|  |  |
| --- | --- |
| **Российский университет транспорта (МИИТ)**  **Институт транспортной техники и систем управления**  **Кафедра «Управление и защита информации»** | |
| **Отчет**  **по практическому заданию**  **по теме «Разработка моноалфавитного шифра замены»**  **по дисциплине «Криптографические методы защиты информации»** | |
|  | Выполнил:  Студент группы ТКИ-342  Дроздов А.Д.  Проверил:  Доцент кафедры УиЗи, к.т.н., с.н.с.  Михалевич И.Ф. |
| Москва 2023 | |

**Оглавление**

[Задание 5](#_Toc129262633)

[Исходные данные 5](#_Toc129262634)

[1. Способы преобразования и проверки правильности преобразования 6](#_Toc129262635)

[1.1. Метод разбиения (breakdown method) 6](#_Toc129262636)

[1.2. Преобразование чисел методом вычисления значений полиномов (многочленов) 6](#_Toc129262637)

[1.3. Метод преобразования числа ручным пересчётом 7](#_Toc129262638)

[1.4. Схема Горнера 7](#_Toc129262639)

[2. Преобразование и проверка для двоичной системы 8](#_Toc129262640)

[2.1. Вычисление значения исходного числа ДР 8](#_Toc129262641)

[2.1.1. Метод деления 8](#_Toc129262642)

[2.1.2. Проверка методом полиномов и Горнера 8](#_Toc129262643)

[2.2. Вычисление значения исходного числа ДЗ 9](#_Toc129262644)

[2.2.1. Метод деления 9](#_Toc129262645)

[2.2.2. Проверка методом полиномов и Горнера 9](#_Toc129262646)

[2.3. Вычисление значения суммы чисел ДР и ДЗ 10](#_Toc129262647)

[2.3.1. Метод деления 10](#_Toc129262648)

[2.3.2. Проверка методом полиномов и Горнера 10](#_Toc129262649)

[3. Преобразование и проверка для троичной системы 11](#_Toc129262650)

[3.1. Вычисление значения исходного числа ДР 11](#_Toc129262651)

[3.1.1. Метод деления 11](#_Toc129262652)

[3.1.2. Проверка методом полиномов и Горнера 11](#_Toc129262653)

[3.2. Вычисление значения исходного числа ДЗ 12](#_Toc129262654)

[3.2.1. Метод деления 12](#_Toc129262655)

[3.2.2. Проверка методом полиномов и Горнера 12](#_Toc129262656)

[3.3. Вычисление значения суммы чисел ДР и ДЗ 13](#_Toc129262657)

[3.3.1. Метод деления 13](#_Toc129262658)

[3.3.2. Проверка методом полиномов и Горнера 13](#_Toc129262659)

[4. Преобразование и проверка для четверичной системы 14](#_Toc129262660)

[4.1. Вычисление значения исходного числа ДР 14](#_Toc129262661)

[4.1.1. Метод деления 14](#_Toc129262662)

[4.1.2. Проверка методом полиномов и Горнера 14](#_Toc129262663)

[4.2. Вычисление значения исходного числа ДЗ 15](#_Toc129262664)

[4.2.1. Метод деления 15](#_Toc129262665)

[4.2.2. Проверка методом полиномов и Горнера 15](#_Toc129262666)

[4.3. Вычисление значения суммы чисел ДР и ДЗ 16](#_Toc129262667)

[4.3.1. Метод деления 16](#_Toc129262668)

[4.3.2. Проверка методом полиномов и Горнера 16](#_Toc129262669)

[5. Преобразование и проверка для восьмеричной системы 17](#_Toc129262670)

[5.1. Вычисление значения исходного числа ДР 17](#_Toc129262671)

[5.1.1. Метод деления 17](#_Toc129262672)

[5.1.2. Проверка методом полиномов и Горнера 17](#_Toc129262673)

[5.2. Вычисление значения исходного числа ДЗ 18](#_Toc129262674)

[5.2.1. Метод деления 18](#_Toc129262675)

[5.2.2. Проверка методом полиномов и Горнера 18](#_Toc129262676)

[5.3. Вычисление значения суммы чисел ДР и ДЗ 19](#_Toc129262677)

[5.3.1. Метод деления 19](#_Toc129262678)

[5.3.2. Проверка методом полиномов и Горнера 19](#_Toc129262679)

[6. Преобразование и проверка для шестнадцатеричной системы 20](#_Toc129262680)

[6.1. Вычисление значения исходного числа ДР 20](#_Toc129262681)

[6.1.1. Метод деления 20](#_Toc129262682)

[6.1.2. Проверка методом полиномов и Горнера 20](#_Toc129262683)

[6.2. Вычисление значения исходного числа ДЗ 21](#_Toc129262684)

[6.2.1. Метод деления 21](#_Toc129262685)

[6.2.2. Проверка методом полиномов и Горнера 21](#_Toc129262686)

[6.3. Вычисление значения суммы чисел ДР и ДЗ 22](#_Toc129262687)

[6.3.1. Метод деления 22](#_Toc129262688)

[6.3.2. Проверка методом полиномов и Горнера 22](#_Toc129262689)

[7. Заключение 23](#_Toc129262690)

# Задание

Разработать моноалфавитный шифр, таблицы шифрования / расшифрования (для варианта шифра). Подготовить сообщение путем СЛИЯНИЯ сообщений инициатора и ответчика. Зашифровать и расшифровать сообщение. Провести анализ слабостей шифра (привести таблицы и гистограммы частотности символов исходного алфавита и сообщения, зашифрованного разработанным шифром, описать слабости шифра). Оформить отчет.

# Исходные данные

|  |
| --- |
|  |
| 1. – Исходные данные практического задания |

# 1. Способы преобразования и проверки правильности преобразования

## Метод разбиения (breakdown method)

Преобразуемое число последовательно делим на основание целевой системы счисления. Следующее деление использует частное предыдущей операции. Так продолжается до тех пор, пока остаток в пределах целевой системы счисления и частное не достигнут значения 0. Полученные остатки заполняют разряды в целевой системе счисления, начиная с самого младшего разряда.

## 1.2. Преобразование чисел методом вычисления значений полиномов (многочленов)

Полином (греч. пολυ - «много» + лат. nomen «имя»). Полином от одной переменной есть конечная формальная сумма вида:

|  |  |
| --- | --- |
| , |  |

где: - фиксированные коэффициенты, - степень полинома, – основание системы счисления.

Наблюдение: значение нулевого разряда полинома всегда равно значению коэффициента при его нулевом элементе.

Определение: нулевой элемент полинома называется свободным членом.

## 1.3. Метод преобразования числа ручным пересчётом

Правила преобразования двоичного числа в *k*-ричные числа с основаниями :

* исходная двоичная последовательность разделяется на группы по *k* двоичных символов справа налево;
* старшая группа символов может дополняться до общего размера в *k* символов необходимым числом нулей слева.

## 1.4. Схема Горнера

Альтернативой полиномиальному методу перевода чисел в десятичную форму является схема Горнера. По схеме Горнера легко перевести в десятичное число любое число по основанию *p*, представив его в виде алгебраического многочлена *n*-й степени:

|  |  |
| --- | --- |
|  |  |

Для перевода числа не требуется операция возведения в степень *n*, достаточно произвести *n* операций умножения и *n* операций сложения, не прибегая к операциям возведения в степень.

|  |  |
| --- | --- |
|  |  |

1. Цифру в старшем разряде умножить на основание *p*;
2. к результату добавить цифру в предыдущем разряде;
3. результат умножить на основание *p*;
4. повторить операции 2, 3 к цифрам в остальных разрядах;
5. на операции с цифрой в нулевом разряде получено число в десятичной записи.

# 2. Преобразование и проверка для двоичной системы

## 2.1. Вычисление значения исходного числа ДР

ДР = 03122002

### 2.1.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для числа «ДР» в 2сс |
|  |
| 1. – Метод деления по шагам для числа «ДР» в 2сс |

### 2.1.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для числа «ДР» в 2сс |
|  |
| 1. – Метод Горнера для числа «ДР» в 2сс |

## 2.2. Вычисление значения исходного числа ДЗ

ДЗ = 06032023

### 2.2.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для числа «ДЗ» в 2сс |
|  |
| 1. – Метод деления по шагам для числа «ДЗ» в 2сс |

### 2.2.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для числа «ДЗ» в 2сс |
|  |
| 1. – Метод Горнера для числа «ДЗ» в 2сс |

## 2.3. Вычисление значения суммы чисел ДР и ДЗ

ДР + ДЗ = 03122002 + 06032023 = 9154025

### 2.3.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для суммы чисел «ДР» и «ДЗ» в 2сс |
|  |
| 1. – Метод деления по шагам для суммы чисел «ДР» и «ДЗ» в 2сс |

### 2.3.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для суммы чисел «ДР» и «ДЗ» в 2сс |
|  |
| 1. – Метод Горнера для суммы чисел «ДР» и «ДЗ» в 2сс |

# 3. Преобразование и проверка для троичной системы

## 3.1. Вычисление значения исходного числа ДР

ДР = 03122002

### 3.1.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для числа «ДР» в 3сс |
|  |
| 1. – Метод деления по шагам для числа «ДР» в 3сс |

### 3.1.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для числа «ДР» в 3сс |
|  |
| 1. – Метод Горнера для числа «ДР» в 3сс |

## 3.2. Вычисление значения исходного числа ДЗ

ДЗ = 06032023

### 3.2.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для числа «ДЗ» в 3сс |
|  |
| 1. – Метод деления по шагам для числа «ДЗ» в 3сс |

### 3.2.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для числа «ДЗ» в 3сс |
|  |
| 1. – Метод Горнера для числа «ДЗ» в 3сс |

## 3.3. Вычисление значения суммы чисел ДР и ДЗ

ДР + ДЗ = 03122002 + 06032023 = 9154025

### 3.3.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для суммы чисел «ДР» и «ДЗ» в 3сс |
|  |
| 1. – Метод деления по шагам для суммы чисел «ДР» и «ДЗ» в 3сс |

### 3.3.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для суммы чисел «ДР» и «ДЗ» в 3сс |
|  |
| 1. – Метод Горнера для суммы чисел «ДР» и «ДЗ» в 3сс |

# 4. Преобразование и проверка для четверичной системы

## 4.1. Вычисление значения исходного числа ДР

ДР = 03122002

### 4.1.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для числа «ДР» в 4сс |
|  |
| 1. – Метод деления по шагам для числа «ДР» в 4сс |

### 4.1.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для числа «ДР» в 4сс |
|  |
| 1. – Метод Горнера для числа «ДР» в 4сс |

## 4.2. Вычисление значения исходного числа ДЗ

ДЗ = 06032023

### 4.2.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для числа «ДЗ» в 4сс |
|  |
| 1. – Метод деления по шагам для числа «ДЗ» в 4сс |

### 4.2.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для числа «ДЗ» в 4сс |
|  |
| 1. – Метод Горнера для числа «ДЗ» в 4сс |

## 4.3. Вычисление значения суммы чисел ДР и ДЗ

ДР + ДЗ = 03122002 + 06032023 = 9154025

### 4.3.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для суммы чисел «ДР» и «ДЗ» в 4сс |
|  |
| 1. – Метод деления по шагам для суммы чисел «ДР» и «ДЗ» в 4сс |

### 4.3.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для суммы чисел «ДР» и «ДЗ» в 4сс |
|  |
| 1. – Метод Горнера для суммы чисел «ДР» и «ДЗ» в 4сс |

# 5. Преобразование и проверка для восьмеричной системы

## 5.1. Вычисление значения исходного числа ДР

ДР = 03122002

### 5.1.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для числа «ДР» в 8сс |
|  |
| 1. – Метод деления по шагам для числа «ДР» в 8сс |

### 5.1.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для числа «ДР» в 8сс |
|  |
| 1. – Метод Горнера для числа «ДР» в 8сс |

## 5.2. Вычисление значения исходного числа ДЗ

ДЗ = 06032023

### 5.2.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для числа «ДЗ» в 8сс |
|  |
| 1. – Метод деления по шагам для числа «ДЗ» в 8сс |

### 5.2.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для числа «ДЗ» в 8сс |
|  |
| 1. – Метод Горнера для числа «ДЗ» в 8сс |

## 5.3. Вычисление значения суммы чисел ДР и ДЗ

ДР + ДЗ = 03122002 + 06032023 = 9154025

### 5.3.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для суммы чисел «ДР» и «ДЗ» в 8сс |
|  |
| 1. – Метод деления по шагам для суммы чисел «ДР» и «ДЗ» в 8сс |

### 5.3.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для суммы чисел «ДР» и «ДЗ» в 8сс |
|  |
| 1. – Метод Горнера для суммы чисел «ДР» и «ДЗ» в 8сс |

# 6. Преобразование и проверка для шестнадцатеричной системы

## 6.1. Вычисление значения исходного числа ДР

ДР = 03122002

### 6.1.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для числа «ДР» в 16сс |
|  |
| 1. – Метод деления по шагам для числа «ДР» в 16сс |

### 6.1.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для числа «ДР» в 16сс |
|  |
| 1. – Метод Горнера для числа «ДР» в 16сс |

## 6.2. Вычисление значения исходного числа ДЗ

ДЗ = 06032023

### 6.2.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для числа «ДЗ» в 16сс |
|  |
| 1. – Метод деления по шагам для числа «ДЗ» в 16сс |

### 6.2.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для числа «ДЗ» в 16сс |
|  |
| 1. – Метод Горнера для числа «ДЗ» в 16сс |

## 6.3. Вычисление значения суммы чисел ДР и ДЗ

ДР + ДЗ = 03122002 + 06032023 = 9154025

### 6.3.1. Метод деления

|  |
| --- |
|  |
| 1. – Метод деления для суммы чисел «ДР» и «ДЗ» в 16сс |
|  |
| 1. – Метод деления по шагам для суммы чисел «ДР» и «ДЗ» в 16сс |

### 6.3.2. Проверка методом полиномов и Горнера

|  |
| --- |
|  |
| 1. – Метод полиномов для суммы чисел «ДР» и «ДЗ» в 16сс |
|  |
| 1. – Метод Горнера для суммы чисел «ДР» и «ДЗ» в 16сс |

# 7. Заключение

В ходе решения практического задания были преобразованы в различные системы счисления следующие значения: ДР – день рождения, ДЗ – день выполнения задания. Применялись следующие методы: разбиения (деления), полиномов, многочлена, по схеме Горнера, «ручным» пересчетом. Все значения были перепроверены и соответствуют исходным данным.