УО «Белорусский государственный университет   
информатики и радиоэлектроники»

Кафедра ПОИТ

Отчёт по лабораторной работе № 3  
по предмету «Теория информации»  
Вариант 2

Выполнила:

Сучёк Е.А.

гр. 351003

Проверила:

Болтак С.В.

Минск 2025

1. **Пример работы алгоритма быстрого возведения в степень с модульной арифметикой**:

**13217 mod 57 = (13128 \* 1364 \* 1316 \* 138 \* 13) mod 57 = 13**

|  |  |  |
| --- | --- | --- |
| **Шаг** | **Основание степени** | **Результат** |
| 0 | 13 | 13 mod 57 = 13 |
| 1 | 13 mod 57 | (13 \* 13) mod 57 = 55  132 mod 57 = 55 |
| 2 | 132 mod 57 | (55 \* 55) mod 57 = 4  134 mod 57 = 4 |
| 3 | 134 mod 57 | (4 \* 4) mod 57 = 16  138 mod 57 = 16 |
| 4 | 138 mod 57 | (16 \* 16) mod 57 = 28  1316 mod 57 = 28 |
| 5 | 1316 mod 57 | (28 \* 28) mod 57 = 43  1332 mod 57 = 43 |
| 6 | 1332 mod 57 | (43 \* 43) mod 57 = 25  1364 mod 57 = 25 |
| 7 | 1364 mod 57 | (25 \*25) mod 57 = 55  13128 mod 57 = 55 |

13 mod 57 = 13

138 mod 57 = 16

1316 mod 57 = 28

1364 mod 57 = 25

13128 mod 57 = 55

(55 \* 25 \* 28 \* 16 \* 13) mod 57 = 13217 mod 57**;**

(55 \* 25) mod 57 \* (28 \* 16) mod 57 \* 13 mod 57 = (7 \* 49) mod 57 \* 13 mod 57 = (1 \* 13) mod 57 = **13**

1. **Пример поиска всех первообразных корней по заданному модулю**

Простое число **p = 157**Простые делители **p - 1 = phi = 156 ={2, 3, 13}**Итерируем от **1** до **p – 1**Если результат возведения в степень будет равен 1 по модулю p – значит порядок числа **g** меньше **p – 1** и он не является первообразным корнем:  
  **g (phi / factor) mod p != 1**

Возможные степени:  
 **156 / 2 = 78;  
 156 / 3 = 52;  
 156 / 13 = 12.**

**g = 1:**

1⁷⁸ mod 157 = 1

1⁵² mod 157 = 1

1¹² mod 157 = 1

**Не является первообразным корнем.**

**g = 2:**

2⁷⁸ mod 157 = 156

2⁵² mod 157 = 1

2¹² mod 157 = 14

**Не является первообразным корнем.**

**g = 3:**

3⁷⁸ mod 157 = 1

3⁵² mod 157 = 113

3¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 4:**

4⁷⁸ mod 157 = 1

4⁵² mod 157 = 64

4¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 5:**

5⁷⁸ mod 157 = 156

5⁵² mod 157 = 25

5¹² mod 157 = 125

**Является первообразным корнем.**

**g = 6:**

6⁷⁸ mod 157 = 156

6⁵² mod 157 = 113

6¹² mod 157 = 144

**Является первообразным корнем.**

**g = 7:**

7⁷⁸ mod 157 = 156

7⁵² mod 157 = 1

7¹² mod 157 = 138

**Не является первообразным корнем.**

**g = 8:**

8⁷⁸ mod 157 = 1

8⁵² mod 157 = 64

8¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 9:**

9⁷⁸ mod 157 = 1

9⁵² mod 157 = 113

9¹² mod 157 = 144

**Не является первообразным корнем (9⁷⁸ = 1).**

**g = 10:**

10⁷⁸ mod 157 = 1

10⁵² mod 157 = 25

10¹² mod 157 = 125

**Не является первообразным корнем (10⁷⁸ = 1).**

**g = 11:**

11⁷⁸ mod 157 = 1

11⁵² mod 157 = 12

11¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 12:**

12⁷⁸ mod 157 = 1

12⁵² mod 157 = 64

12¹² mod 157 = 60

**Не является первообразным корнем (12⁷⁸ = 1).**

**g = 13:**

13⁷⁸ mod 157 = 1

13⁵² mod 157 = 58

13¹² mod 157 = 129

**Не является первообразным корнем (13⁷⁸ = 1).**

**g = 14:**

14⁷⁸ mod 157 = 1

14⁵² mod 157 = 42

14¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 15:**

15⁷⁸ mod 157 = 156

15⁵² mod 157 = 113

15¹² mod 157 = 144

**Является первообразным корнем.**

**g = 16:**

16⁷⁸ mod 157 = 1

16⁵² mod 157 = 64

16¹² mod 157 = 60

**Не является первообразным корнем (16⁷⁸ = 1).**

**g = 17:**

17⁷⁸ mod 157 = 1

17⁵² mod 157 = 153

17¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 18:**

18⁷⁸ mod 157 = 156

18⁵² mod 157 = 113

18¹² mod 157 = 144

**Является первообразным корнем.**

**g = 19:**

19⁷⁸ mod 157 = 1

19⁵² mod 157 = 58

19¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 20:**

20⁷⁸ mod 157 = 156

20⁵² mod 157 = 25

20¹² mod 157 = 125

**Является первообразным корнем.**

**g = 21:**

21⁷⁸ mod 157 = 156

21⁵² mod 157 = 113

21¹² mod 157 = 144

**Является первообразным корнем.**

**g = 22:**

22⁷⁸ mod 157 = 1

22⁵² mod 157 = 121

22¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 23:**

23⁷⁸ mod 157 = 1

23⁵² mod 157 = 58

23¹² mod 157 = 129

**Не является первообразным корнем (23⁷⁸=1).**

**g = 24:**

24⁷⁸ mod 157 = 156

24⁵² mod 157 = 64

24¹² mod 157 = 60

**Является первообразным корнем.**

**g = 25:**

25⁷⁸ mod 157 = 1

25⁵² mod 157 = 25

25¹² mod 157 = 125

**Не является первообразным корнем (25⁷⁸=1).**

**g = 26:**

26⁷⁸ mod 157 = 156

26⁵² mod 157 = 64

26¹² mod 157 = 14

**Является первообразным корнем.**

**g = 27:**

27⁷⁸ mod 157 = 1

27⁵² mod 157 = 113

27¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 28:**

28⁷⁸ mod 157 = 1

28⁵² mod 157 = 42

28¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 29:**

29⁷⁸ mod 157 = 1

29⁵² mod 157 = 153

29¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 30:**

30⁷⁸ mod 157 = 1

30⁵² mod 157 = 113

30¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 31:**

31⁷⁸ mod 157 = 1

31⁵² mod 157 = 25

31¹² mod 157 = 125

**Не является первообразным корнем.**

**g = 32:**

32⁷⁸ mod 157 = 1

32⁵² mod 157 = 64

32¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 33:**

33⁷⁸ mod 157 = 1

33⁵² mod 157 = 113

33¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 34:**

34⁷⁸ mod 157 = 156

34⁵² mod 157 = 64

34¹² mod 157 = 14

**Является первообразным корнем.**

**g = 35:**

35⁷⁸ mod 157 = 1

35⁵² mod 157 = 42

35¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 36:**

36⁷⁸ mod 157 = 1

36⁵² mod 157 = 113

36¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 37:**

37⁷⁸ mod 157 = 156

37⁵² mod 157 = 58

37¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 38:**

38⁷⁸ mod 157 = 156

38⁵² mod 157 = 42

38¹² mod 157 = 60

**Является первообразным корнем.**

**g = 39:**

39⁷⁸ mod 157 = 1

39⁵² mod 157 = 113

39¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 40:**

40⁷⁸ mod 157 = 1

40⁵² mod 157 = 25

40¹² mod 157 = 125

**Не является первообразным корнем.**

**g = 41:**

41⁷⁸ mod 157 = 1

41⁵² mod 157 = 64

41¹² mod 157 = 14

**Не является первообразным корнем.**

**g = 42:**

42⁷⁸ mod 157 = 1

42⁵² mod 157 = 113

42¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 43:**

43⁷⁸ mod 157 = 156

43⁵² mod 157 = 58

43¹² mod 157 = 129

**Является первообразным корнем.**

**g = 44:**

44⁷⁸ mod 157 = 1

44⁵² mod 157 = 42

44¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 45:**

45⁷⁸ mod 157 = 1

45⁵² mod 157 = 113

45¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 46:**

46⁷⁸ mod 157 = 1

46⁵² mod 157 = 153

46¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 47:**

47⁷⁸ mod 157 = 1

47⁵² mod 157 = 58

47¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 48:**

48⁷⁸ mod 157 = 1

48⁵² mod 157 = 64

48¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 49:**

49⁷⁸ mod 157 = 1

49⁵² mod 157 = 25

49¹² mod 157 = 125

**Не является первообразным корнем.**

**g = 50:**

50⁷⁸ mod 157 = 1

50⁵² mod 157 = 64

50¹² mod 157 = 14

**Не является первообразным корнем.**

**g = 51:**

51⁷⁸ mod 157 = 1

51⁵² mod 157 = 113

51¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 52:**

52⁷⁸ mod 157 = 1

52⁵² mod 157 = 64

52¹² mod 157 = 14

**Не является первообразным корнем.**

**g = 53:**

53⁷⁸ mod 157 = 156

53⁵² mod 157 = 153

53¹² mod 157 = 152

**Является первообразным корнем.**

**g = 54:**

54⁷⁸ mod 157 = 1

54⁵² mod 157 = 113

54¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 55:**

55⁷⁸ mod 157 = 156

55⁵² mod 157 = 25

55¹² mod 157 = 125

**Является первообразным корнем.**

**g = 56:**

56⁷⁸ mod 157 = 1

56⁵² mod 157 = 42

56¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 57:**

57⁷⁸ mod 157 = 1

57⁵² mod 157 = 113

57¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 58:**

58⁷⁸ mod 157 = 1

58⁵² mod 157 = 58

58¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 59:**

59⁷⁸ mod 157 = 1

59⁵² mod 157 = 153

59¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 60:**

60⁷⁸ mod 157 = 156

60⁵² mod 157 = 42

60¹² mod 157 = 60

**Является первообразным корнем.**

**g = 61:**

61⁷⁸ mod 157 = 156

61⁵² mod 157 = 58

61¹² mod 157 = 129

**Является первообразным корнем.**

**g = 62:**

62⁷⁸ mod 157 = 156

62⁵² mod 157 = 113

62¹² mod 157 = 144

**Является первообразным корнем.**

**g = 63:**

63⁷⁸ mod 157 = 156

63⁵² mod 157 = 25

63¹² mod 157 = 125

**Является первообразным корнем.**

**g = 64:**

64⁷⁸ mod 157 = 1

64⁵² mod 157 = 64

64¹² mod 157 = 14

**Не является первообразным корнем.**

**g = 65:**

65⁷⁸ mod 157 = 1

65⁵² mod 157 = 153

65¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 66:**

66⁷⁸ mod 157 = 156

66⁵² mod 157 = 113

66¹² mod 157 = 144

**Является первообразным корнем.**

**g = 67:**

67⁷⁸ mod 157 = 1

67⁵² mod 157 = 58

67¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 68:**

68⁷⁸ mod 157 = 1

68⁵² mod 157 = 42

68¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 69:**

69⁷⁸ mod 157 = 156

69⁵² mod 157 = 113

69¹² mod 157 = 144

**Является первообразным корнем.**

**g = 70:**

70⁷⁸ mod 157 = 156

70⁵² mod 157 = 153

70¹² mod 157 = 152

**Является первообразным корнем.**

**g = 71:**

71⁷⁸ mod 157 = 1

71⁵² mod 157 = 58

71¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 72:**

72⁷⁸ mod 157 = 1

72⁵² mod 157 = 64

72¹² mod 157 = 60

**Является первообразным корнем.**

**g = 73:**

73⁷⁸ mod 157 = 156

73⁵² mod 157 = 113

73¹² mod 157 = 144

**Является первообразным корнем.**

**g = 74:**

74⁷⁸ mod 157 = 156

74⁵² mod 157 = 42

74¹² mod 157 = 60

**Является первообразным корнем.**

**g = 75:**

75⁷⁸ mod 157 = 1

75⁵² mod 157 = 25

75¹² mod 157 = 125

**Не является первообразным корнем.**

**g = 76:**

76⁷⁸ mod 157 = 1

76⁵² mod 157 = 153

76¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 77:**

77⁷⁸ mod 157 = 156

77⁵² mod 157 = 58

77¹² mod 157 = 129

**Является первообразным корнем.**

**g = 78:**

78⁷⁸ mod 157 = 1

78⁵² mod 157 = 113

78¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 79:**

79⁷⁸ mod 157 = 1

79⁵² mod 157 = 42

79¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 80:**

80⁷⁸ mod 157 = 156

80⁵² mod 157 = 64

80¹² mod 157 = 14

**Является первообразным корнем.**

**g = 81:**

81⁷⁸ mod 157 = 1

81⁵² mod 157 = 113

81¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 82:**

82⁷⁸ mod 157 = 1

82⁵² mod 157 = 153

82¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 83:**

83⁷⁸ mod 157 = 156

83⁵² mod 157 = 58

83¹² mod 157 = 129

**Является первообразным корнем.**

**g = 84:**

84⁷⁸ mod 157 = 156

84⁵² mod 157 = 42

84¹² mod 157 = 60

**Является первообразным корнем.**

**g = 85:**

85⁷⁸ mod 157 = 156

85⁵² mod 157 = 113

85¹² mod 157 = 144

**Является первообразным корнем.**

**g = 86:**

86⁷⁸ mod 157 = 1

86⁵² mod 157 = 153

86¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 87:**

87⁷⁸ mod 157 = 156

87⁵² mod 157 = 58

87¹² mod 157 = 129

**Является первообразным корнем.**

**g = 88:**

88⁷⁸ mod 157 = 156

88⁵² mod 157 = 64

88¹² mod 157 = 60

**Является первообразным корнем.**

**g = 89:**

89⁷⁸ mod 157 = 1

89⁵² mod 157 = 113

89¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 90:**

90⁷⁸ mod 157 = 1

90⁵² mod 157 = 42

90¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 91:**

91⁷⁸ mod 157 = 156

91⁵² mod 157 = 153

91¹² mod 157 = 152

**Является первообразным корнем.**

**g = 92:**

92⁷⁸ mod 157 = 1

92⁵² mod 157 = 58

92¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 93:**

93⁷⁸ mod 157 = 1

93⁵² mod 157 = 113

93¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 94:**

94⁷⁸ mod 157 = 156

94⁵² mod 157 = 42

94¹² mod 157 = 60

**Является первообразным корнем.**

**g = 95:**

95⁷⁸ mod 157 = 156

95⁵² mod 157 = 64

95¹² mod 157 = 14

**Является первообразным корнем.**

**g = 96:**

96⁷⁸ mod 157 = 156

96⁵² mod 157 = 113

96¹² mod 157 = 144

**Является первообразным корнем.**

**g = 97:**

97⁷⁸ mod 157 = 156

97⁵² mod 157 = 153

97¹² mod 157 = 152

**Является первообразным корнем.**

**g = 98:**

98⁷⁸ mod 157 = 1

98⁵² mod 157 = 58

98¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 99:**

99⁷⁸ mod 157 = 1

99⁵² mod 157 = 42

99¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 100:**

100⁷⁸ mod 157 = 1

100⁵² mod 157 = 25

100¹² mod 157 = 125

**Не является первообразным корнем.**

**g = 101:**

101⁷⁸ mod 157 = 1

101⁵² mod 157 = 153

101¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 102:**

102⁷⁸ mod 157 = 156

102⁵² mod 157 = 113

102¹² mod 157 = 144

**Является первообразным корнем.**

**g = 103:**

103⁷⁸ mod 157 = 1

103⁵² mod 157 = 58

103¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 104:**

104⁷⁸ mod 157 = 156

104⁵² mod 157 = 42

104¹² mod 157 = 60

**Является первообразным корнем.**

**g = 105:**

105⁷⁸ mod 157 = 1

105⁵² mod 157 = 25

105¹² mod 157 = 125

**Не является первообразным корнем.**

**g = 106:**

106⁷⁸ mod 157 = 1

106⁵² mod 157 = 64

106¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 107:**

107⁷⁸ mod 157 = 1

107⁵² mod 157 = 113

107¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 108:**

108⁷⁸ mod 157 = 1

108⁵² mod 157 = 42

108¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 109:**

109⁷⁸ mod 157 = 1

109⁵² mod 157 = 153

109¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 110:**

110⁷⁸ mod 157 = 1

110⁵² mod 157 = 58

110¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 111:**

111⁷⁸ mod 157 = 1

111⁵² mod 157 = 113

111¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 112:**

112⁷⁸ mod 157 = 1

112⁵² mod 157 = 42

112¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 113:**

113⁷⁸ mod 157 = 1

113⁵² mod 157 = 113

113¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 114:**

114⁷⁸ mod 157 = 156

114⁵² mod 157 = 153

114¹² mod 157 = 152

**Является первообразным корнем.**

**g = 115:**

115⁷⁸ mod 157 = 1

115⁵² mod 157 = 58

115¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 116:**

116⁷⁸ mod 157 = 1

116⁵² mod 157 = 42

116¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 117:**

117⁷⁸ mod 157 = 1

117⁵² mod 157 = 113

117¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 118:**

118⁷⁸ mod 157 = 1

118⁵² mod 157 = 153

118¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 119:**

119⁷⁸ mod 157 = 156

119⁵² mod 157 = 58

119¹² mod 157 = 129

**Является первообразным корнем.**

**g = 120:**

120⁷⁸ mod 157 = 1

120⁵² mod 157 = 42

120¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 121:**

121⁷⁸ mod 157 = 1

121⁵² mod 157 = 121

121¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 122:**

122⁷⁸ mod 157 = 1

122⁵² mod 157 = 113

122¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 123:**

123⁷⁸ mod 157 = 156

123⁵² mod 157 = 153

123¹² mod 157 = 152

**Является первообразным корнем.**

**g = 124:**

124⁷⁸ mod 157 = 1

124⁵² mod 157 = 58

124¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 125:**

125⁷⁸ mod 157 = 1

125⁵² mod 157 = 25

125¹² mod 157 = 125

**Не является первообразным корнем.**

**g = 126:**

126⁷⁸ mod 157 = 1

126⁵² mod 157 = 42

126¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 127:**

127⁷⁸ mod 157 = 1

127⁵² mod 157 = 113

127¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 128:**

128⁷⁸ mod 157 = 1

128⁵² mod 157 = 64

128¹² mod 157 = 14

**Не является первообразным корнем.**

**g = 129:**

129⁷⁸ mod 157 = 1

129⁵² mod 157 = 153

129¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 130:**

130⁷⁸ mod 157 = 1

130⁵² mod 157 = 58

130¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 131:**

131⁷⁸ mod 157 = 156

131⁵² mod 157 = 42

131¹² mod 157 = 60

**Является первообразным корнем.**

**g = 132:**

132⁷⁸ mod 157 = 1

132⁵² mod 157 = 113

132¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 133:**

133⁷⁸ mod 157 = 156

133⁵² mod 157 = 153

133¹² mod 157 = 152

**Является первообразным корнем.**

**g = 134:**

134⁷⁸ mod 157 = 1

134⁵² mod 157 = 58

134¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 135:**

135⁷⁸ mod 157 = 1

135⁵² mod 157 = 42

135¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 136:**

136⁷⁸ mod 157 = 156

136⁵² mod 157 = 113

136¹² mod 157 = 144

**Является первообразным корнем.**

**g = 137:**

137⁷⁸ mod 157 = 156

137⁵² mod 157 = 153

137¹² mod 157 = 152

**Является первообразным корнем.**

**g = 138:**

138⁷⁸ mod 157 = 1

138⁵² mod 157 = 58

138¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 139:**

139⁷⁸ mod 157 = 156

139⁵² mod 157 = 42

139¹² mod 157 = 60

**Является первообразным корнем.**

**g = 140:**

140⁷⁸ mod 157 = 1

140⁵² mod 157 = 113

140¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 141:**

141⁷⁸ mod 157 = 1

141⁵² mod 157 = 153

141¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 142:**

142⁷⁸ mod 157 = 156

142⁵² mod 157 = 58

142¹² mod 157 = 129

**Является первообразным корнем.**

**g = 143:**

143⁷⁸ mod 157 = 1

143⁵² mod 157 = 42

143¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 144:**

144⁷⁸ mod 157 = 1

144⁵² mod 157 = 144

144¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 145:**

145⁷⁸ mod 157 = 1

145⁵² mod 157 = 113

145¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 146:**

146⁷⁸ mod 157 = 1

146⁵² mod 157 = 153

146¹² mod 157 = 152

**Не является первообразным корнем.**

**g = 147:**

147⁷⁸ mod 157 = 1

147⁵² mod 157 = 58

147¹² mod 157 = 129

**Не является первообразным корнем.**

**g = 148:**

148⁷⁸ mod 157 = 15

148⁵² mod 157 = 42

148¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 149:**

149⁷⁸ mod 157 = 1

149⁵² mod 157 = 113

149¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 150:**

150⁷⁸ mod 157 = 1

150⁵² mod 157 = 153

150¹² mod 157 = 25

**Не является первообразным корнем.**

**g = 151:**

151⁷⁸ mod 157 = 156

151⁵² mod 157 = 36

151¹² mod 157 = 144

**Является первообразным корнем.**

**g = 152:**

152⁷⁸ mod 157 = 156

152⁵² mod 157 = 153

152¹² mod 157 = 152

**Является первообразным корнем.**

**g = 153:**

153⁷⁸ mod 157 = 1

153⁵² mod 157 = 153

153¹² mod 157 = 144

**Не является первообразным корнем.**

**g = 154:**

154⁷⁸ mod 157 = 1

154⁵² mod 157 = 42

154¹² mod 157 = 60

**Не является первообразным корнем.**

**g = 155:**

155⁷⁸ mod 157 = 1

155⁵² mod 157 = 121

155¹² mod 157 = 125

**Не является первообразным корнем.**

**g = 156:**

156⁷⁸ mod 157 = 1

156⁵² mod 157 = 1

156¹² mod 157 = 1

**Не является первообразным корнем.**

**Итоговый список первообразных корней (48 штук):**

5 6 15 18 20 21 24 26 34 38 43 53 55 60 61 62 63 66 69 70 72 73 74 77 80 83 84 85 87 88 91 94 95 96 97 102 104 114 119 123 131 133 136 137 139 142 151 152

**Количество: 48** (что соответствует φ(156) = 48).

1. **Пример работы расширенного алгоритма Евклида с взаимно простыми числами**

x1\*a + y1\*b = НОД(a, b), a = **59**, b = **37**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 59 | 37 | 1 | 0 | 0 | 1 |
| 1 | 1 | 37 | 22 | 0 | 1 | 1 | -1 |
| 2 | 1 | 22 | 15 | 1 | -1 | -1 | 2 |
| 3 | 1 | 15 | 7 | -1 | 2 | 2 | -3 |
| 4 | 2 | 7 | 1 | 2 | -3 | -3 | 8 |
| 5 | 7 | 1 | 0 | **-3** | 8 | **8** | -59 |

x1 = -3

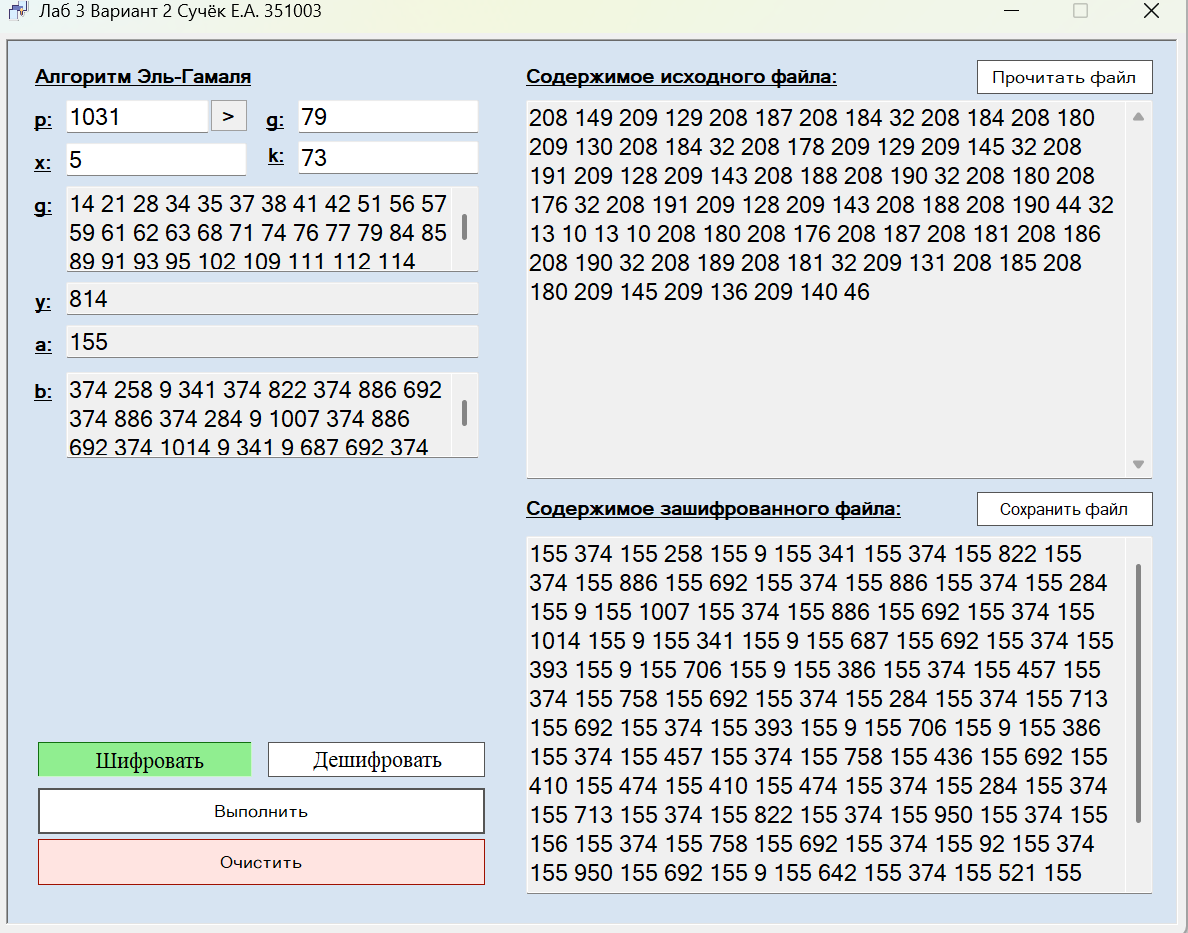
y1 = 8

-3 \* 59 + 8 \* 37 = **1**

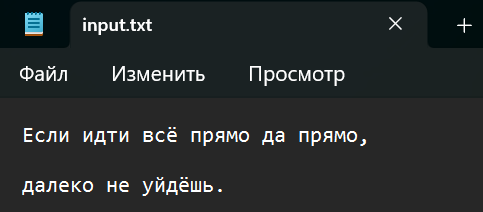
**Пример выполнения программы:**

**Шифрование(***текстовый файл***)**

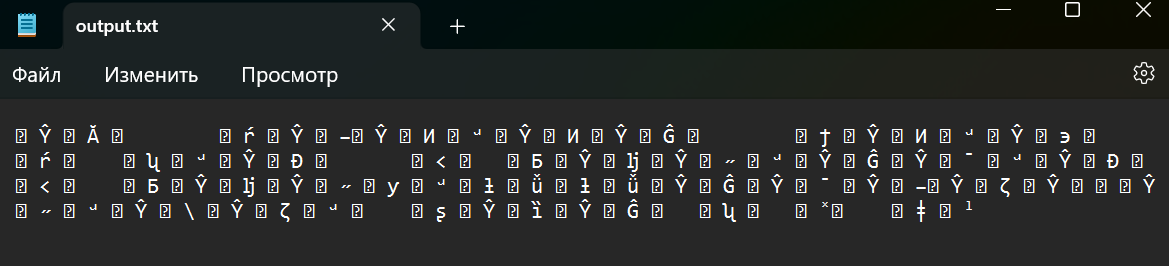
**Процесс шифрования:**



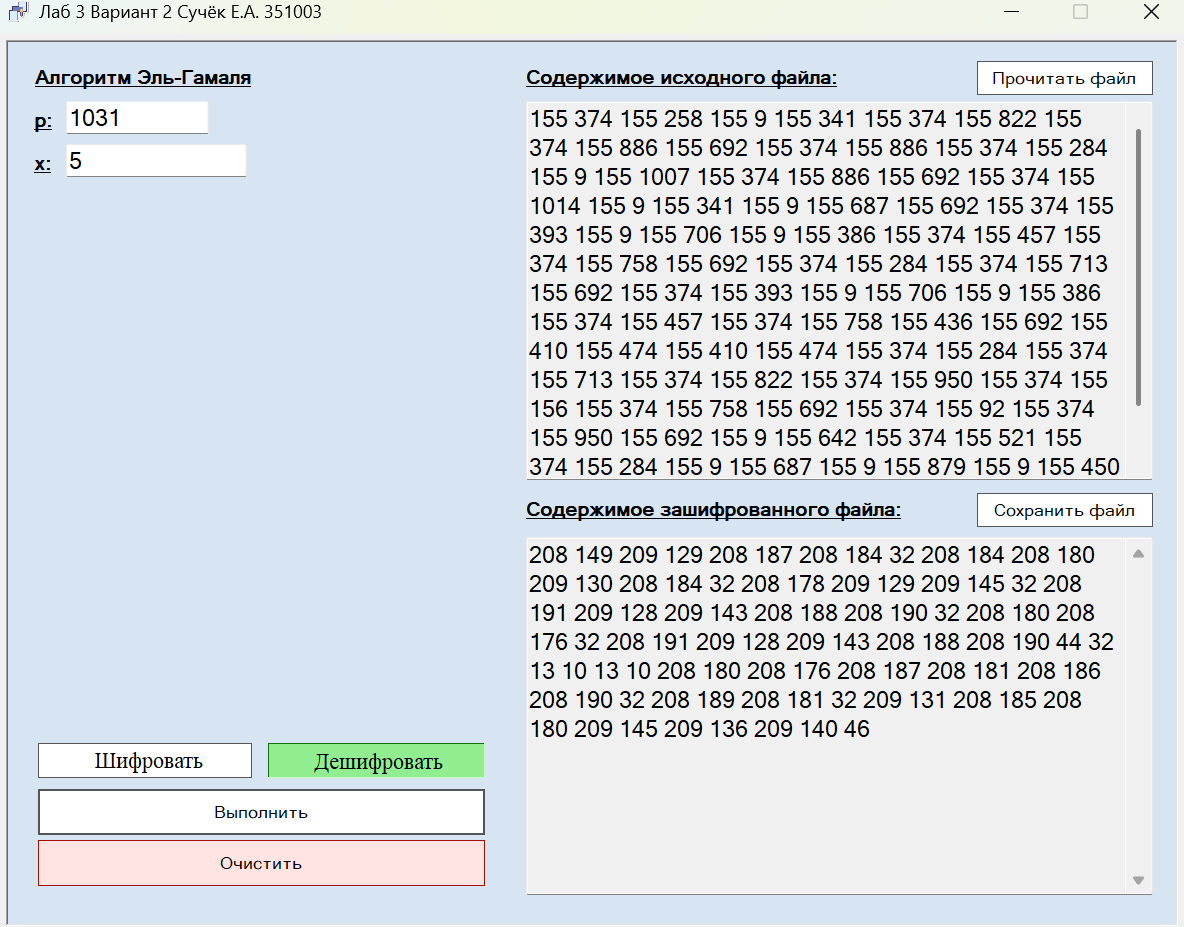
**Содержимое исходного файла:**



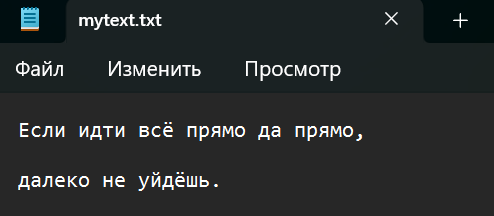
**Содержимое зашифрованного файла:**



**Процесс дешифрации:**

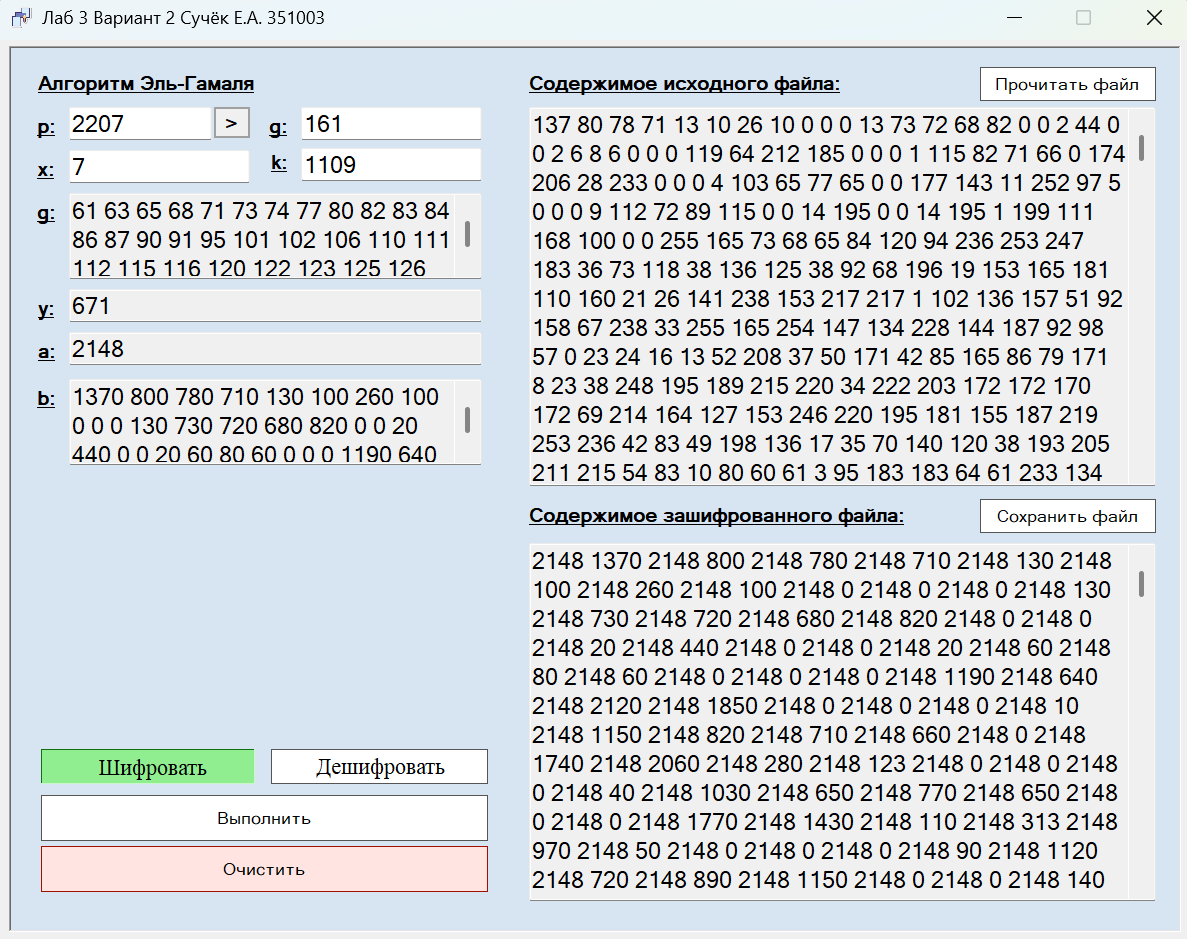


**Содержимое полученного файла:**



**Шифрование(***картинка***)**

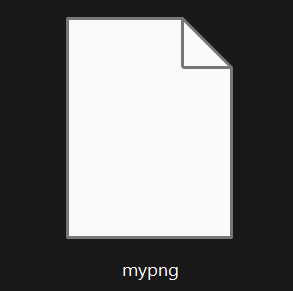
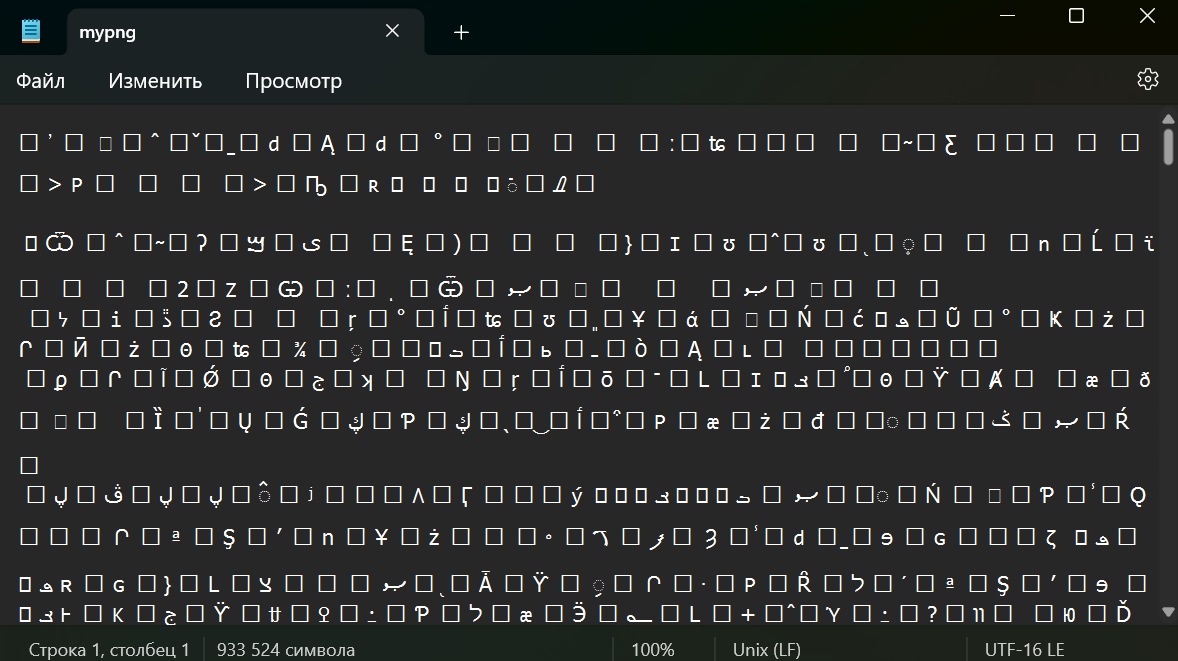
**Процесс шифрования:**



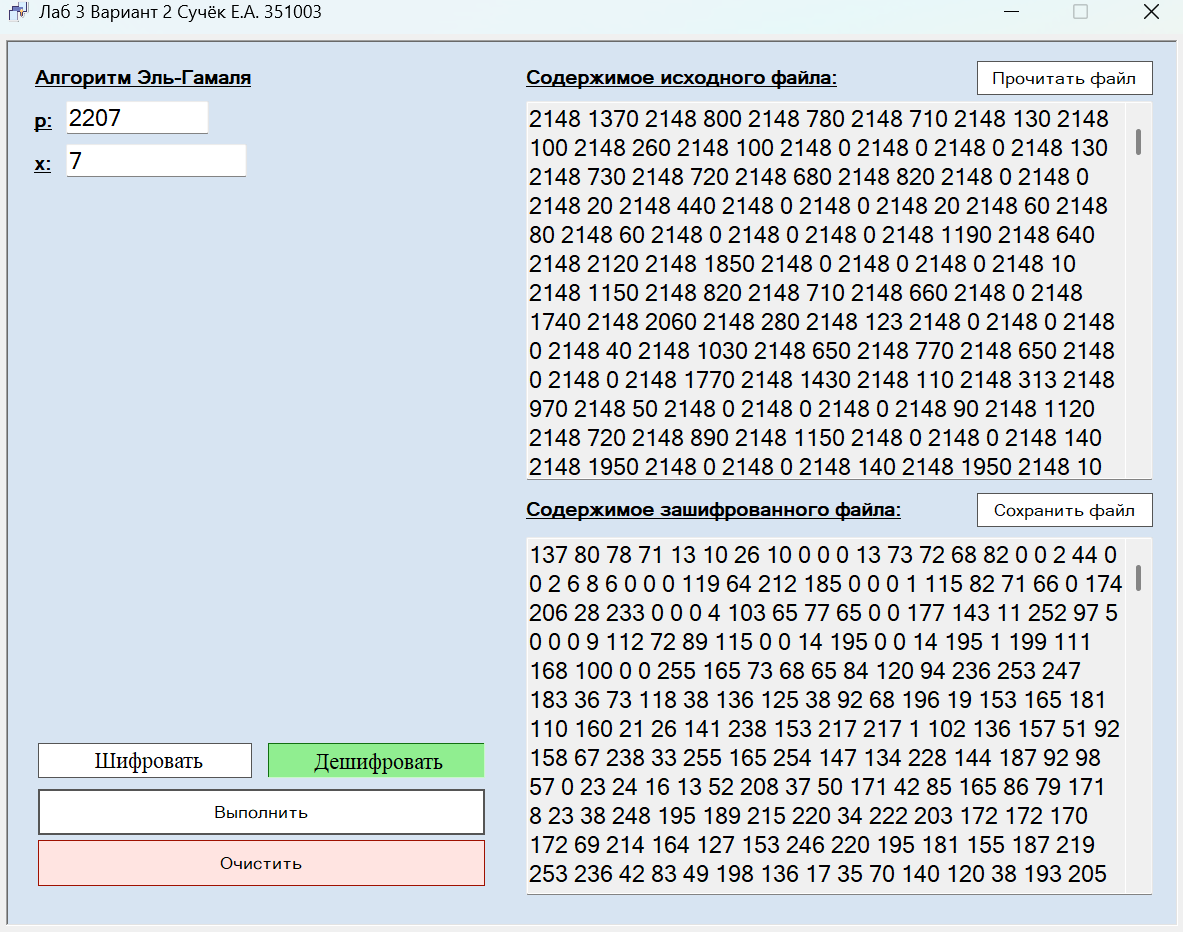
**Содержимое исходного файла:**



**Содержимое зашифрованного файла:**

**Процесс дешифрации:**



**Содержимое полученного файла:**

