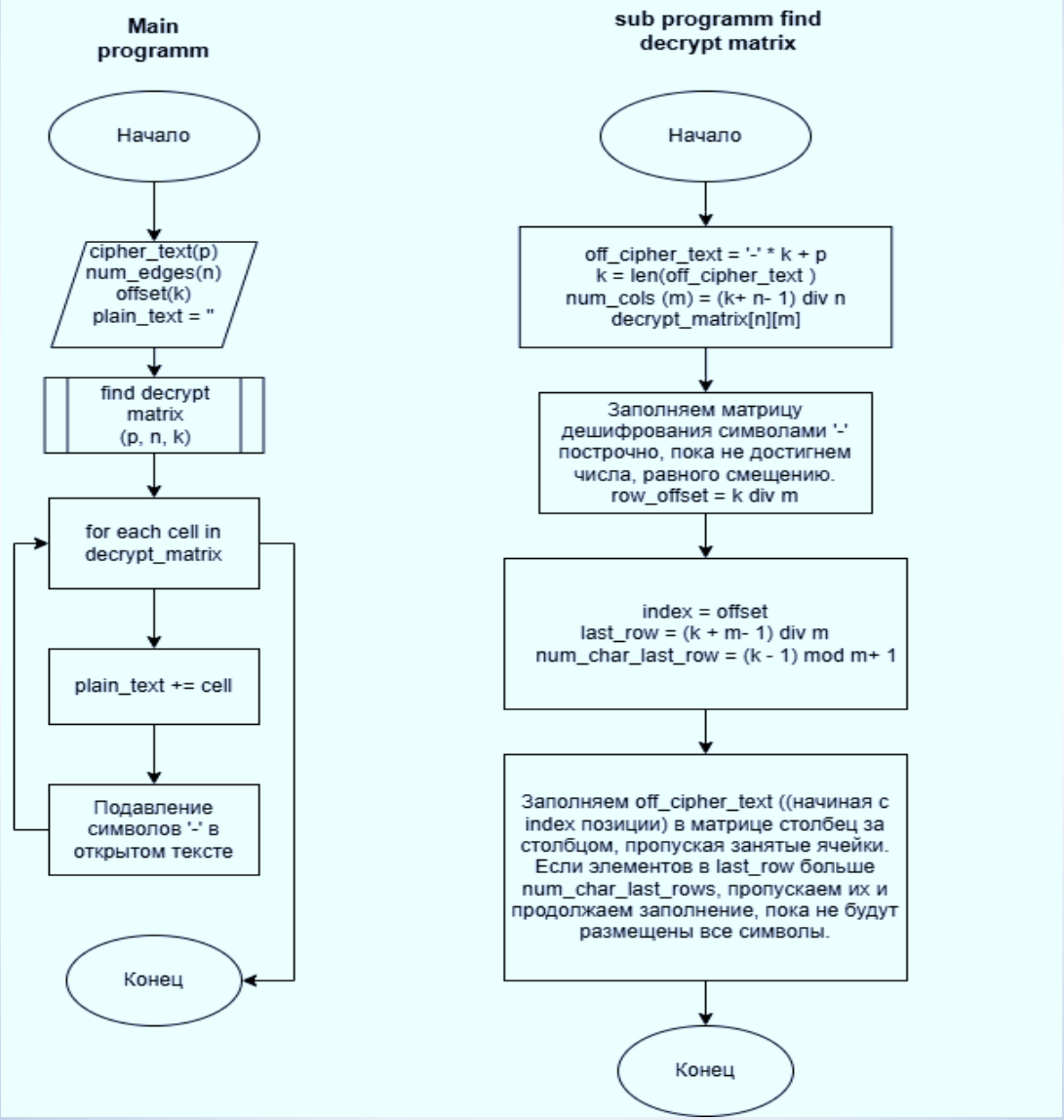
-	-	-	-	-
V	u	o	n	g
	V	a	n	
D	u	y		

Шифровка: V DuVuoaynng

Схему инструмента CrypTool 1 для исследования протокола зашифрования и расшифрования сообщения



Блок-схему алгоритма расшифрования сообщения



Визуализация алгоритма зашифрования Caesar в инфографике

Открытый текст: Vuong Van Duy

Алфавит: ABCDEFGHIJKLMNOPQRSTUVWXYZ

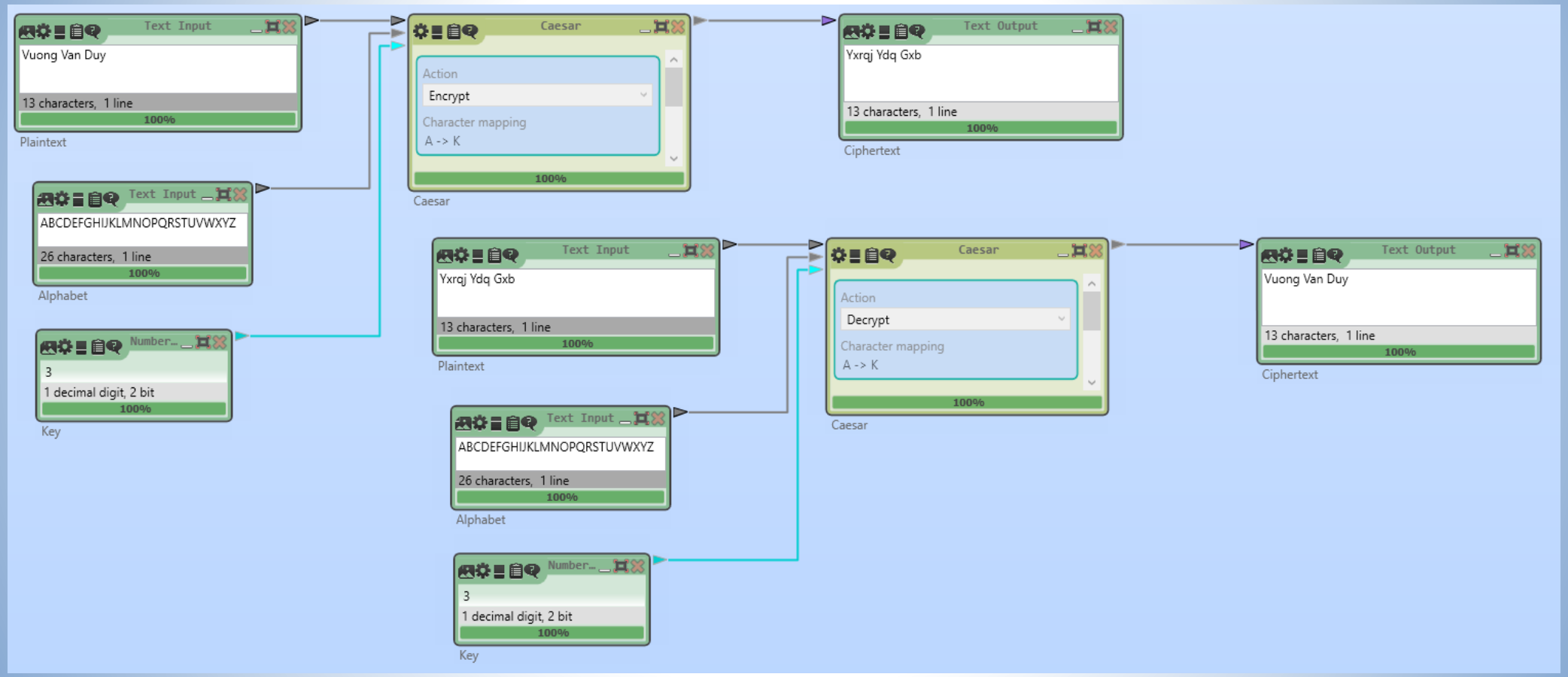
Сдвиг: 3

Алфавит после сдвига: defghijklmnopqrstuvwxyzabcDEFGHIJKLMNOPQRSTUVWXYZABC

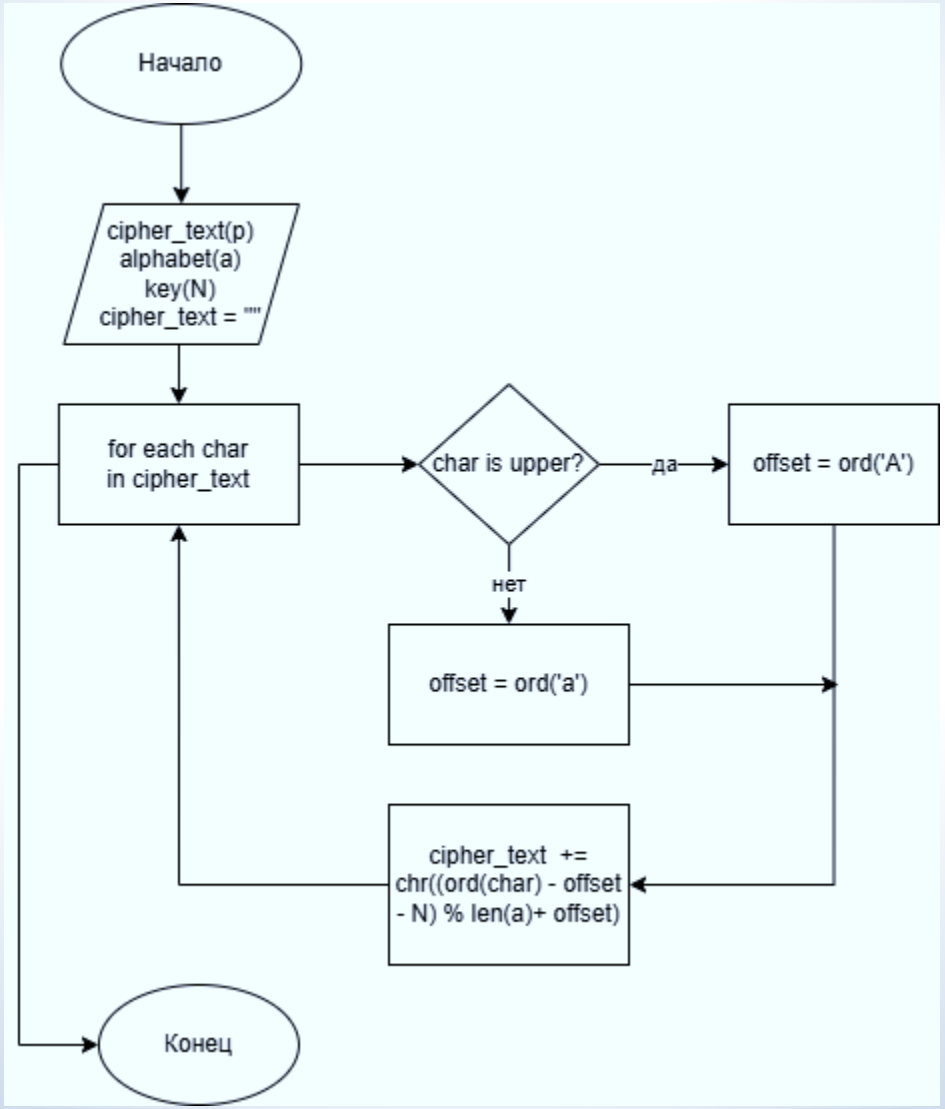
a	b	…	g	h	…	n	o	p	…	u	v	…	y	z	…	D	E	…	V	…	Z
d	e	…	j	k	…	q	r	s	…	x	y	…	b	c	…	G	H	…	Y	…	C

Шифровка: Yxrqj Ydq Gxb

Схему инструмента CrypTool 2 для исследования протокола зашифрования и расшифрования сообщения



Блок-схему алгоритма расшифрования сообщения



Визуализация алгоритма зашифрования Substitution в инфографике

Открытый текст: Vuong Van Duy

Алфавит: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Кодовое слово: password

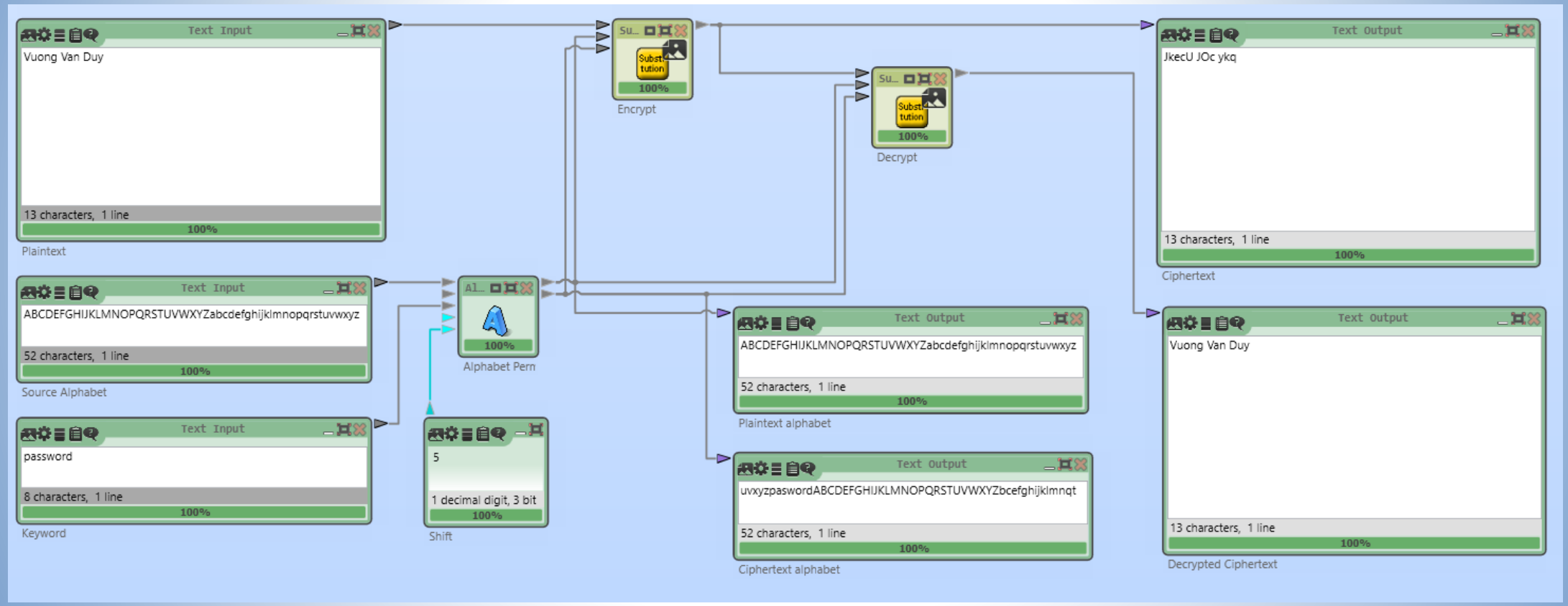
Смещение: 5

Шифр алфавита: uvxyzpaswordABCDEFGHIJKLMNOPQRSTUVWXYZbcefghijklmnqt

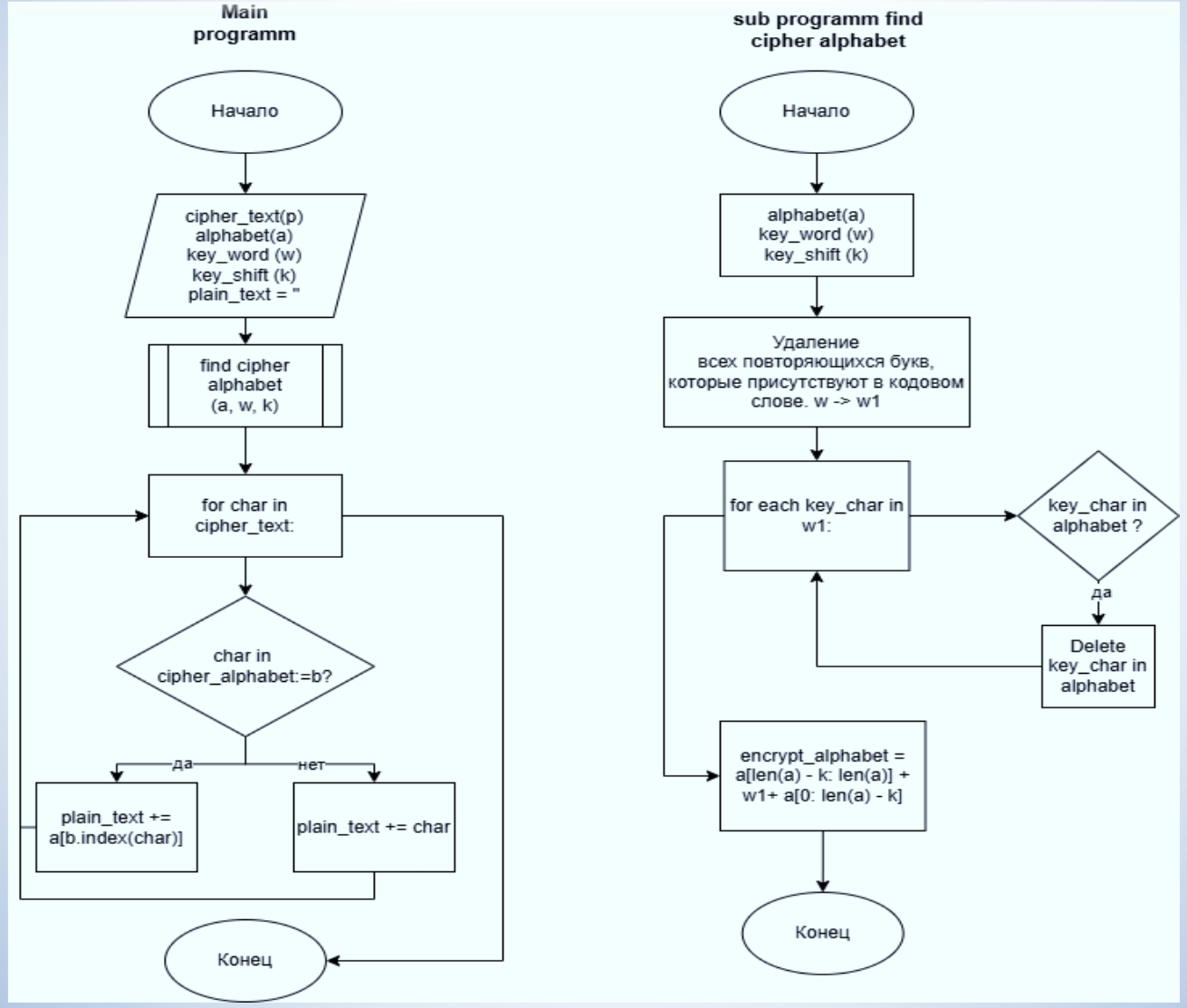
A	B	…	D	E	…	V	W	…	a	b	…	g	h	…	n	o	p	…	u	v	…	y	z
u	v	…	y	z	…	J	K	…	O	P	…	U	V	…	c	e	f	…	k	l	…	q	t

Шифровка: JkecU JOc ykq

Схему инструмента CrypTool 2 для исследования протокола зашифрования и расшифрования сообщения



Блок-схему алгоритма расшифрования сообщения



Визуализация алгоритма зашифрования Permutation/Transposition в инфографике

Открытый текст: My name is Vuong Van Duy from group 1362

Кодовое слово: secret

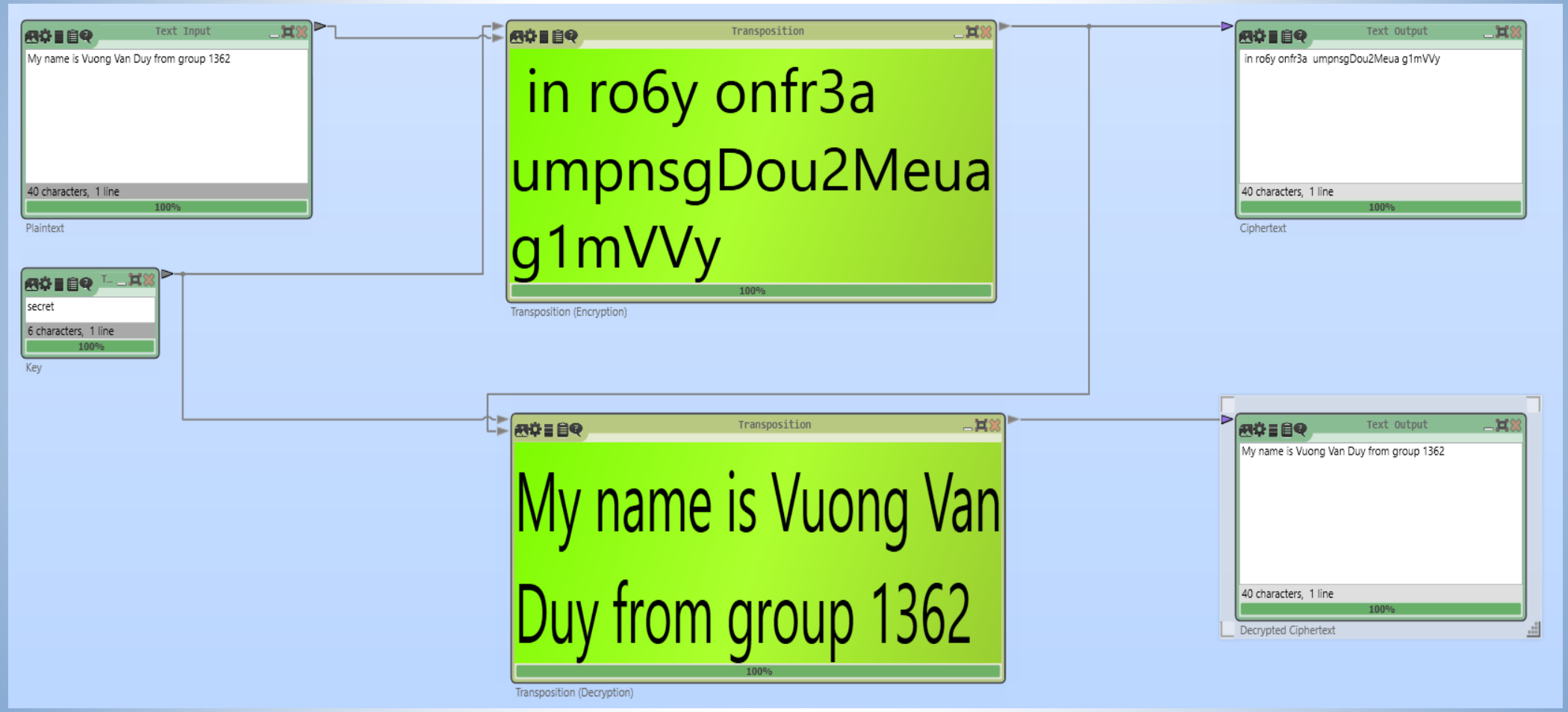
5	2	1	4	3	6
s	e	c	r	e	t
M	y		n	a	m
e		i	s		V
u	o	n	g		V
a	n		D	u	y
	f	r	o	m	
g	r	o	u	p	
1	3	6	2	-	-

Шифровка

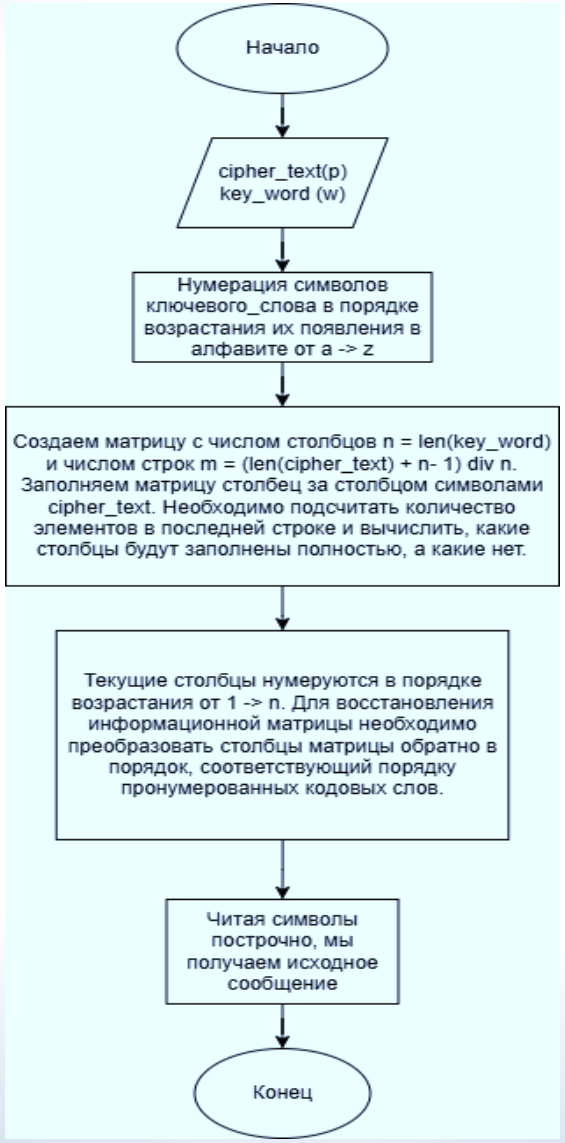
1	2	3	4	5	6
c	e	e	r	s	t
	y	a	n	M	m
i			s	e	V
n	o		g	u	V
	n	u	D	a	y
r	f	m	o		
o	r	p	u	g	
6	3	-	2	1	-

Шифровка: in ro6y onfr3a umpnsgDou2Meua g1mVVy

Схему инструмента CrypTool 2 для исследования протокола зашифрования и расшифрования сообщения



Блок-схему алгоритма расшифрования сообщения



Визуализация алгоритма зашифрования Vigenere в инфографике

Открытый текст: My name is Vuong Van Duy from group 1362

Кодовое слово: secret

Таблица замен:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

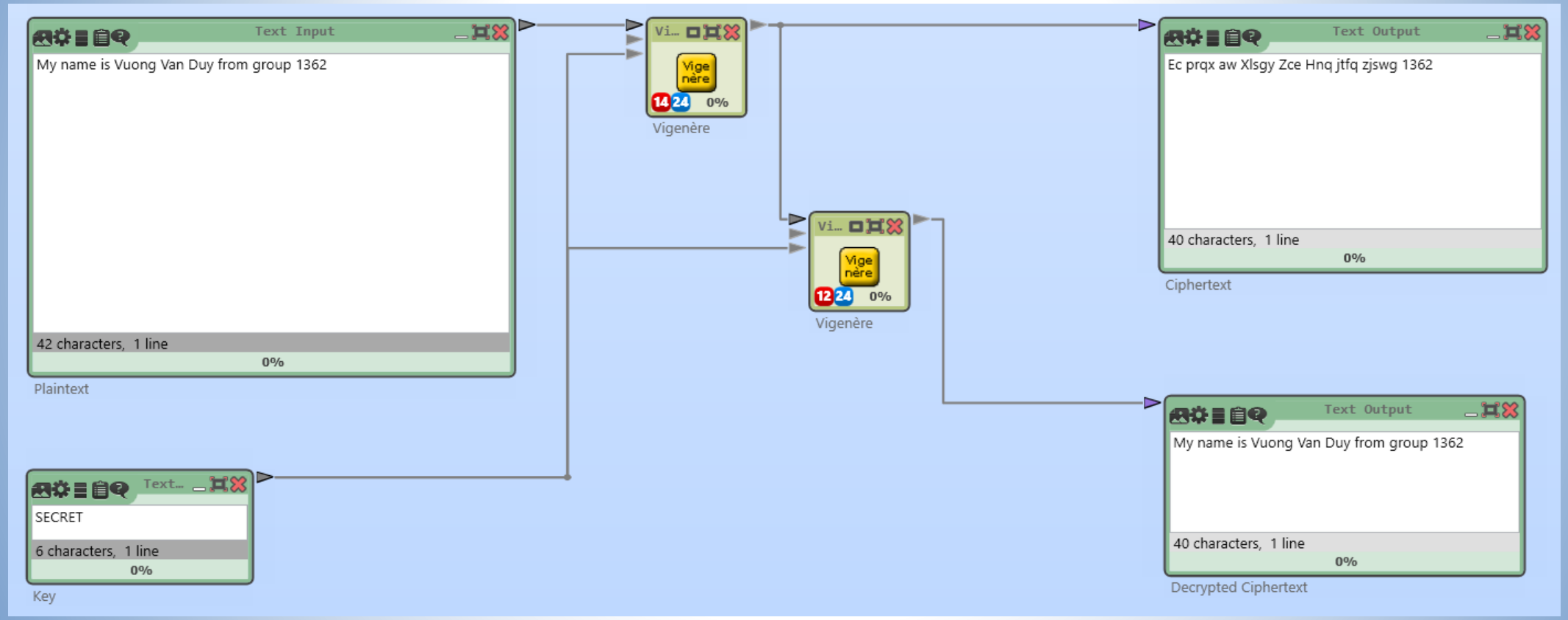
MYNAME	ISVUON	GVANDU	YFROMG	ROUP

Шифровка

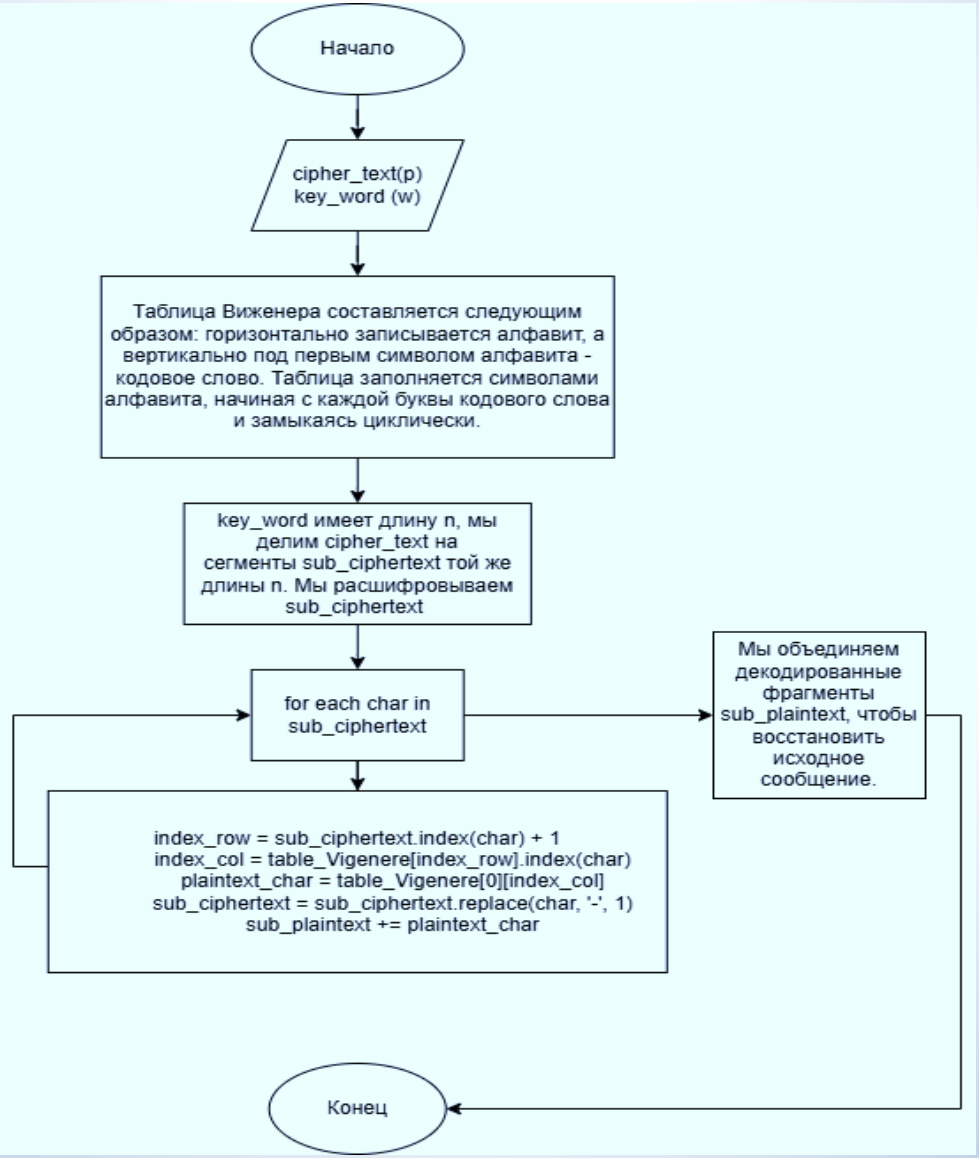
ECPRQX	AWXLSG	YZCEHN	QJTFQZ	JSWG

Шифровка: Ec prqx aw Xlsgy Zce Hnq jtfq zjswg 1362

Схему инструмента CrypTool 2 для исследования протокола зашифрования и расшифрования сообщения



Блок-схему алгоритма расшифрования сообщения



Визуализация алгоритма зашифрования Hill в инфографике

Открытый текст: VUONGVANDUY

Матрица Хилла:

2	15	22	3
1	9	1	12
16	7	13	11
8	5	9	6

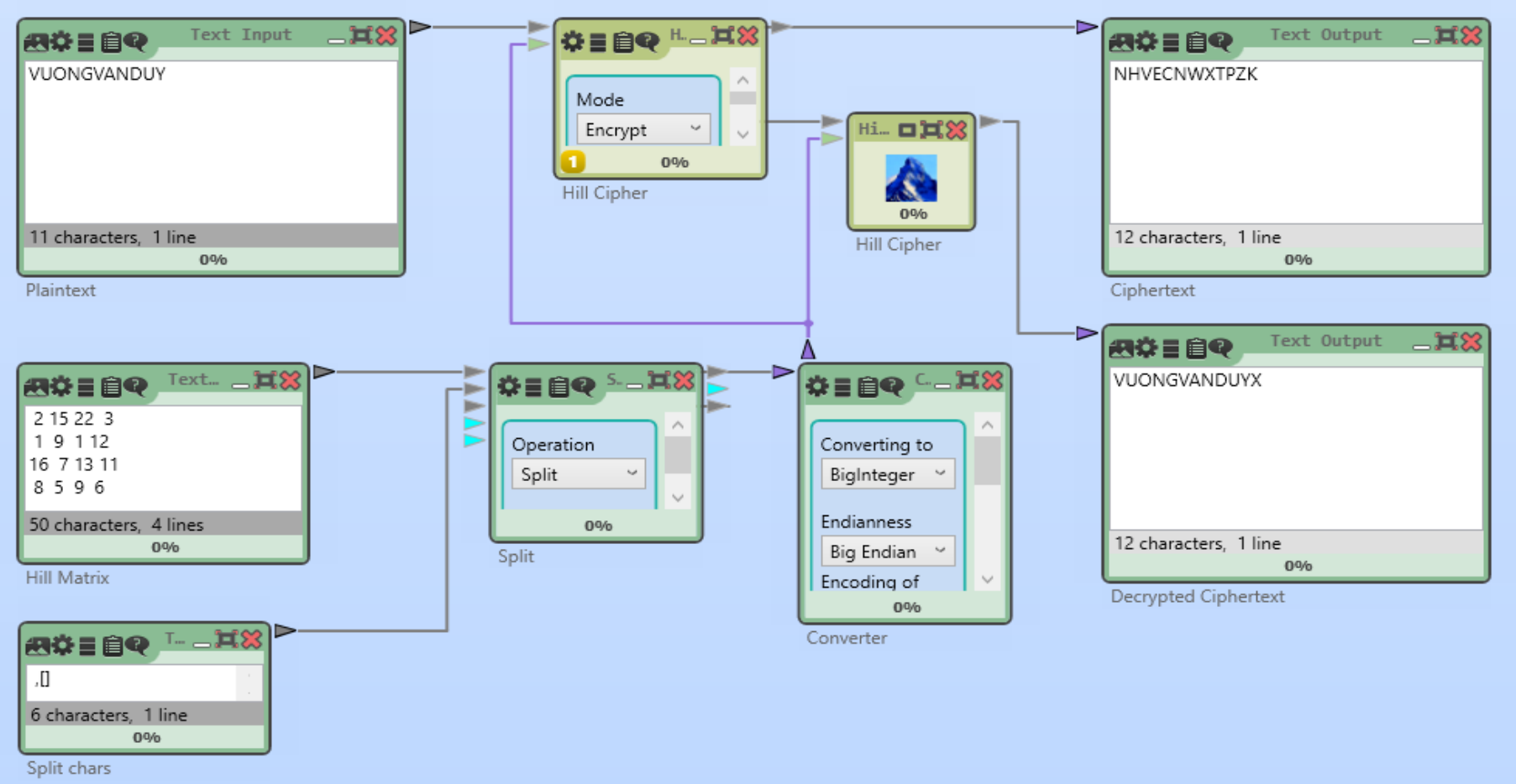
Матрица открытого текста:

21	20	14	13
6	21	0	13
3	20	24	23

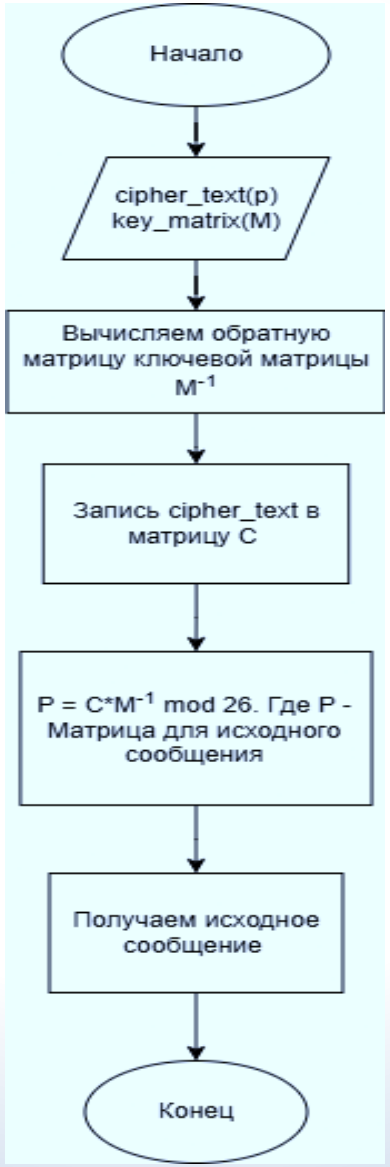
21	20	14	13		2	15	22	3		0	8	1	15
6	21	0	13	×	1	9	1	12	=	7	6	10	10
3	20	24	23		16	7	13	11		22	14	7	1
					8	5	9	6					

Шифровка: AIBPHGKKWOHB

Схему инструмента CrypTool 2 для исследования протокола зашифрования и расшифрования сообщения



Блок-схему алгоритма расшифрования сообщения



Визуализация алгоритма зашифрования ADFGVX в инфографике

Открытый текст: My name is Vuong Van Duy from group 1362

Substitution key: SUBSTITUTION

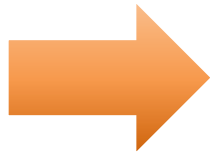
Transposition key: TRANSPOSITION

Substitution matrix

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

Произвести перестановку

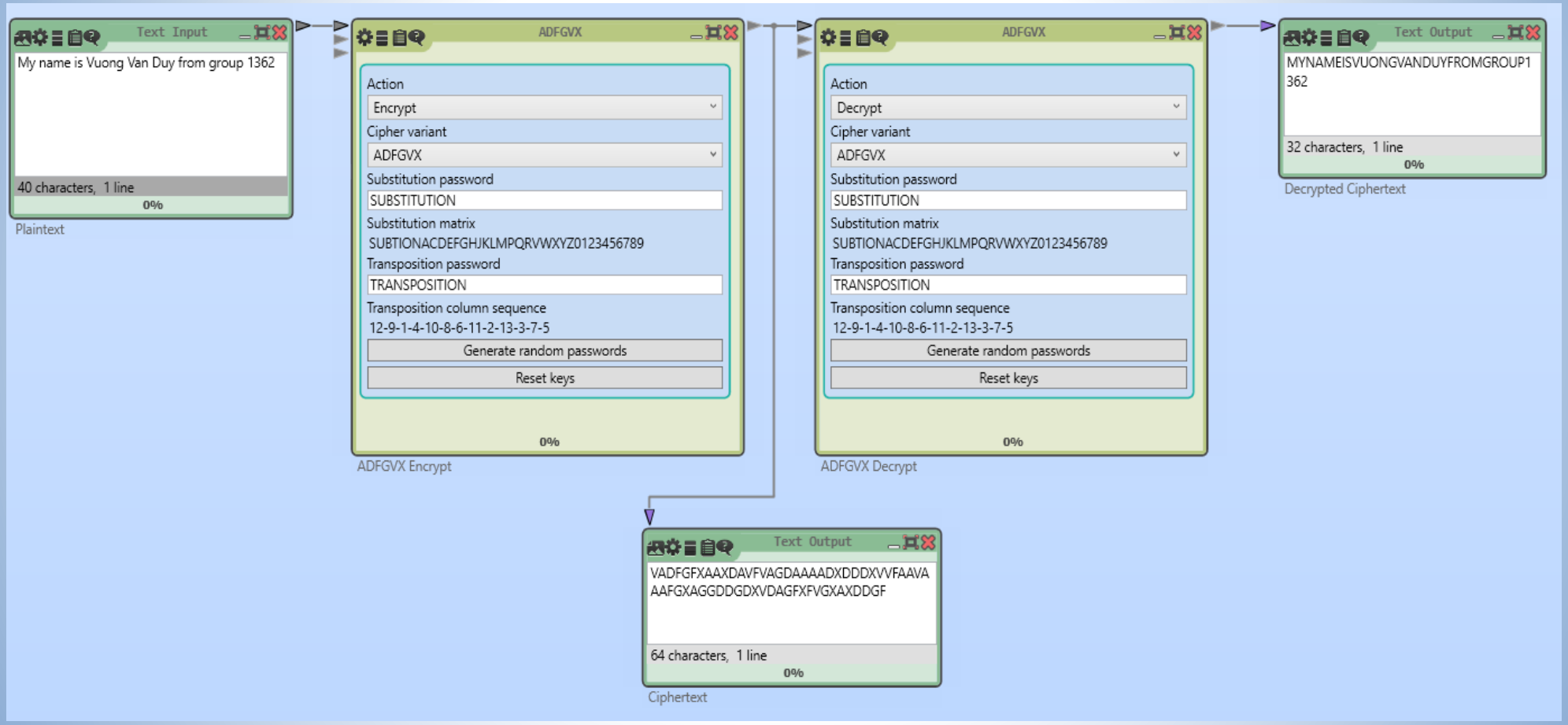
12	9	1	4	10	8	6	11	2	13	3	7	5
T	R	A	N	S	P	O	S	I	T	I	O	N
-	-	-	-	-	-	-	-	-	-	-	-	-
F	X	V	A	D	A	D	D	F	X	D	V	A
V	A	A	G	G	A	D	A	X	D	A	F	A
G	G	D	D	D	A	D	G	A	D	V	A	D
X	G	F	A	X	F	X	F	A	G	F	A	X
A	D	G	A	V	G	V	X	X	F	V	V	-



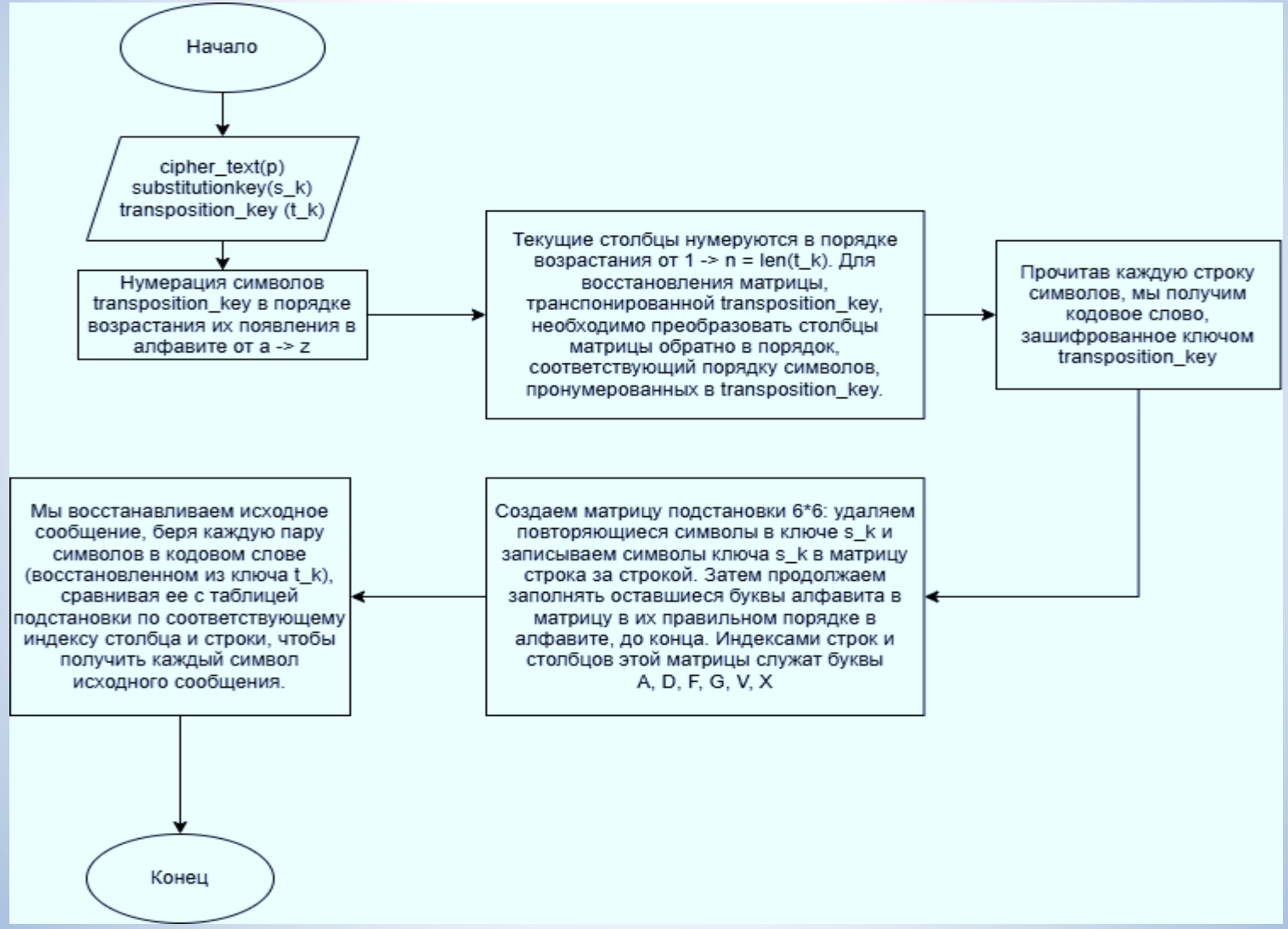
1	2	3	4	5	6	7	8	9	10	11	12	13
A	I	I	N	N	O	O	P	R	S	S	T	T
-	-	-	-	-	-	-	-	-	-	-	-	-
V	F	D	A	A	D	V	A	X	D	D	F	X
A	X	A	G	A	D	F	A	A	G	A	V	D
D	A	V	D	D	D	A	A	G	D	G	G	D
F	A	F	A	X	X	A	F	G	X	F	X	G
G	X	V	A	-	V	V	G	D	V	X	A	F

Шифровка: VADFGFXAAXDAVFVAGDAAAADXDDDXVVFAAVAAAFGXAGGDDGDXVDAGFXFVGXAXDDGF

Схему инструмента CrypTool 2 для исследования протокола зашифрования и расшифрования сообщения



Блок-схему алгоритма расшифрования сообщения

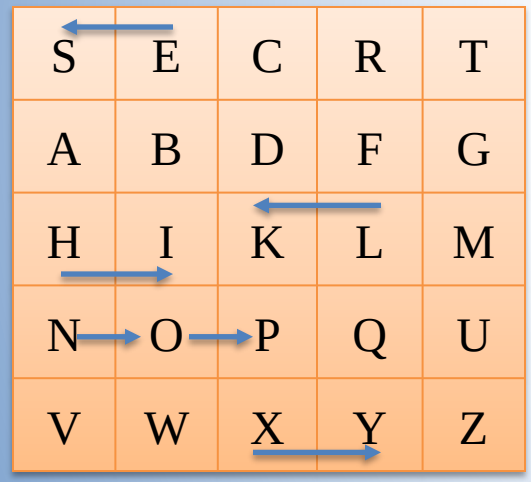


Визуализация алгоритма зашифрования Playfair в инфографике

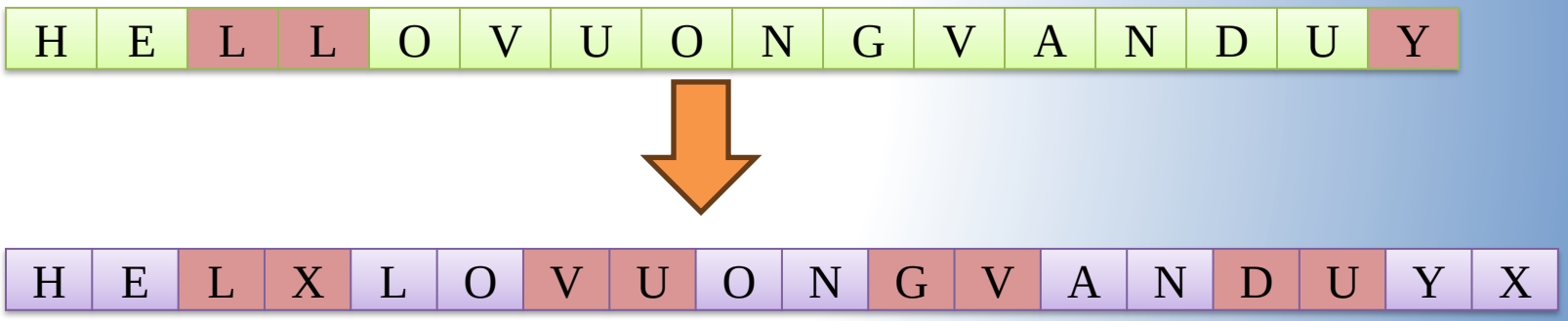
Открытый текст: Hello Vuong Van Duy

Key word: SECRET

Encryption matrix

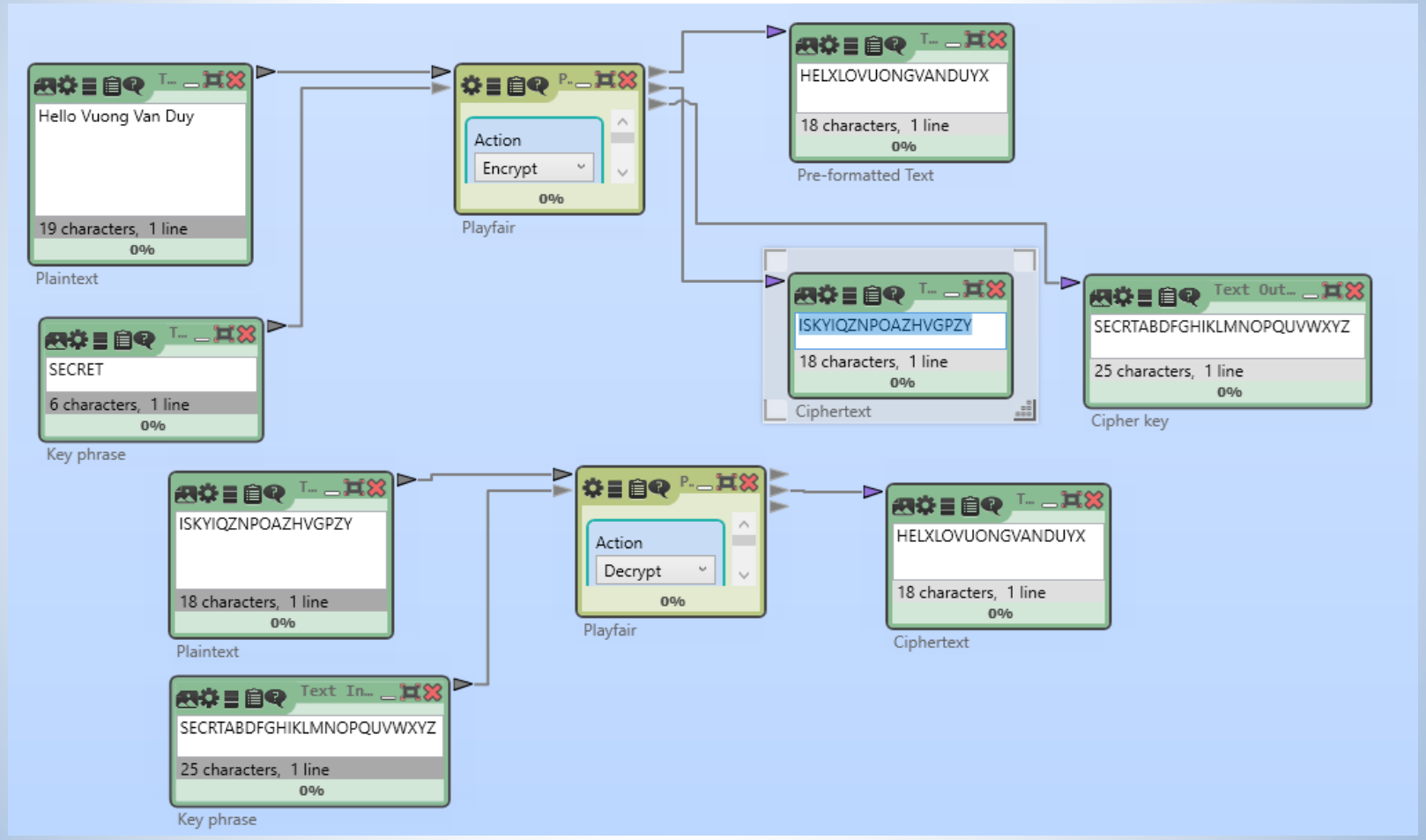


Формат для открытого текста

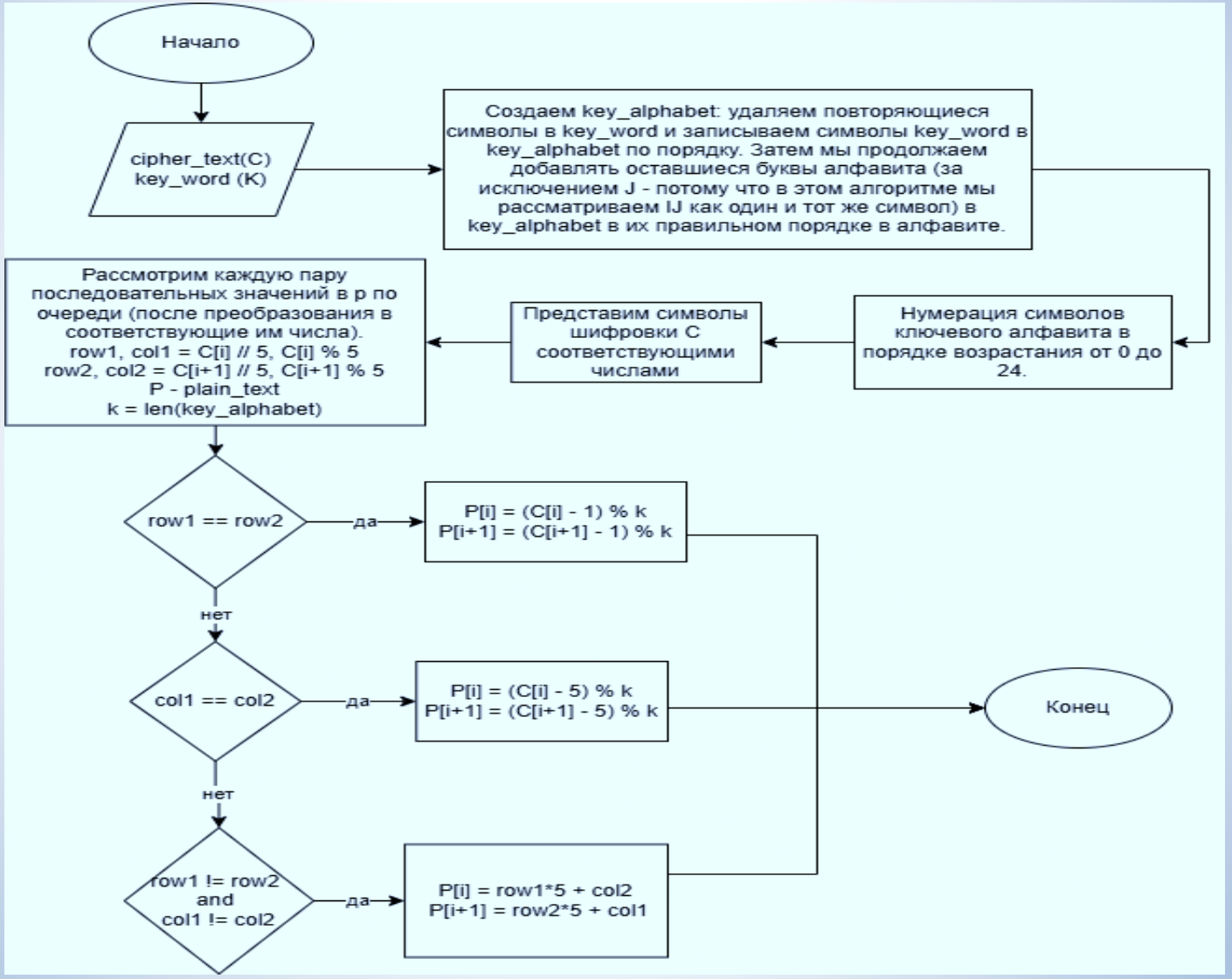


Шифровка: ISKYIQZNPOAZHVGPZY

Схему инструмента CrypTool 2 для исследования протокола зашифрования и расшифрования сообщения



Блок-схему алгоритма расшифрования сообщения



Заключение

Был исследован шифр **Rail Fence** и получены следующие выводы и характеристики:

- **Ключевые параметры:** количество строк и смещение
- **Метод шифрования:** перестановка символов по определённому узору.
- Этот шифр легко взломать. Сложность атаки грубой силы O(n) при отсутствии сдвига, O(n^2) если присутствует сдвиг, где n – длина шифротекста

Был исследован шифр **Scytale** и получены следующие выводы и характеристик:

- **Ключевые параметры:** количество граней и смещение
- **Метод шифрования:** перестановка символов в зависимости от количества граней и смещения.
- Этот шифр легко взломать. Сложность атаки грубой силы O(n) при отсутствии сдвига, O(n^2) если присутствует сдвиг, где n – длина шифротекста

Был исследован шифр **Caesar** и получены следующие выводы и характеристик:

- **Ключевые параметры:** алфавит и смещение
- **Метод шифрования:** простой метод подстановки, где каждая буква заменяется на другую в соответствии с заданным сдвигом.
- Этот шифр легко взломать. Сложность атаки грубой силы O(n), где n – мощность алфавита

Был исследован шифр **Substitution** и получены следующие выводы и характеристик:

- **Ключевые параметры:** алфавит, кодовое слово и смещение
- **Метод шифрования:** подстановка символов в соответствии с таблицей соответствий.
- Сложность атаки грубой силы O(n!), где n – мощность алфавита

Был исследован шифр **Permutation/Transposition** и получены следующие выводы и характеристик:

- **Ключевые параметры:** алфавит, пара кодовых слов
- **Метод шифрования:** перестановка символов в зависимости от заданного ключа.
- Сложность атаки грубой силы O(n!*m!), где n и m – количество строк и столбцов соответственно.

Заключение

Был исследован шифр **Vigenere** и получены следующие выводы и характеристик:

- **Ключевые параметры:** алфавит, кодовое слово
- **Метод шифрования:** это метод замены, в котором каждый символ открытого текста заменяется на другой, в зависимости от соответствующего символа в кодовом слове.
- Сложность атаки грубой силы O($\frac{n!}{(n-m)!}$), где n – мощность алфавита, m – длина ключа

Был исследован шифр **Hill** и получены следующие выводы и характеристик:

- **Ключевые параметры:** алфавит и ключ-матрица
- **Вид шифрования:** это многобуквенная подстановка, где группы символов заменяются с помощью линейных алгебраических преобразований.
- Сложность атаки грубой силы O(n^{m*m}), где n – мощность алфавита, m –размерность ключа

Был исследован шифр **ADFGVX** и получены следующие выводы и характеристик:

- **Ключевые параметры:** ключ
- **Вид шифрования:** это комбинированный метод, объединяющий подстановку и перестановку. Вначале текст шифруется по таблице, затем подвергается перестановке.
- Сложность атаки грубой силы O(36!n!), где n – длина шифротекста

Был исследован шифр **Playfair** и выявлены получены следующие выводы и характеристик:

- **Ключевые параметры:** алфавит и кодовое слово
- **Вид шифрования:** парная подстановка, где каждая пара букв заменяется в соответствии с правилами таблицы 5x5, основанной на ключевом слове.
- Сложность атаки грубой силы O(n!), где n – мощность алфавита