



КРИПТОГРАФИЯ, МАТЕМАТИЧЕСКИЕ АЛГОРИТМЫ ПРИ ШИФРОВАНИИ.

00110011

$$Y=2*X+5$$

00110011

$$Y=2*X+5$$

00110011

$$Y=2*X+5$$

00110011

$$Y=2*X+5$$

00110011

$$Y=2*X+5$$

00110011

$$Y=2*X+5$$

00110011

$$Y=2*X+5$$

00110011

$$Y=2*X+5$$

00110011

$$Y=2*X+5$$

00110011

$$Y=2*X+5$$

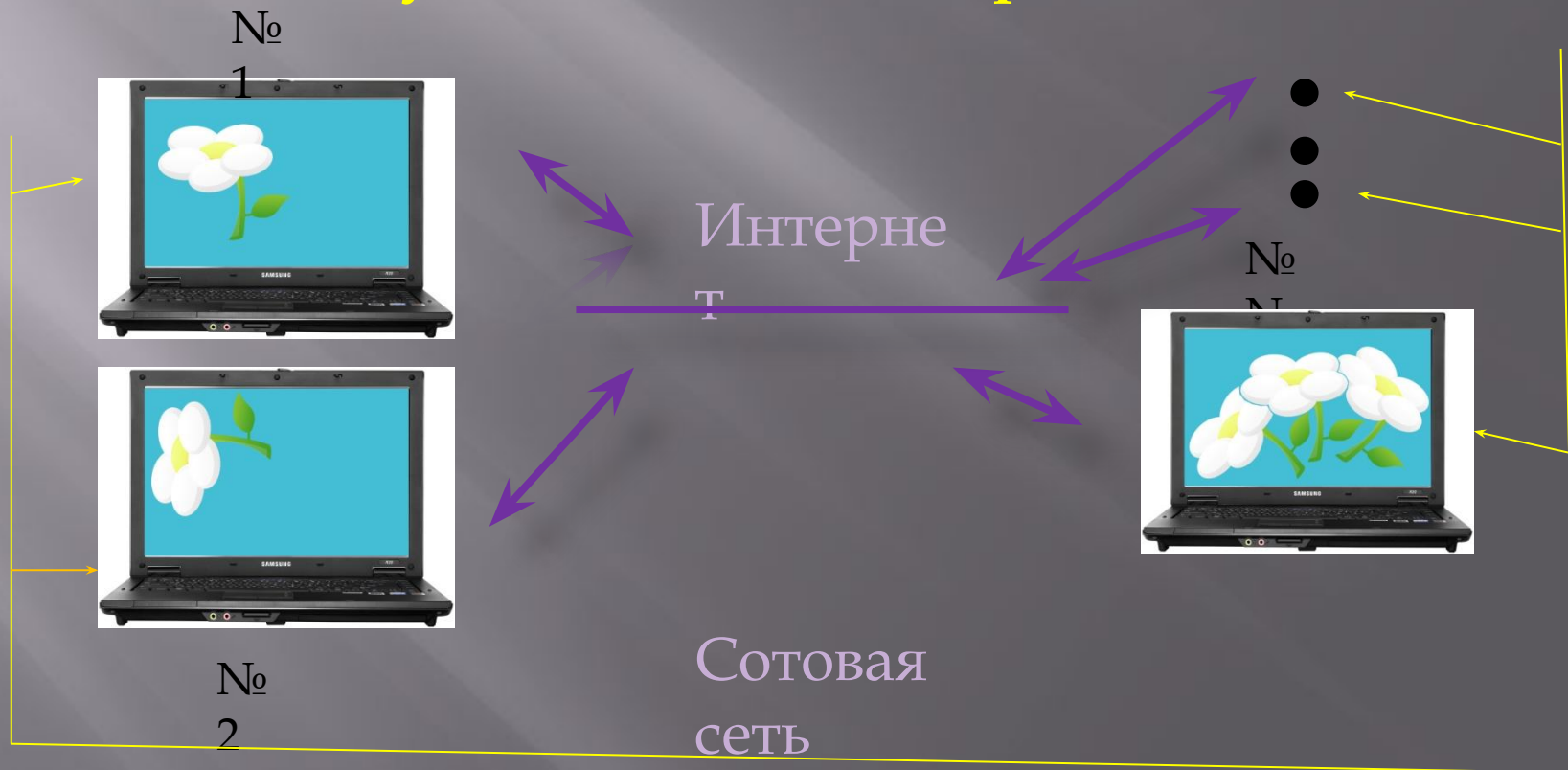
Секретность личной переписки через Интернет.



- Криптография означает тайное письмо. Все, что связано с тайной, вызывает интерес. Издавна люди изыскивали способы уберечь некоторые важные сообщения от посторонних глаз. В наше время все пользуются Интернетом. Это электронные письма, чаты, социальные сети и т.д. Представляем разработанную систему передачи зашифрованных данных через Интернет с большой степенью защиты от взлома. Программный продукт - шифровальная и дешифровальная программы на Delphi, с использованием секретного асимметричного ключа.
- Система работает с сообщениями, которые передаются через Интернет. Текст шифруется в цифры, пересылается через Интернет, а затем цифры дешифруются в текст. Сообщения для шифрования вводятся с клавиатуры. Зашифрованные сообщения могут выводиться либо на монитор, либо в файл. Зашифрованные сообщения могут вводиться, как с клавиатуры, так и из файла. Номер ключа вводится с клавиатуры. Для усложнения взлома посторонними на каждый сеанс передачи новых сообщений выбирается ключ из нескольких заданных в программе, номер выбранного ключа передается получателю сообщения по сотовой связи через СМС.

Передача шифровок через Интернет.

Для работы нашей системы нужны компьютеры подключенные к Интернету для отправки сообщений и сотовый телефон у каждого пользователя системы для получения СМС с номером ключа.



Разработка системы.

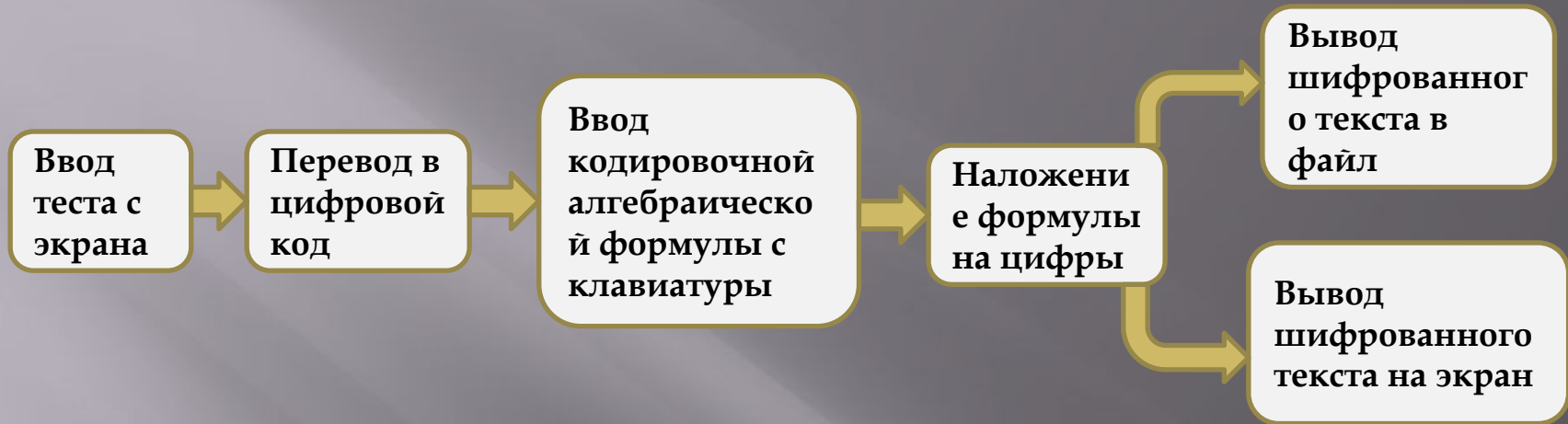
Таблица перевода сообщений в цифры.

0 - 9	7 - 2	Д - 14	К - 21	С - 28	Ш - 35	Я - 42
1 - 8	8 - 1	Е - 15	Л - 22	Т - 29	Щ - 36	Пробел - 50
2 - 7	9 - 0	Ё - 16	М - 23	У - 30	Ъ - 37	Точка - 51
3 - 6	А - 10	Ж - 17	Н - 24	Ф - 31	Ы - 38	Запятая - 52
4 - 5	Б - 11	З - 18	О - 25	Х - 32	Ь - 39	Дефис - 53
5 - 4	В - 12	И - 19	П - 26	Ц - 33	Э - 40	Точка с запятой - 54
6 - 3	Г - 13	Й - 20	Р - 27	Ч - 34	Ю - 41	Двоеточие - 55

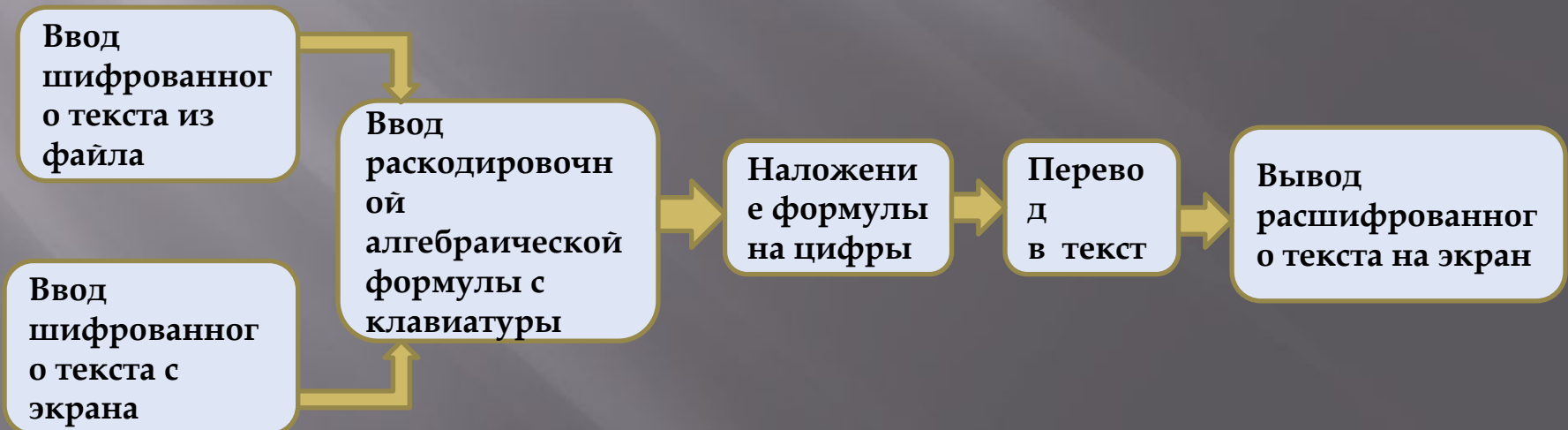
Пример ключа.

$$Y=2*X+5$$

Алгоритм шифровальной программы



Алгоритм дешифровальной программы



Проверка работы системы.

Для проверки работы системы нужно два компьютера, подключенные к Интернету и сотовый телефон у каждого пользователя для получения ключа через СМС.

Для проверки работы системы мы послали два сообщения с компьютера №1 на компьютер №2.

Первое сообщение – передача файла по электронной почте с ключом №5.

Второе сообщение - передача сообщения по социальной сети «ВКонтакте», с ключом №7 .

Ключи послали СМС с компьютера №1 (с сайта) на сотовый телефон получателя компьютера №2.

Схема проверки.

№ 2

№ 1



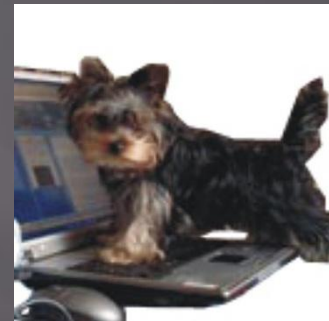
П
Р
О
Г
Р
А
М
М
А

Канал передачи данных



(Интерне
т)

П
Р
О
Г
Р
А
М
М
А



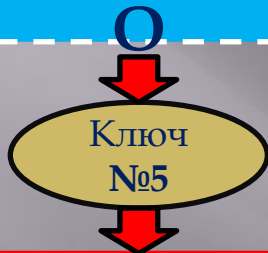
Канал передачи

ключа
(Сотовый
телефон)



1
этап

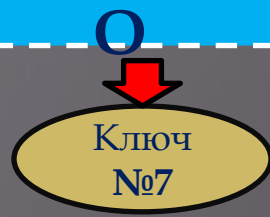
ПОРТФОЛИ



57,55,59,63,67,55,49,43,55,

2

ПОРТФОЛИ

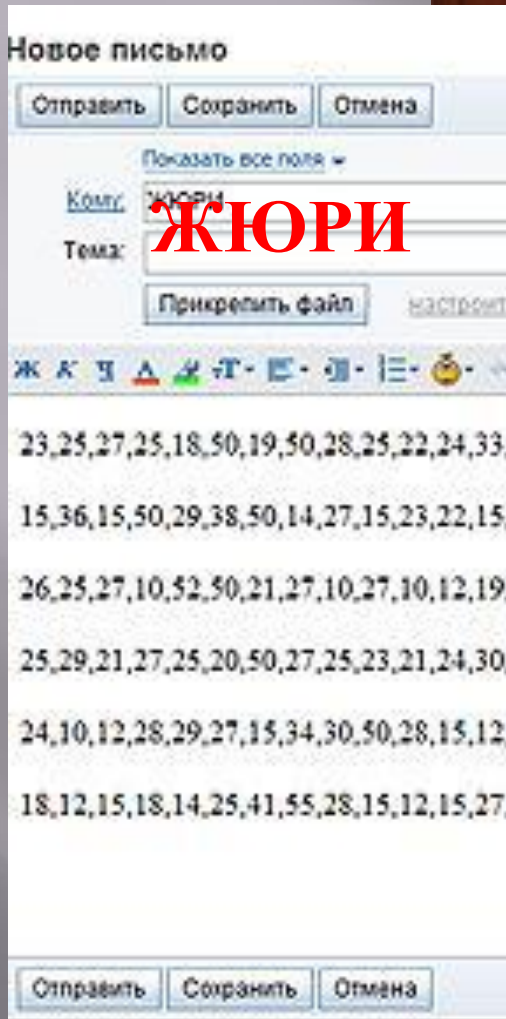


76,73,79,85,91,73,64,55,73,

Если каждый раз менять ключи , то взломать шифр будет практически не ВОЗМОЖНО.

Принцип работы системы.

О
Т
П
Р
А
В
И
Т
Е
Л
Ь
Ш
И
Ф
Р
О
В
К
И



ЖЮРИ

Жюри

Отправить SMS

Принцип работы системы.



23,25
15,36
26,25
25,29
24,10
18,12

**МОРОЗ И СОЛНЦЕ; ДЕНЬ ЧУДЕСНЫЙ!
ЕЩЕ ТЫ ДРЕМЛЕШЬ, ДРУГ ПРЕЛЕСТНЫЙ —
ПОРА, КРАСАВИЦА, ПРОСНИСЬ:
ОТКРОЙ СОМКНУТЫ НЕГОЙ ВЗОРЫ
НАВСТРЕЧУ СЕВЕРНОЙ АВРОРЫ,
ЗВЕЗДОЮ СЕВЕРА ЯВИСЬ!**

53



П
О
Л
У
Ч
А
Т
Е
Л
Ь

Ш
И
Ф
Р
О
В
К
И

Издательство

«1 сентября»

Спасибо за внимание

Конкурс

«Портфолио»