Министерство образования Республики Беларусь

Учреждение образования

«Полоцкий государственный университет»

Ю.Ф. Пастухов, Д.Ф. Пастухов, М.Б. Мередова

ДИНАМИЧЕСКОЕ КОДИРОВАНИЕ.

Учебное пособие к лекционным и практическим занятиям

для студентов специальности

1-98 01 01 Компьютерная безопасность

Новополоцк
ПГУ
2019

УДК 519.72
Рецензенты:
А.А. Козлов, кандидат физико-математических наук, доцент, заведующий кафедрой Высшей математики и дифференциальных уравнений Полоцкого государственного университета;
Р.П. Богуш, кандидат технических наук, доцент, заведующий кафедрой Вычислительных систем и сетей;
О.Н. Петрович, кандидат технических наук, доцент, заведующий кафедрой Технологий программирования;
О.В. Голубева, кандидат физико-математических наук, доцент, декан факультета информационных технологий;
С.Г. Ехилевский, доктор технических наук, профессор кафедры Технологий программирования.
А.Ф. Оськин, кандидат технических наук, доцент, кафедры Технологий программирования.

Пастухов Ю.Ф., Пастухов Д.Ф.,М.Б. Мередова
Динамическое кодирование /Ю.Ф. Пастухов, Д.Ф. Пастухов, М.Б.Мередова.- Новополоцк: ПГУ,2019. - 19 с.

В учебном пособии описан метод динамического кодирования.
Для студентов программистов 98 01 01
(компьютерная безопасность).
Для студентов университетов, педагогических вузов, технических вузов, преподавателей, инженеров, программистов использующих в своей практической деятельности математические методы шифрования.

Одобрено и рекомендовано к изданию
методической комиссией факультета информационных технологий
В качестве учебного пособия

Кафедра технологий программирования

Предисловие

Предлагаемое учебное пособие создано на основе работы авторов со студентами - дипломниками 4 курса специальности Компьютерная безопасность 98 01 01 (математические методы и программные системы) в Полоцком государственном университете.

Динамическое кодирование использует свойства кольца вычетов по модулю m Z_m

Смоделирован генератор псевдослучайных чисел(п.с.ч.) со значениями В кольце вычетов по модулю m Z_m , и на этой основе построен динамически меняющийся шифр. Известные системы шифрования имеют существенный недостаток –дефект статичности. Дефект статичности определяется как одинаковый результат шифрования любого конечного числа раз фиксированного сообщения, что облегчает исследование статистических закономерностей и сокращает время криптографического анализа. Конечно, использование данного метода позволяет устранить этот недостаток в известных старых системах типа DES,AES,RSA и т.д., придав им новый импульс реализации их возможностей, используя комбинированное(гибридное) шифрование.

Генератор динамически меняющегося шифра фиксированное сообщение каждый раз кодирует иначе ,в результате чего становится труднее изучать его статистические характеристики, создавая трудности при изучении его статистических инвариантов. В программе реализована постановка пакета помех случайной длины от 0 до заданного значения, который встраивается между символами, кодируемого сообщения Можно реализовать случайный выбор генераторов и случайной размер пакета, следующих подряд передаваемых зашифрованных символов при реализации данной системы. Дана точная математическая постановка и решения проблемы. В данной работе предложен вариант решения этой задачи. Система реализована на языке Visual Fortran.

Пастухов Ю.Ф., Пастухов Д.Ф.

Динамическое кодирование.

Цели работы

1.Создание метода шифрования, лишенного дефекта статичности (динамически меняющийся).
Дефектом статичности является одинаковый результат шифрования любого конечного числа раз фиксированного сообщения, упрощает изучение статистических характеристик алгоритма шифрования и сокращает время криптоанализа.

Для реализации динамически меняющегося шифра использовались специально сконструированные генераторы последовательностей псевдослучайных чисел с равномерным распределением в области их значений – кольце вычетов по модулю m Z_m.

2.Создание графического интерфейса для работы
с данным методом шифрования.

Графический интерфейс поддерживает следующие функции:

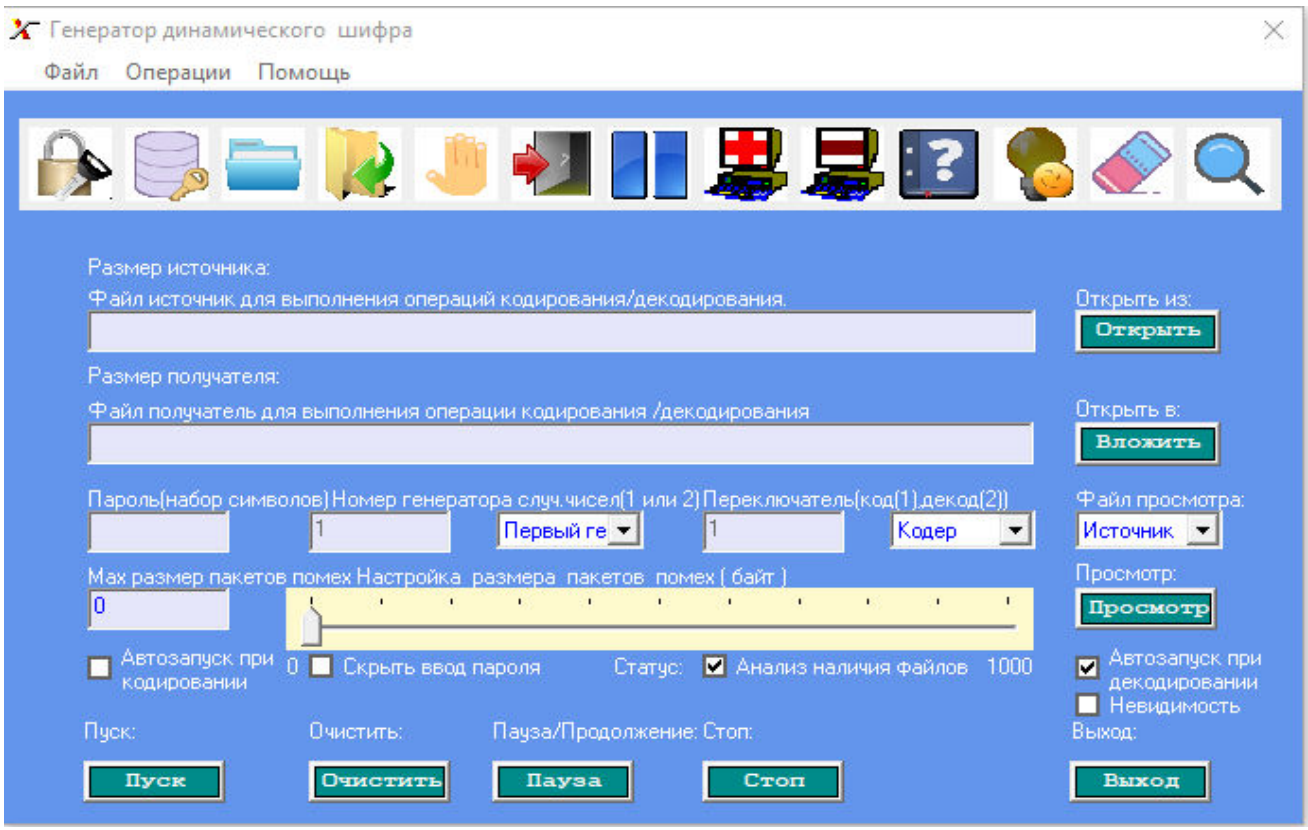
Выбор ввода информации через файл.
Выбор вывода информации через файл.

ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Для решения этой задачи был использован язык программирования Fortran

Интерфейс пользователя

Интерфейс пользователя включает в себя следующие окна - окно выбора файла для кодирования, окно выбора файла для кодирования и декодирования , сохранения зашифрованной информации ,инкремент и декремент размера пакета помех , scrollbar для быстрого изменения размера пакета помех , кнопка перехода в скрытый режим, падающие список, выбор генератора псевдослучайных чисел , падающие список выбора файла просмотра (источник ,получатель) , кнопка открытия файла источника и открытия файла преобразованных (кодирования, декодирования) данных(получатель), редактируемое окно для ввода пароля .



Интерфейс пользователя

Содержит:

- **Панель управления**
- **Меню**
- **кнопки выбора файла для кодирования и декодирования,сохранения зашифрованной информации**
- **инкремент и декремент размера пакета помех**
- **scrollbar для быстрого изменения размера пакета помех**
- **кнопка перехода в скрытый режим**
- **падающие список выбора генератора псевдослучайных чисел**
- **падающие список выбора файла просмотра (источник, цель)**
- **редактируемые окна для ввода пароля, путей для открытия и сохранения данных и другие элементы.**
- **Все вышеописанные операции продублированы в меню, панели инструментов реализованы в виде комбинации горячих клавиш. Для удобства ознакомления с работой программы в панели инструментов предусмотрены всплывающие подсказки.**

Принцип построения генератора п.с.ч. в кольце вычетов Zm

$G: X \times N \to X \subset \Re$ **-генератор п.с.ч. на X**

$G(x_0, n) = g_n(x_0): N \to X$ **- значения генератора на** X **с начальной настроечной точкой** $x_0 \in X$ A **-алфавит ,** $|A| = m \in N$

$$G_m(x_0,n) = \begin{cases} \text{int}(m \cdot G(x_0,n)), & X = [0;1) \\ \text{mod}(G(x_0,n),m), & X = N, Z \\ \text{int}(\text{mod}(G(x_0,n),m)), & X = \Re \end{cases} \Rightarrow 0 \le G_m(x_0,n) \in Z_+,\ G_m(x_0,n) < m \Rightarrow G_m(x_0,n) \in Z_m$$

$G_m: X \times N \to Z_m$, $G_m(x_0,n) = g_{x0_m}(n): N \to Z_m$ **-значения генератора в кольце вычетов** Z_m **с начальной настроечной точкой** $x_0 \in X$

Принцип построения динамически-меняющегося шифра на основе генератора п.с.ч. в кольце вычетов Zm

$T: Z_m \to A$ - биективное отображение - кодовая таблица алфавита A : $T(i) = a_i \in A, i \in Z_m$

$T^{-1}: A \to Z_m$ -обратное отображение к кодовой таблице $T: Z_m \to A$ (T-table) .

$S_k: (Z_m)^k \to A^k$ - сообщение длины k на A $S_k(i_1, i_2, ..., i_k) = a_{i_1} a_{i_2} ... a_{i_k}$ $a_{i_{nk}} \in A$ $n \in \overline{1,k}$

$G_m: X \times N \to Z_m$, $G_m(x_0,n) = g_{x0_m}(n): N \to Z_m$ - генератор п.с.ч. в кольце вычетов Z_m с начальной настроечной точкой $x_0 \in X$

Кодирование: $F = K \circ (T^{-1} + G_m(x_0,n)): A \times N \to A$

$F(a_{i_n}) = \overline{a_{i_n}} = T(T^{-1}(a_{i_n}) + G_m(x_0,n)) \in A$, $T^{-1}(a_{i_n}), G_m(x_0,n) \in Z_m \Rightarrow T^{-1}(a_{i_n}) + G_m(x_0,n) \in Z_m$

Декодирование(обратное преобразование): $F = T \circ (T^{-1} - G_m(x_0,n)): A \times N \to A$

$a_{i_n} = F^{-1}(\overline{a_{i_n}}) = T(T^{-1}(\overline{a_{i_n}}) - G_m(x_0,n)) \in A$, $T^{-1}(\overline{a_{i_n}}), G_m(x_0,n) \in Z_m \Rightarrow T^{-1}(\overline{a_{i_n}}) - G_m(x_0,n) \in Z_m$

Влияние(действие) ключа на процесс шифрования данных.

Пусть K - множество(пространство) ключей, $k \in K$ - ключ

Действием пространства ключей K на множество X называется однопараметрическое семейство отображений $A: K \times X \to X$ такое что

$\forall k \in K \ \ A_k : X \to X$ -изоморфизм, называемый действие ключа $k \in K$ на X: $A_k(x) = A(k,x)$

В частности ,если X -кольцо, и $K = X$,то $A_k(x) = A(k,x) = k + x \in X$ -изоморфизм

Тогда ключ $k \in K$ следующим образом влияет на преобразование данных:

Кодирование: $F(a_{i_n}) = \overline{a_{i_n}} = T(T^{-1}(a_{i_n}) + G_m(A_k(x_0), n)) \in A$

Декодирование: $a_{i_-} = F^{-1}(\overline{a_{i_-}}) = T(T^{-1}(\overline{a_{i_-}}) - G_m(A_k(x_0), n)) \in A$

Оценка мощности пространства ключей

Для 4-хбайтовых действительных генераторов

$|K| \approx 10^{38+7} = 10^{45} = (10^3)^{15} = (1000)^{15} \approx (1024)^{15} = (2^{10})^{15} = 2^{150}$ то есть длина ключа 150 бит

Более точная оценка $|K| \approx 10^{38+7} = 10^{45} = 2^{45\log_2 10} \approx 2^{45\frac{\log_{10} 10}{\log_{10} 2}} = 2^{45\frac{1}{\log_{10} 2}} \approx 2^{149.5}$

Для 8-хбайтовых действительных генераторов(с двойной точностью)

$|K| \approx 10^{308+16} = 10^{324} = (10^3)^{108} = (1000)^{108} \approx (1024)^{108} = (2^{10})^{108} = 2^{1080}$ то есть длина ключа 1080 бит.

Более точная оценка $|K| \approx 10^{308+16} = 10^{324} = 2^{324\log_2 10} \approx 2^{324\frac{\log_{10} 10}{\log_{10} 2}} = 2^{324\frac{1}{\log_{10} 2}} \approx 2^{1076,3}$

Для 16-ибайтовых действительных генераторов(с четверной точностью)

$|K| \approx 10^{4932+33} = 10^{4965} = (10^3)^{1655} = (1000)^{1655} \approx (1024)^{1655} = (2^{10})^{1655} = 2^{16550}$ то есть длина ключа

более16500 бит. Точнее $|K| \approx 10^{4932+33} = 10^{4965} = 2^{4965\log_2 10} \approx 2^{4965\frac{\log_{10} 10}{\log_{10} 2}} = 2^{4965\frac{1}{\log_{10} 2}} \approx 2^{16493,4}$

Таким образом, данный алгоритм конкурентоспособен.

Диаграмма преобразования данных

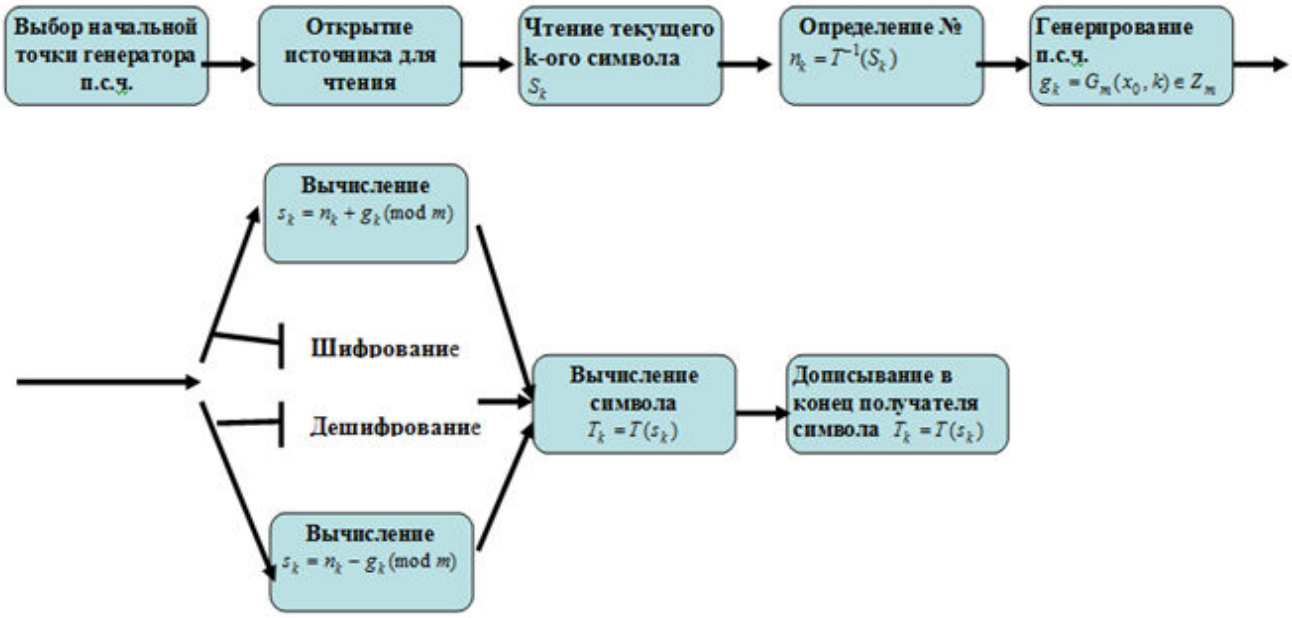


Диаграмма вариантов использования

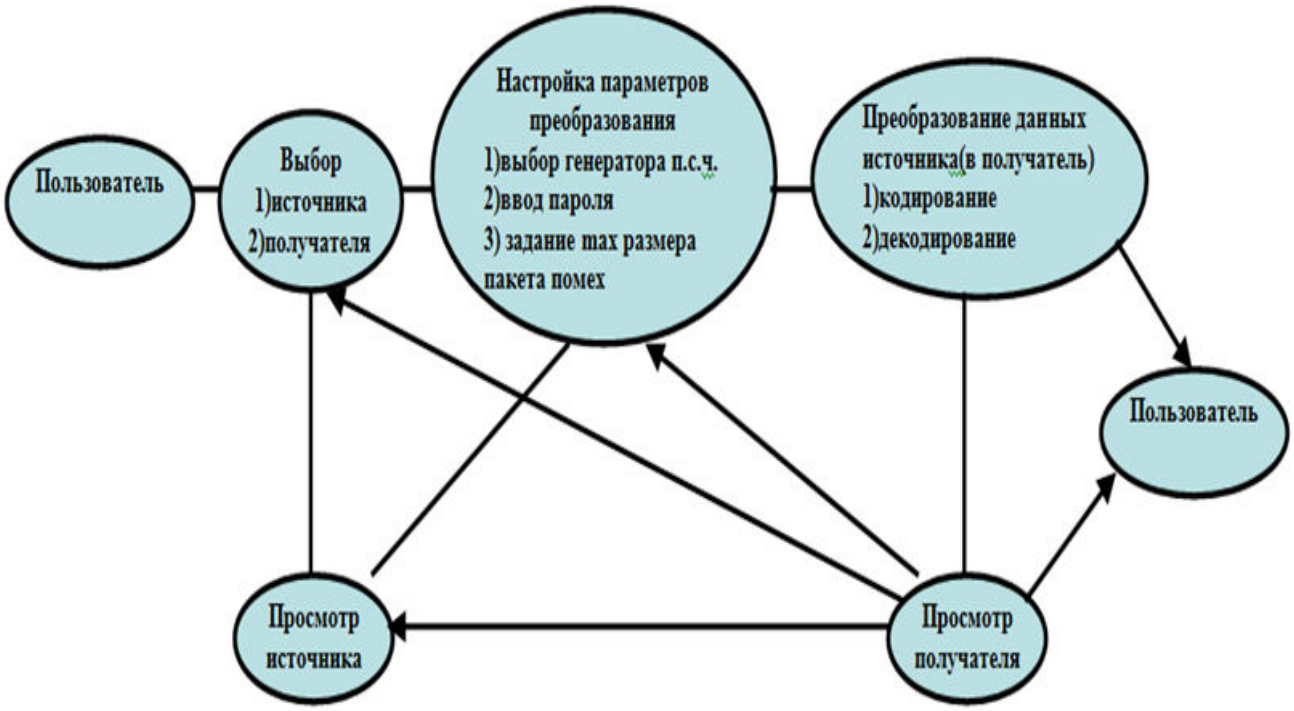
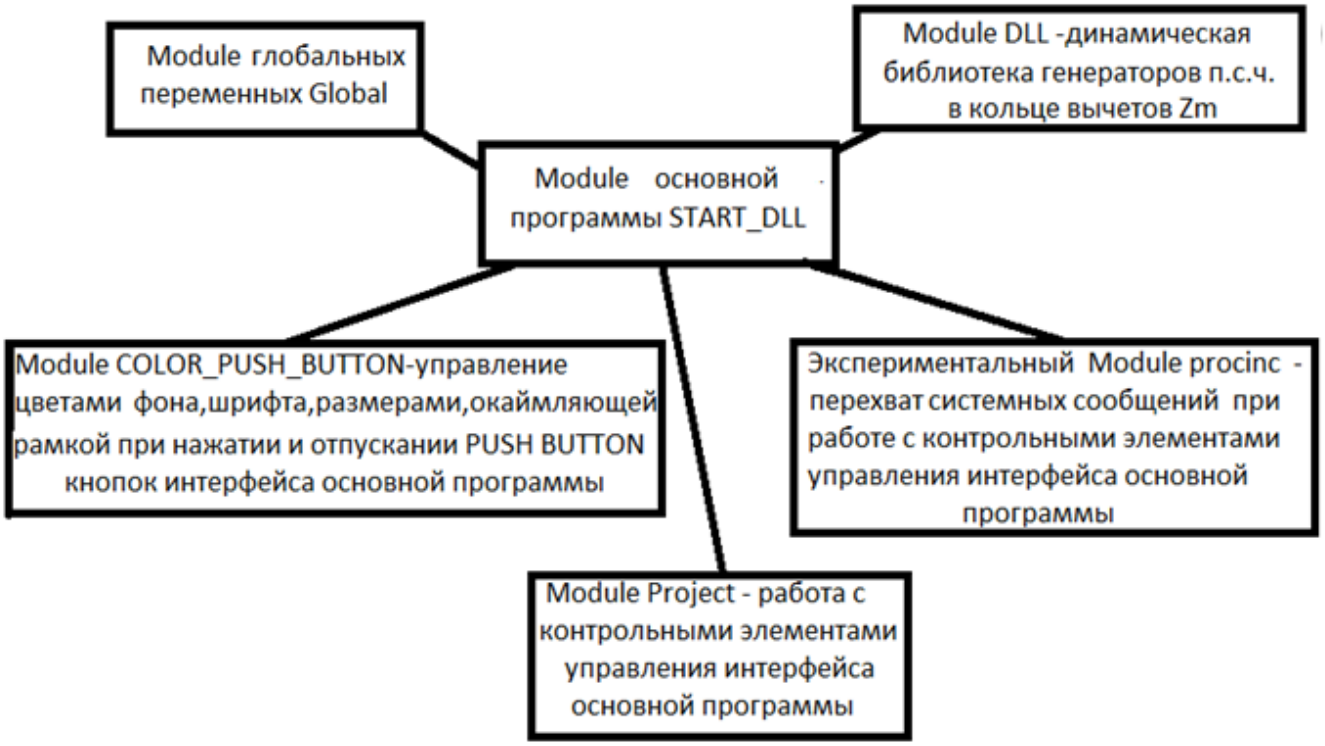
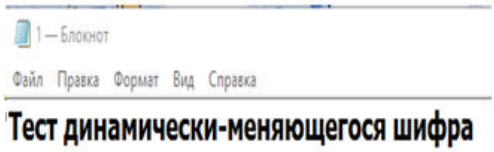


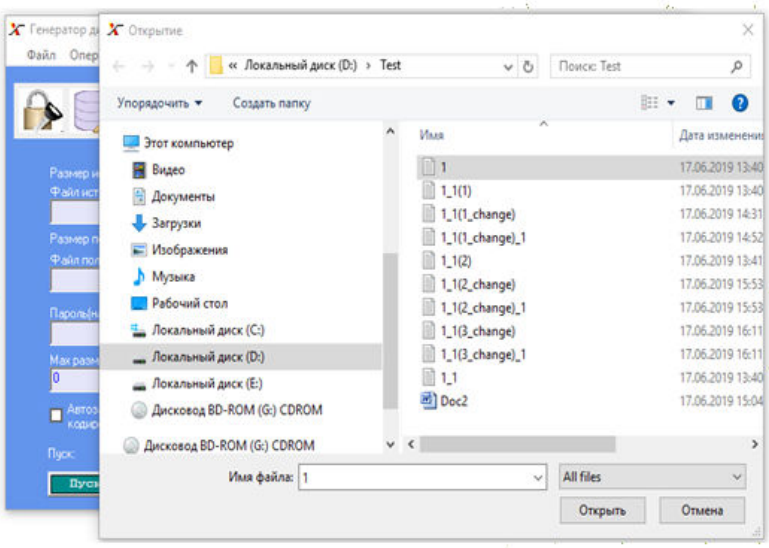
Диаграмма модулей



Шифрование данных.

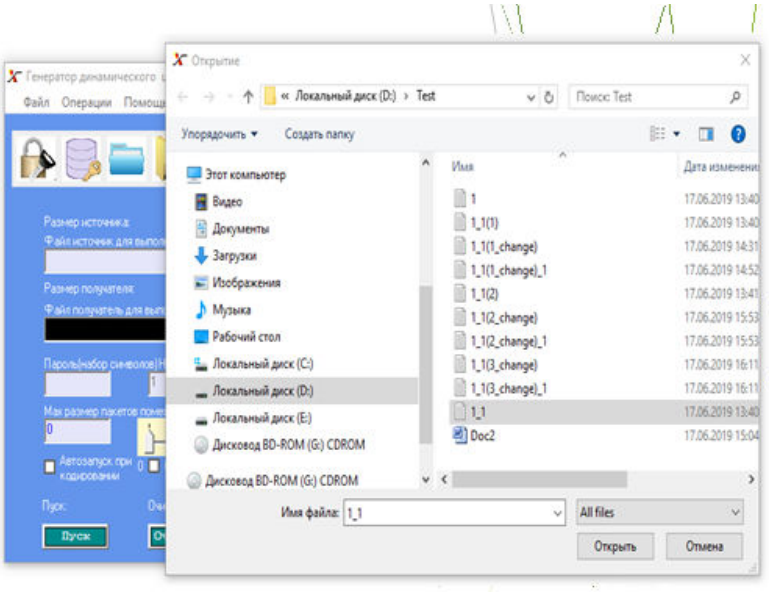
Для шифрования можно использовать любые типы файлов. В качестве примера используем файл 1.txt
с содержимым:





Дешифрование данных.

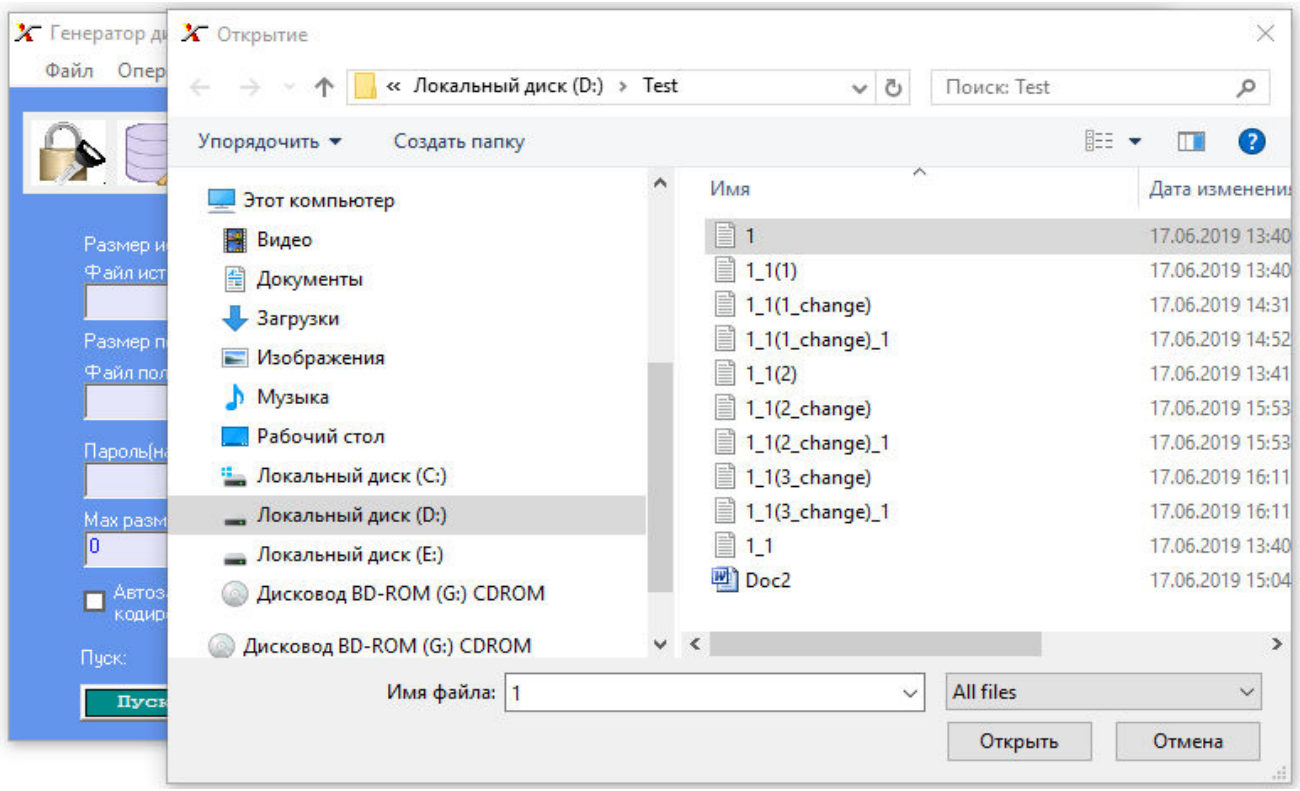
Для декодирования данных необходимо открыть шифрованный файл
1_1.txt. На рисунке отражен процесс декодирования данных.



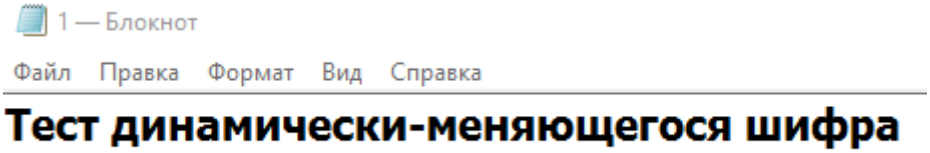
3 ШИФРОВАНИЕ, ДЕШИФРОВАНИЕ И ТЕСТИРОВАНИЕ

3.1 Примеры шифрования данных

Для тестирования шифрования можно использовать любые типы файлов. В качестве примера используем файл 1.txt. Результат ввода данных приведен на рисунке.



С содержимым :



Результат шифрования :

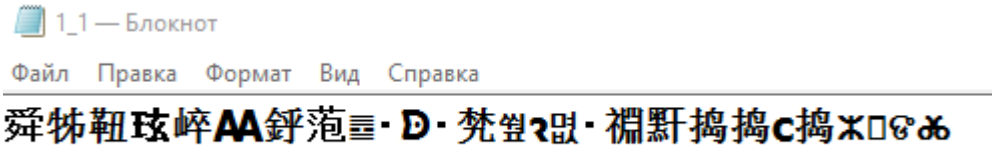
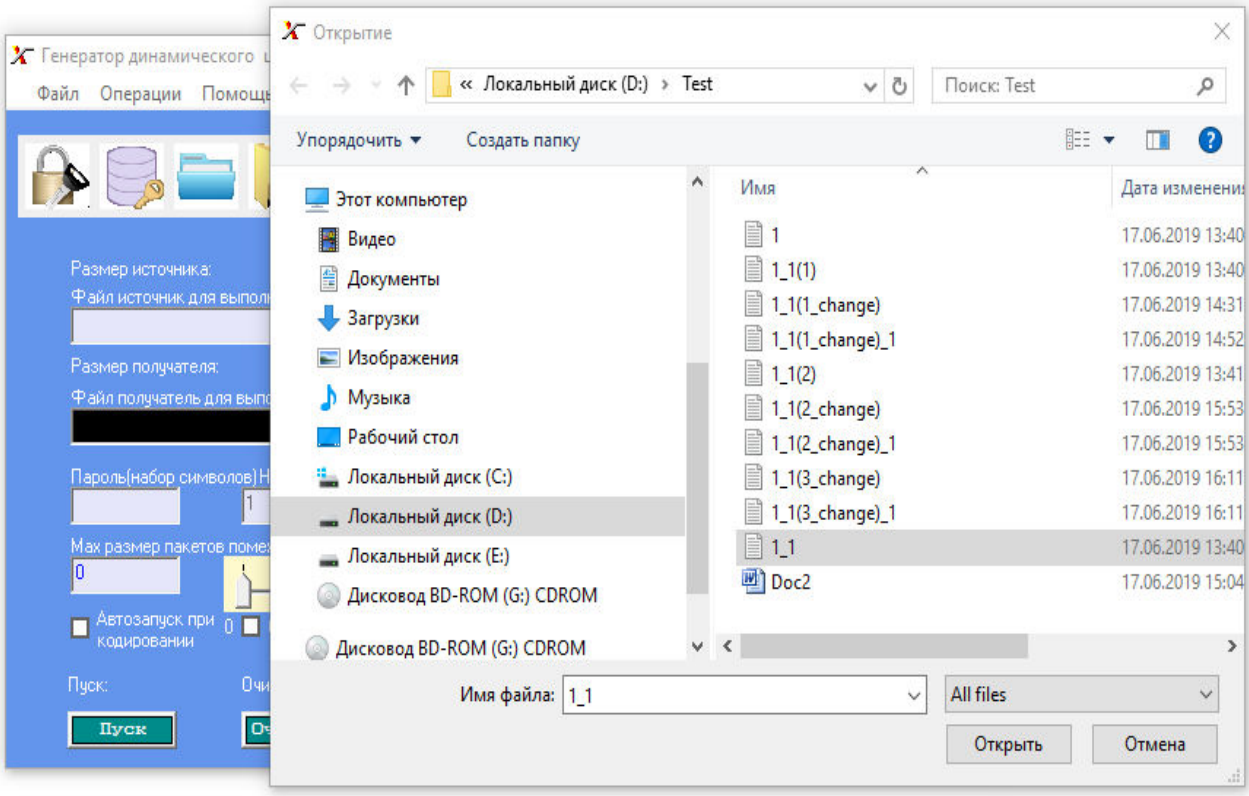


Рисунок 4 – Шифрование данных

Примеры дешифрования данных

Для расшифровки данных необходимо выбрать файл, в котором находится зашифрованные данные. На рисунке изображен процесс декодирования данных.



Пример шифрования и дешифрования. На рисунке представлен шифр записанный в файл 1_1.txt. Начальная точка генератора последовательностей псевдослучайных чисел меняется при каждом шифровании, в результате чего коды одного и того же сообщения отличаются, но декодируются они одинаково.

Исходный текст:
Тест динамически-меняющегося шифра

Кодированный текст:
1 тест) ·4≒狗○▯籙쉜♀滉譒傘⑮▯灌↓課眏悚▯掬掬c掬ж□▯(

2 тест) ɕ˷+ꟾ鴉¸㗊ˀ窒丰ṙ専黴用○ϲ⎵갭饉矓掬掬c掬ж□▯▯

Декодированный текст:
Тест динамически-меняющегося шифра

Тестирование с изменением пароля при декодировании:

Исходный текст:

Тест динамически-меняющегося шифра

Кодированный текст с апролем 0:

□4 ≒ 狗○▯薇剴漶譒傘㊺□ 灌↓課眏悚▯搗搗c搗ж○̊□ □

Декодированный текст :

Тест динамически-меняющегося шифра

Декодированнный текст с паролем 1:

Т°хЊЋ-В/Я№▯ “Вчф}ЧА‰Њуш

Тестирование с добавлением 1 символа:

Исходный текст:

Тест динамически-меняющегося шифра

Кодированный текст:

□4 ≒ 狗○▯薇剴漶譒傘㊺□ 灌↓課眏悚▯搗搗c搗ж○̊□ □

Кодированный текст с добавлением 1 символа:

□4 ≒ 狗○▯薇剴漶譒傘㊺&□ 灌↓課眏悚▯搗搗c搗ж○̊□ □

Декодированный текст:

Тест динамически-меняющегося шифра

Декодированнный текст с добавлением 1 символа:

р…е[1]ВсќѓЕјОU^х±F‰ЬС№9ЧДЛЏ†Ц,Ъ l%4нЊАiШЯ

Тестирование с удалением 1 символа:

Исходный текст:

Тест динамически-меняющегося шифра

Кодированный текст:

▫4 ≒ 狗◌▯薇剴瀧譒傘㊺▫ 灌↓課睞悚▯搗搗c搗ж◌̊▫ ▫

Кодированный текст с удалением 1 символа:

▫4 ≒ 狗◌▯薇剴瀧譒傘㊺▫ 灌↓課悚▯搗搗c搗ж◌̊▫ ▫

Декодированный текст:

Тест динамически-меняющегося шифра

Декодированнный текст с удалением 1 символа:

р…е[1]ВсќѓЕjОU^х±F‰ЬС№9ЧД~щ=©•ЯЛ

Тестирование с заменой 1 символа:

Исходный текст:

Тест динамически-меняющегося шифра

Кодированный текст:

▫4 ≒ 狗◌▯薇剴瀧譒傘㊺▫ 灌↓課睞悚▯搗搗c搗ж◌̊▫ ▫

Кодированный текст с заменой 1 символа:

▫4 ≒ 狗◌▯薇剴瀧譒傘!▫ 灌↓課睞悚▯搗搗c搗ж◌̊▫ ▫

Декодированный текст:

Тест динамически-меняющегося шифра

Декодированнный текст с удалением 1 символа:

р…е[1]ВсќѓЕjОU^х±F‰ЬС№9ЧД~щ=©•ЯЛ

Комбинированное тестирование с добавлением, удалением, заменой 2-х символов:

Исходный текст:

Тест динамически меняющегося шифра

Кодированный текст:

□4 ≒ 狗◌▯黴剴澁譒傘㊺□ 灌↓課眏悚▯搗搗c搗ж◌̊□ □

Кодированный текст с добавлением,удалением,заменой 2 символов:

1234◌▯黴剴澁譒傘㊺□ 灌↓課眏悚▯搗搗c搗ж◌̊□ □

Декодированный текст:

Тест динамически-меняющегося шифра

Декодированнный текст с комбинированным изменением:

□□숀㼝폠캄幕ㄴ樸텐뤓ӎ̓◌ᆨ顾熚闐畾鏥≣炊

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. FORTRAN & WIN32 API. Создание программного интерфейса для Windows средствами современного Фортрана — В. В. Штыков
2. Современный Fortran на практике
Автор: Маркус Арьен Издательство: ДМК Пресс
3. CUDA Fortran для ученых и инженеров: Рекомендации по эффективному программированию на языке CUDA Fortran
Автор: Рутш Грегори Издательство: ДМК Пресс
4. Программирование Windows-приложений на языке Fortran: элементы управления и графика Windows
Автор: Васильченко В.В. Издательство: Диалог-МИФИ
5. Современный Фортран
Автор: Рыжиков Ю.И.Жанр: FortranИздательство: Корона-Век Год: 2007
6. Фортран в задачах и примерах
Автор: Немнюгин С.А. Издательство: БХВ-Петербург
7. Программирование на Visual Fortran
Автор: Алгазин С.Д. Издательство: Диалог-МИФИ Год: 2008
8. Пастухов Д.Ф.,Пастухов Ю.Ф., Смоляк А.И. Шифрование гиперболическими ункциями(http://elib.psu.by:8080/handle/123456789/22089).
9. Пастухов Д.Ф., Пастухов Ю.Ф., Синица П.Р. Шифрование данных на базе эллиптических кривых: учебно-методическое пособие для студентов спец.1-98 01 01(http://elib.psu.by:8080/handle/123456789/16814).
10. Пастухов Д.Ф., Пастухов Ю.Ф., И.С. Глебко Полиномиальное кодирование /Д.Ф. Пастухов, Ю.Ф. Пастухов, И.С.Глебко.- Новополоцк: ПГУ,2019. - 23 с.
11. Пастухов Д.Ф., Пастухов Ю.Ф.,Сонич А.Д., Ченторицкий А.Ю. Обобщение метода шифрования Владимира Сизова на случай произвольных периодических и апериодических функций: учебное пособие /Д.Ф. Пастухов, Ю.Ф. Пастухов, Сонич А.Д., Ченторицкий А.Ю.- Новополоцк: ПГУ,2019. - 15с.

УДК 519.72

Кандидат физико-математических наук Юрий Пастухов Феликсович

Кандидат физико-математических наук Пастухов Дмитрий Феликсович

Мередова Маягозель Бяшимовна

Полоцкий государственный университет

2019