

ОТЧЁТ
ПО ПРАКТИКЕ
на тему

“Шифрование и дешифрование матрицы с использованием ключа.”

Руководитель:
Милинчук М.А.
Атурина В.А.

Разработал:
Болсуновский В.Н

ВВЕДЕНИЕ

Вовремя прохождения практики были рассмотрены следующие этапы:

1. Постановка цели и задач.
2. Формулирование шагов к созданию.
3. Выбор механизма шифрования.
4. Проектирование модели разработки.
5. Производство реализации продукта.
6. Выполнения тестирования продукта.
7. Совершенная отладка продукта.

Цели и задачи

Целью практики является разработать систему шифрования удовлетворяющую следующим требованиям:

1. Шифрование и дешифрование выполнять с использованием ключа.
2. Задача должна быть реализована как законченное приложение со скрытыми формулами и открытыми полями ввода.
3. При реализации учитывать особенности ввода данных так чтобы избежать переполнения или ошибок ввода.

Для реализации поставленной цели были выявлены следующие задачи:

1. Освоение первичных навыков программирования.
2. Провести исследовательскую работу через создания приложения.

Шаги к созданию

Шифрование - процесс, который преобразует сообщение в нечитаемую форму для всех кроме того, кто знает, как расшифровать его обратно в Читаемую форму.

Дешифрование - получение открытых данных по зашифрованным в условиях, когда алгоритм расшифрования и его секретные параметры не являются полностью известными и расшифрование не может быть выполнено обычным путем.

ВЫБОР МЕХАНИЗМА ШИФРОВАНИЯ

После проведения анализа методов шифрования были выявлены два

наиболее подходящих методов шифрования для реализации программного продукта. Выбор был сделан для удовлетворения следующих критерий:

1. Шифрование и дешифрование выполнять с использованием ключа.
2. Задача должна быть реализована как законченное приложение со скрытыми формулами и открытыми полями ввода.

Шифр Цезаря

Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в

открытом тексте заменяется символом, находящимся на некотором постоянном

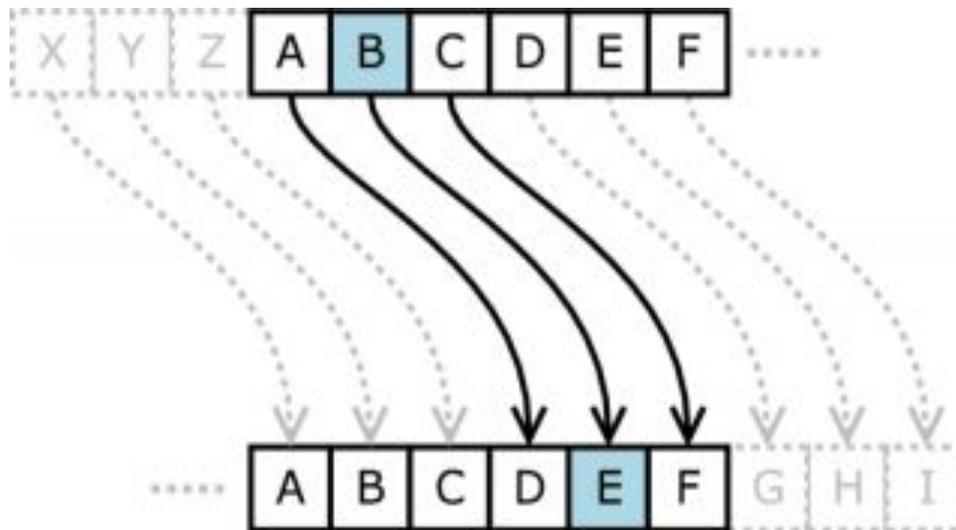
числе позиций левее или правее него в алфавите. Например, в шифре со

сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр

назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шифр Цезаря



Гай Юлий Цезарь



Реализация

Реализация продукта происходит с помощью Microsoft Excel, так как он позволяет легко выполнить поставленную задачу используя базовые знания программирования.

В реализации я использовал следующие формулы:

=ИНДЕКС

=ПОИСКПОЗ

=ПСТР

=ПРОПИСН

И другие

Тестирование и отладка

Цель тестирования – обнаружить ситуацию, когда результаты работы программы не соответствуют входным данным. Существует два подхода к формулированию критериев полноты тестирования: критерии «черного ящика» и критерии «белого ящика». Критерии черного ящика описывают тестирование с точки зрения поставленной задачи внутреннего устройства программы. Критерии белого ящика учитывают структуры программы. И как раз-таки этим методом, белого ящика, я воспользовалась. При тестировании продукта проблема возникла при незаполненном поле буквенного ключа пользователем. Для устранения неполадки было создано дополнительное поле буквенного ключа, которое само заполнит пустые клетки, оставленные пользователем при помощи функции ЕСЛИ.

Болсуновский Валерий Николаевич	31
БОЛСУНОВСКИЙ ВАЛЕРИЙ НИКОЛАЕВИЧ	5

31
Ёурцштужцпноджерйхнодтнпурейжнь
Ёурцштужцпноджерйхнодтнпурейжнь

31
БОЛСУНОВСКИЙ ВАЛЕРИЙ НИКОЛАЕВИЧ

1 Б	5	10 Ё	Ё
2 О	19	24 У	ЁУ
3 Л	16	21 Р	ЁУР
4 С	22	27 Ц	ЁУРЦ
5 У	24	29 Ш	ЁУРЦШ
6 Н	18	23 Т	ЁУРЦШТ
7 О	19	24 У	ЁУРЦШТУ
8 В	6	11 Ж	ЁУРЦШТУЖ
9 С	22	27 Ц	ЁУРЦШТУЖЦ
10 К	15	20 П	ЁУРЦШТУЖЦП
11 И	13	18 Н	ЁУРЦШТУЖЦПН
12 Ё	14	19 О	ЁУРЦШТУЖЦПНО
13	3	8 Д	ЁУРЦШТУЖЦПНОД
14 В	6	11 Ж	ЁУРЦШТУЖЦПНОДЖ
15 А	4	9 Е	ЁУРЦШТУЖЦПНОДЖЕ
16 Л	16	21 Р	ЁУРЦШТУЖЦПНОДЖЕР
17 Е	9	14 Й	ЁУРЦШТУЖЦПНОДЖЕРЙ
18 Р	21	26 Х	ЁУРЦШТУЖЦПНОДЖЕРЙХ
19 И	13	18 Н	ЁУРЦШТУЖЦПНОДЖЕРЙХН
20 Ё	14	19 О	ЁУРЦШТУЖЦПНОДЖЕРЙХНО
21	3	8 Д	ЁУРЦШТУЖЦПНОДЖЕРЙХНОД
22 Н	18	23 Т	ЁУРЦШТУЖЦПНОДЖЕРЙХНОДТ
23 И	13	18 Н	ЁУРЦШТУЖЦПНОДЖЕРЙХНОДТН
24 К	15	20 П	ЁУРЦШТУЖЦПНОДЖЕРЙХНОДТНП
25 О	19	24 У	ЁУРЦШТУЖЦПНОДЖЕРЙХНОДТНПУ
26 Л	16	21 Р	ЁУРЦШТУЖЦПНОДЖЕРЙХНОДТНПУР
27 А	4	9 Е	ЁУРЦШТУЖЦПНОДЖЕРЙХНОДТНПУРЕ
28 Е	9	14 Й	ЁУРЦШТУЖЦПНОДЖЕРЙХНОДТНПУРЕЙ
29 В	6	11 Ж	ЁУРЦШТУЖЦПНОДЖЕРЙХНОДТНПУРЕЙЖ
30 И	13	18 Н	ЁУРЦШТУЖЦПНОДЖЕРЙХНОДТНПУРЕЙЖН
31 Ч	28	33 Ъ	ЁУРЦШТУЖЦПНОДЖЕРЙХНОДТНПУРЕЙЖНЪ

1 Ё	10	5 Б	Б
2 У	24	19 О	БО
3 Р	21	16 Л	БОЛ
4 Ц	27	22 С	БОЛС
5 Ш	29	24 У	БОЛСУ
6 Т	23	18 Н	БОЛСУН
7 У	24	19 О	БОЛСУНО
8 Ж	11	6 В	БОЛСУНОВ
9 Ц	27	22 С	БОЛСУНОВС
10 П	20	15 К	БОЛСУНОВСК
11 Н	18	13 И	БОЛСУНОВСКИ
12 О	19	14 Й	БОЛСУНОВСКИЙ
13 Д	8	3	БОЛСУНОВСКИЙ
14 Ж	11	6 В	БОЛСУНОВСКИЙ В
15 Е	9	4 А	БОЛСУНОВСКИЙ ВА
16 Р	21	16 Л	БОЛСУНОВСКИЙ ВАЛ
17 Й	14	9 Е	БОЛСУНОВСКИЙ ВАЛЕ
18 Х	26	21 Р	БОЛСУНОВСКИЙ ВАЛЕР
19 Н	18	13 И	БОЛСУНОВСКИЙ ВАЛЕРИ
20 О	19	14 Й	БОЛСУНОВСКИЙ ВАЛЕРИЙ
21 Д	8	3	БОЛСУНОВСКИЙ ВАЛЕРИЙ
22 Т	23	18 Н	БОЛСУНОВСКИЙ ВАЛЕРИЙ Н
23 Н	18	13 И	БОЛСУНОВСКИЙ ВАЛЕРИЙ НИ
24 П	20	15 К	БОЛСУНОВСКИЙ ВАЛЕРИЙ НИК
25 У	24	19 О	БОЛСУНОВСКИЙ ВАЛЕРИЙ НИКО
26 Р	21	16 Л	БОЛСУНОВСКИЙ ВАЛЕРИЙ НИКОЛ
27 Е	9	4 А	БОЛСУНОВСКИЙ ВАЛЕРИЙ НИКОЛА
28 Й	14	9 Е	БОЛСУНОВСКИЙ ВАЛЕРИЙ НИКОЛАЕ
29 Ж	11	6 В	БОЛСУНОВСКИЙ ВАЛЕРИЙ НИКОЛАЕВ
30 Н	18	13 И	БОЛСУНОВСКИЙ ВАЛЕРИЙ НИКОЛАЕВИ
31 Ъ	33	28 Ч	БОЛСУНОВСКИЙ ВАЛЕРИЙ НИКОЛАЕВИЧ

Заключение

В процессе прохождения практики по профилю специальности были

получены следующие результаты:

1. Поставлены цель и задачи.
8. Сформированы шаги к созданию.
9. Выбран механизма шифрования.
10. Спроектирована модель разработки.
11. Произведена реализация продукта.
12. Выполнено тестирование программы.
13. Совершена отладка продукта.

Список используемых материалов

<https://drive.google.com/drive/folders/15ywOWiyUXvwGkPjRGrSoX5FKtynX3sWv>

https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F

Спасибо за внимание