Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Теория информации

ОТЧЕТ

по лабораторной работе 3

Вариант 3

|  |  |
| --- | --- |
| Выполнил:  Студент гр. 351002 | Филипенко А. С. |
| Проверил: | Болтак С. В. |

Минск 2025

Криптографические системы с открытым ключом

Криптосистема Рабина

Тесты

Тест 1

**Исходные данные:**

p = 331

q = 3331

b = 4444

**Ключи:**

Открытый: (n, b) =>(1102561, 4444)

Закрытый: (p, q) =>(331, 3331)

**Исходный текст:**

0 0 0 32 102 116 121 112 105 115 111 109 0 0 2 0 105 115 111 109 105 115 111 50 97 118 99 49 109 112 52 49 0 0 0 8 102 114 101 101 0 79 228 203 109 100 97 116 1 2 20 25 20 38 51 134 2 193 68 144 133 79 126 19 38 251 251 247 114 164 239 87 41 42 93 18 244 148 42 194 127 26 59 44 239 236 182 237 121 108 225 211 179 64 127 143 194 217 42 233

...

0 79 224 129 0 0 0 96 117 100 116 97 0 0 0 88 109 101 116 97 0 0 0 0 0 0 0 33 104 100 108 114 0 0 0 0 0 0 0 0 109 100 105 114 97 112 112 108 0 0 0 0 0 0 0 0 0 0 0 0 43 105 108 115 116 0 0 0 35 169 116 111 111 0 0 0 27 100 97 116 97 0 0 0 1 0 0 0 0 76 97 118 102 53 51 46 50 52 46 50

**Зашифрованный текст:**

0 0 0 0 0 0 0 0 0 128 47 2 76 19 7 64 18 8 173 109 8 64 201 7 205 73 7 253 255 7 5 183 7 149 146 7 0 0 0 0 0 0 188 34 0 0 0 0 205 73 7 253 255 7 5 183 7 149 146 7 205 73 7 253 255 7 5 183 7 188 109 3 157 184 6 204 54 8 221 220 6 253 91 3 149 146 7 64 201 7 64 145 3 253 91 3 0 0 0 0

...

0 0 0 0 93 100 2 77 229 11 64 18 8 5 183 7 5 183 7 0 0 0 0 0 0 0 0 0 141 215 1 0 239 6 157 184 6 64 18 8 157 184 6 0 0 0 0 0 0 0 0 0 93 17 0 0 0 0 0 0 0 0 0 0 0 0 0 224 61 5 157 184 6 204 54 8 76 19 7 5 163 3 125 127 3 204 38 3 188 109 3 64 145 3 204 38 3 188 109 3

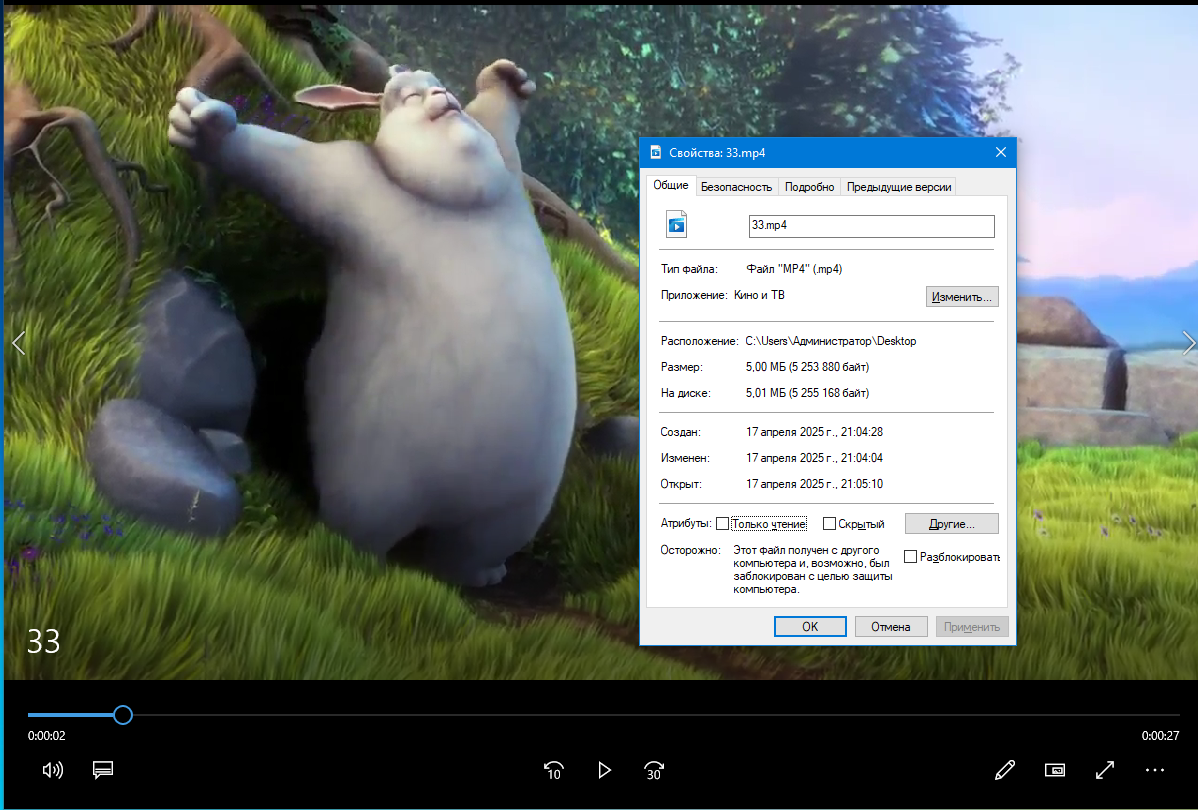


Рис. 1 – Исходные данные

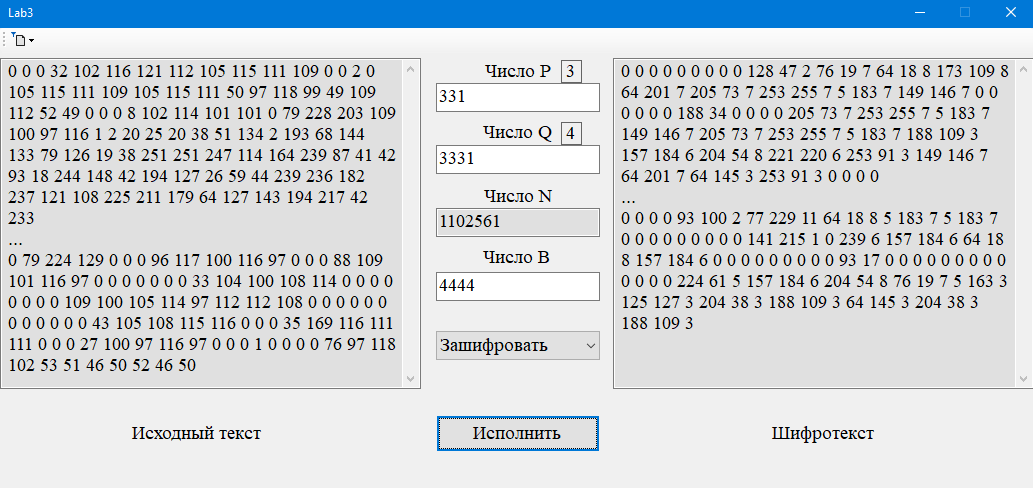


Рис. 2 – Шифрование (после выполнения)

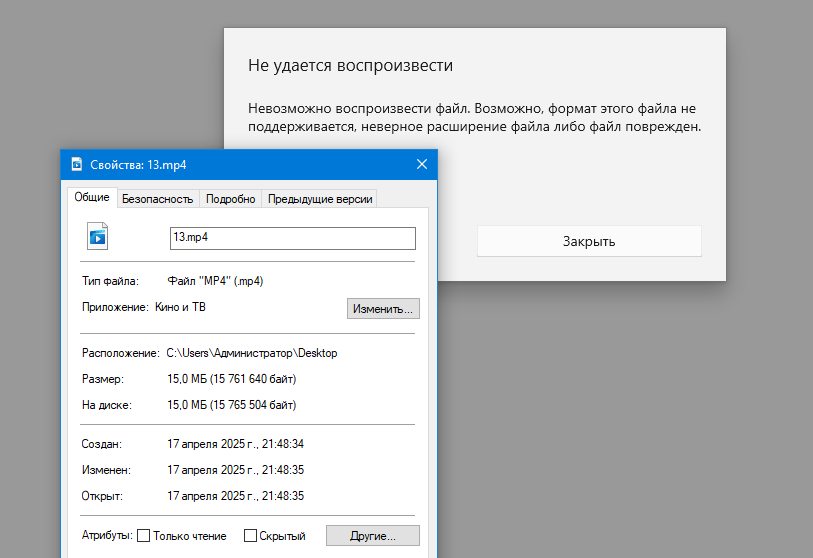


Рис. 3 – Зашифрованные данные

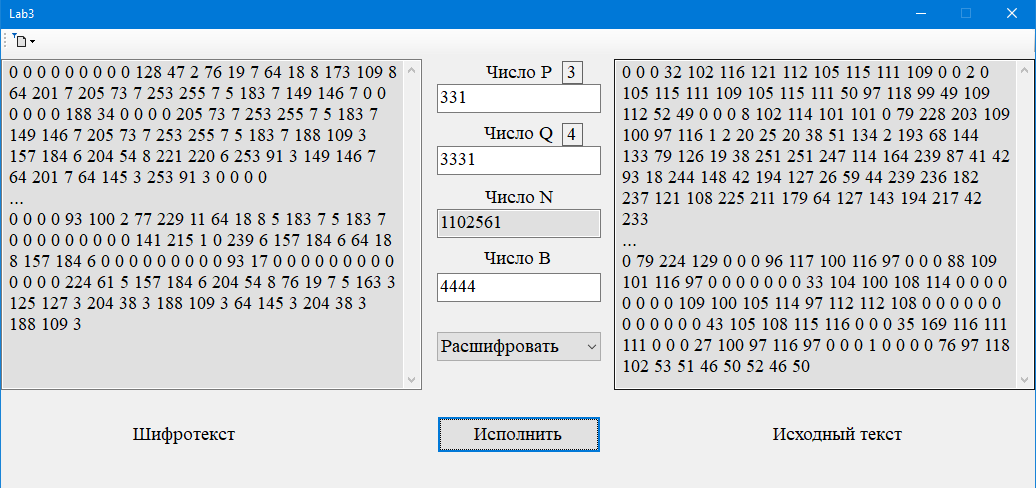


Рис. 4 – Дешифрование (после выполнения)

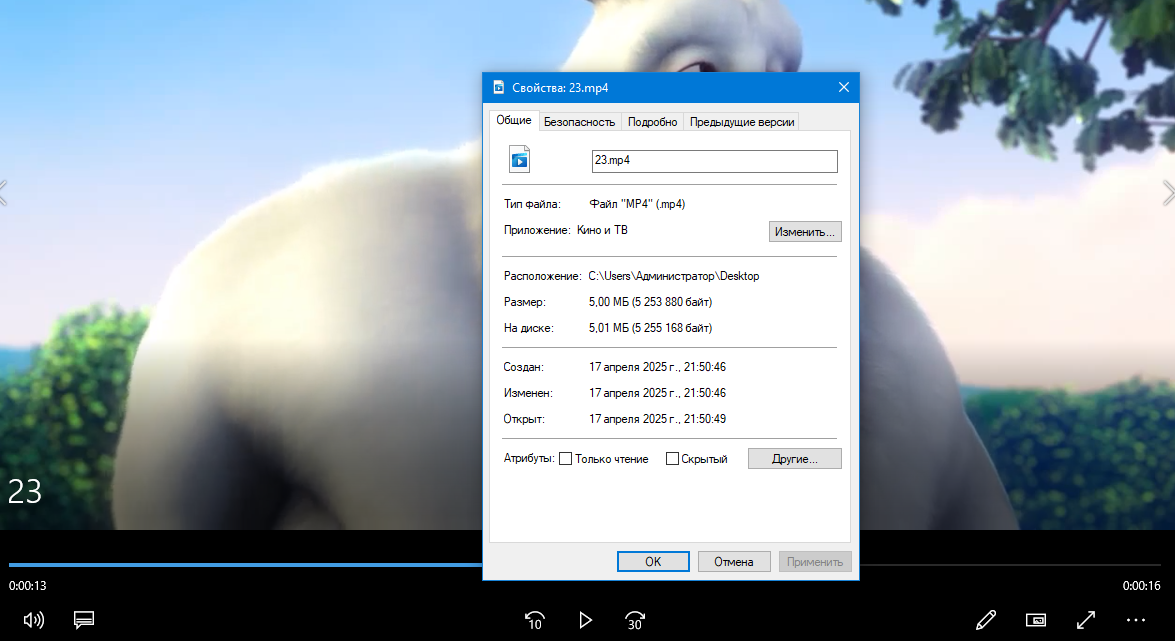


Рис. 5 – Результат дешифрования

Тест 2

**Исходные данные:**

p = 4091

q = 21611

b = 515151

**Ключи:**

Открытый: (n, b) =>(88410601, 515151)

Закрытый: (p, q) =>(4091, 21611)

**Исходный текст:**

255 216 255 224 0 16 74 70 73 70 0 1 1 0 0 1 0 1 0 0 255 226 2 40 73 67 67 95 80 82 79 70 73 76 69 0 1 1 0 0 2 24 0 0 0 0 2 16 0 0 109 110 116 114 82 71 66 32 88 89 90 32 0 0 0 0 0 0 0 0 0 0 0 0 97 99 115 112 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

...

244 225 198 233 195 168 165 251 160 35 125 206 203 82 196 148 209 221 36 0 146 83 119 81 90 150 30 12 217 41 37 118 146 182 148 30 41 56 113 225 36 145 145 100 25 23 184 240 154 210 73 107 49 154 98 226 152 144 66 73 41 136 30 235 69 91 90 73 34 199 95 232 137 191 41 234 210 73 19 198 49 79 186 32 219 221 36 150 189 98 134 38 138 73 36 181 141 227 255 217

**Зашифрованный текст:**

201 102 144 2 255 142 93 1 201 102 144 2 55 127 156 1 0 0 0 0 240 197 125 0 58 196 69 2 190 80 38 2 88 231 61 2 190 80 38 2 0 0 0 0 80 220 7 0 80 220 7 0 0 0 0 0 0 0 0 0 80 220 7 0 0 0 0 0 80 220 7 0 0 0 0 0 0 0 0 0 201 102 144 2 89 59 172 1 162 184 15 0 152 114 58 1 88 231 61 2

...

49 44 235 1 41 91 46 1 88 231 61 2 70 91 149 0 85 244 207 0 128 52 129 1 194 20 109 2 161 142 113 0 224 141 251 0 5 41 117 1 19 229 132 1 44 0 27 1 46 110 155 4 243 39 137 0 194 123 2 3 126 151 29 4 94 185 42 1 250 12 61 4 88 231 61 2 44 0 27 1 235 57 74 0 44 165 84 4 109 25 180 1 201 102 144 2 255 108 101 1

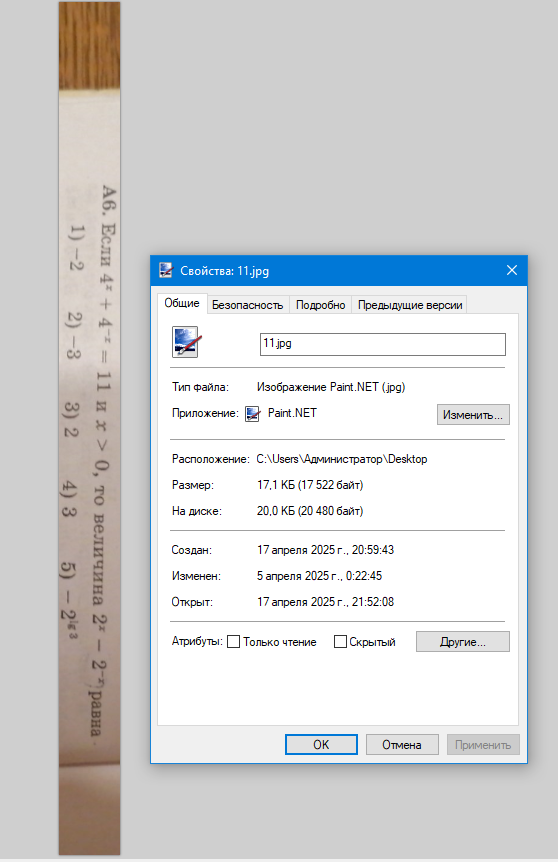


Рис. 6 – Исходные данные

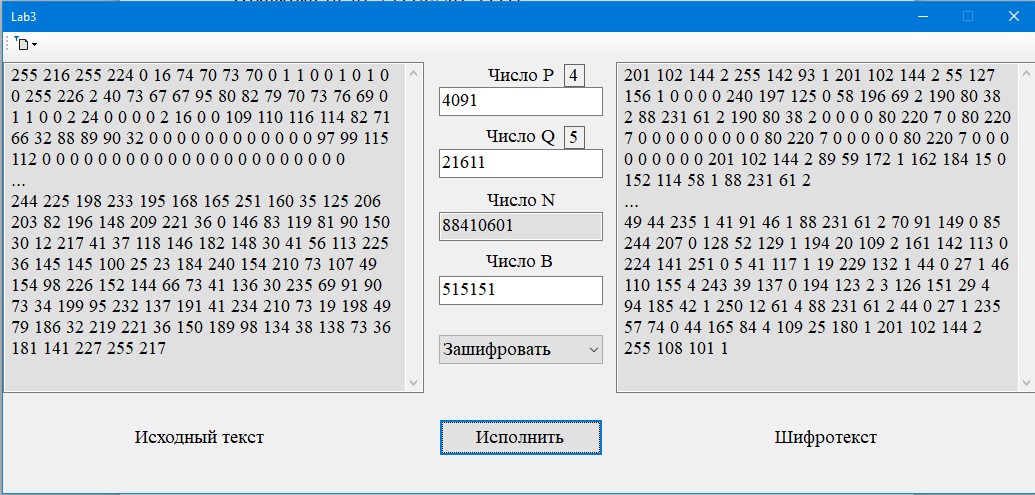


Рис. 7 – Шифрование (после выполнения)

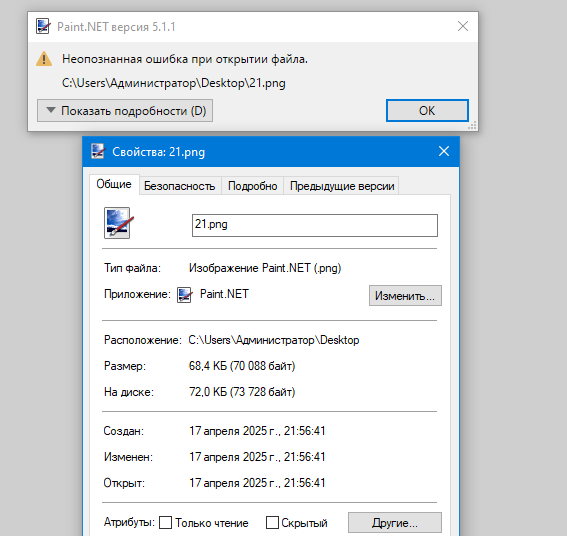


Рис. 8 – Зашифрованные данные

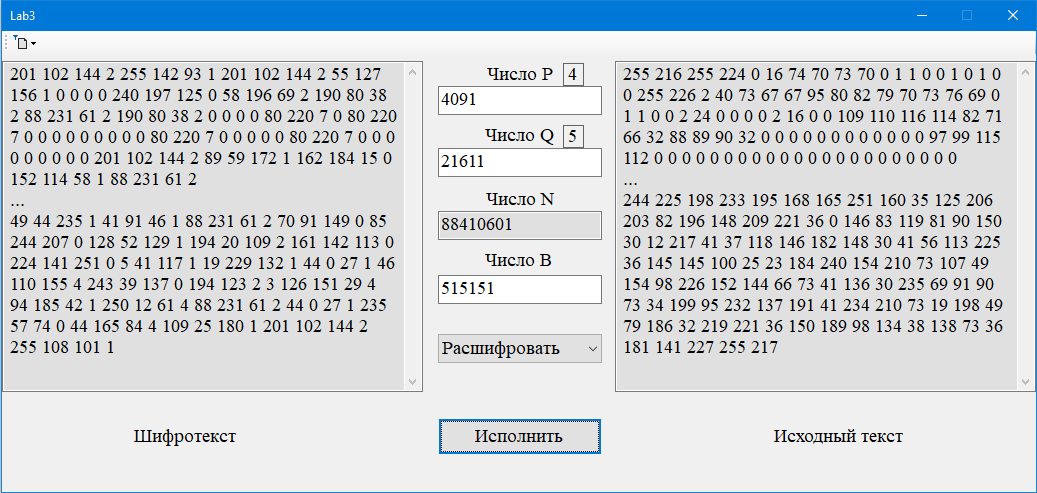


Рис. 9 – Дешифрование (после выполнения)

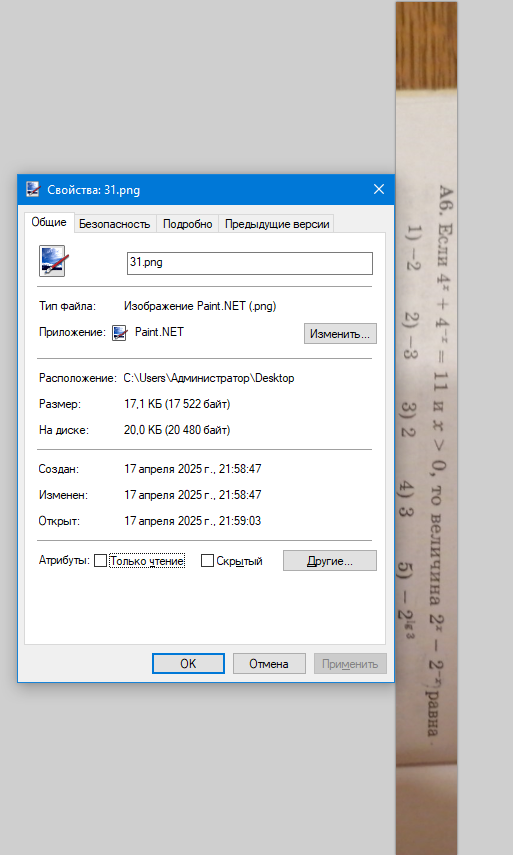


Рис. 10 – Результат дешифрования

Тест 3

**Исходные данные:**

p = 99971

q = 99994813321199

b = 67676781237812

**Ключи:**

Открытый: (n, b) =>( 9996581482533585229, 67676781237812 )

Закрытый: (p, q) =>(99971, 99994813321199)

**Исходный текст:**

208 162 208 176 208 186 32 208 178 32 209 129 209 130 208 176 209 128 208 184 208 189 209 131 32 208 189 208 176 208 183 209 139 208 178 208 176 208 187 208 184 32 209 129 209 130 208 190 209 128 208 190 208 182 208 176 32 208 179 208 190 209 128 208 190 208 180 209 129 208 186 208 184 209 133 32 208 178 208 190 209 128 208 190 209 130 13 10 208 150 208 181 208 187 208 181 208 183 208 189

...

178 208 190 208 179 208 190 32 209 129 208 187 208 190 208 178 208 176 32 208 191 208 181 209 129 208 189 208 184 44 32 208 186 208 190 209 130 208 190 209 128 208 176 209 143 32 209 135 208 176 209 137 208 181 32 208 178 209 129 208 181 208 179 208 190 32 208 189 208 176 32 208 189 208 181 208 188 32 208 184 209 129 208 191 208 190 208 187 208 189 209 143 208 187 208 176 209 129 209 140

**Зашифрованный текст:**

64 179 22 137 191 2 50 0 0 108 243 216 5 95 243 38 0 0 64 179 22 137 191 2 50 0 0 192 188 235 56 24 81 42 0 0 64 179 22 137 191 2 50 0 0 236 40 249 129 156 184 44 0 0 128 202 42 80 167 177 7 0 0 64 179 22 137 191 2 50 0 0 236 107 238 173 50 204 42 0 0 128 202 42 80 167 177 7 0 0 21 11 152 195 76 64 50 0 0 53

...

0 237 47 125 49 68 113 45 0 0 21 11 152 195 76 64 50 0 0 237 118 63 174 227 97 34 0 0 64 179 22 137 191 2 50 0 0 149 128 122 188 41 246 44 0 0 64 179 22 137 191 2 50 0 0 192 188 235 56 24 81 42 0 0 21 11 152 195 76 64 50 0 0 53 177 44 123 42 4 31 0 0 21 11 152 195 76 64 50 0 0 0 113 187 254 59 169 33 0 0

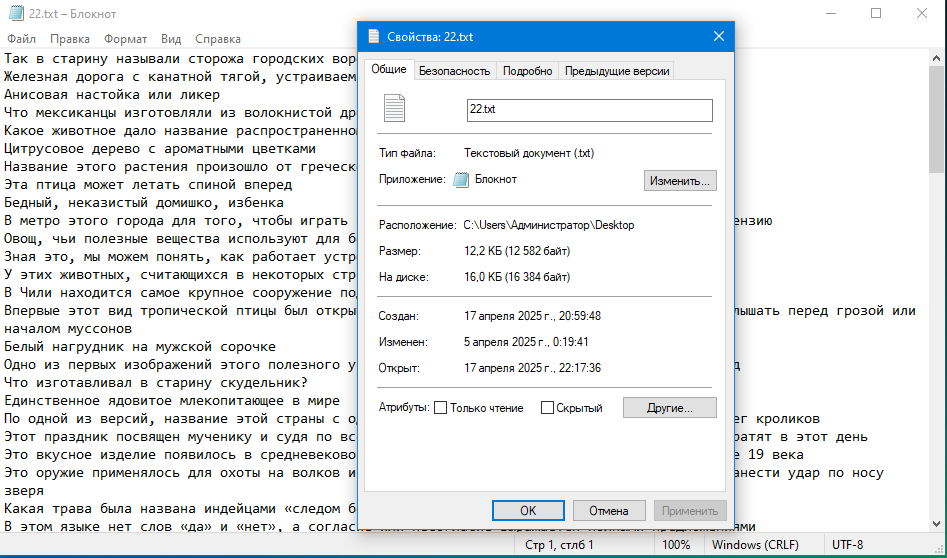


Рис. 11 – Исходные данные

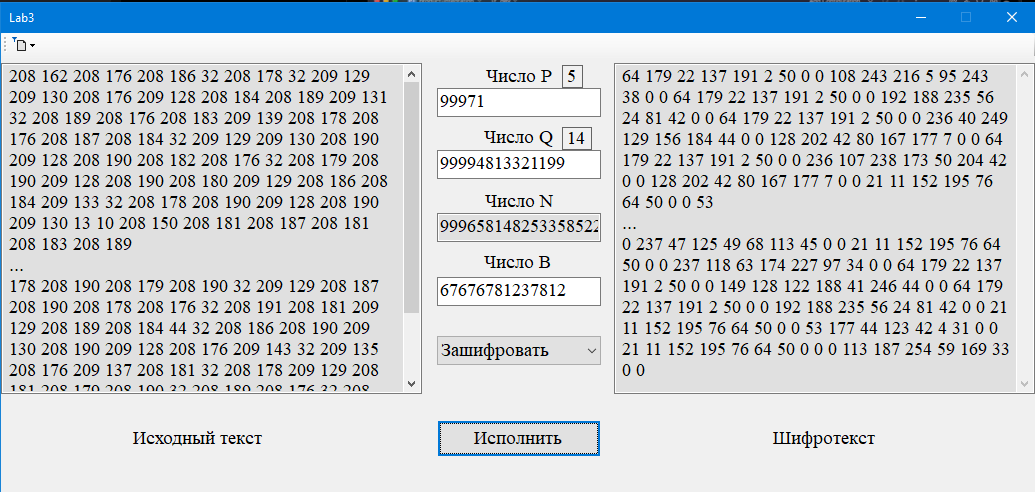


Рис. 12 – Шифрование (после выполнения)

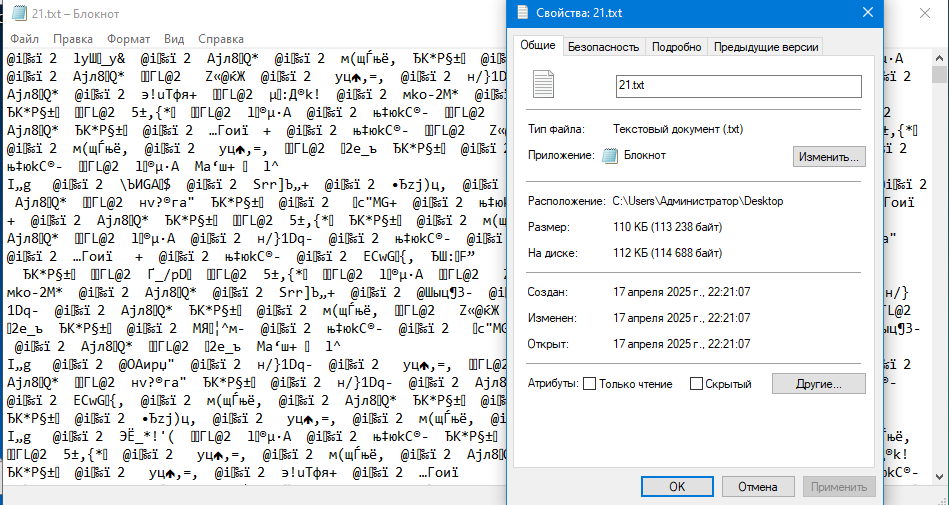


Рис. 13 – Зашифрованные данные

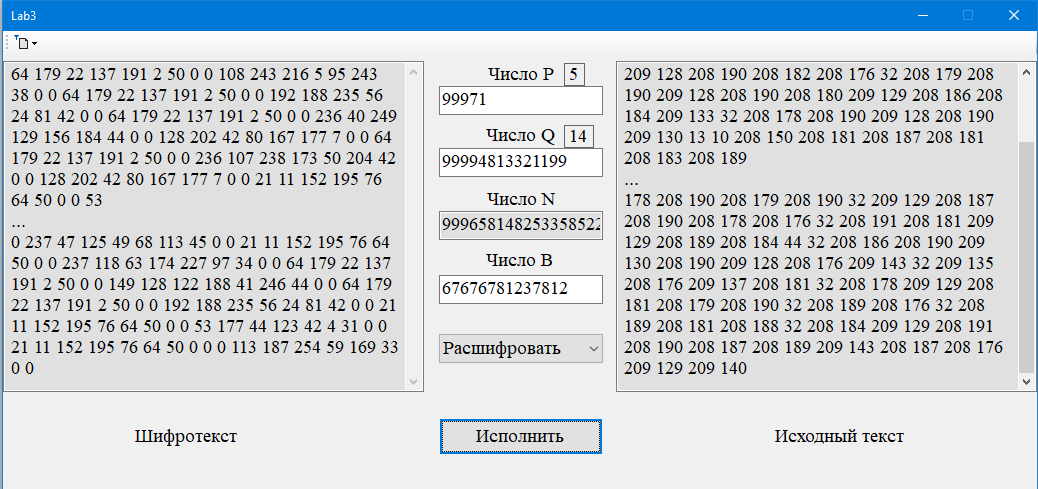


Рис. 14 – Дешифрование (после выполнения)

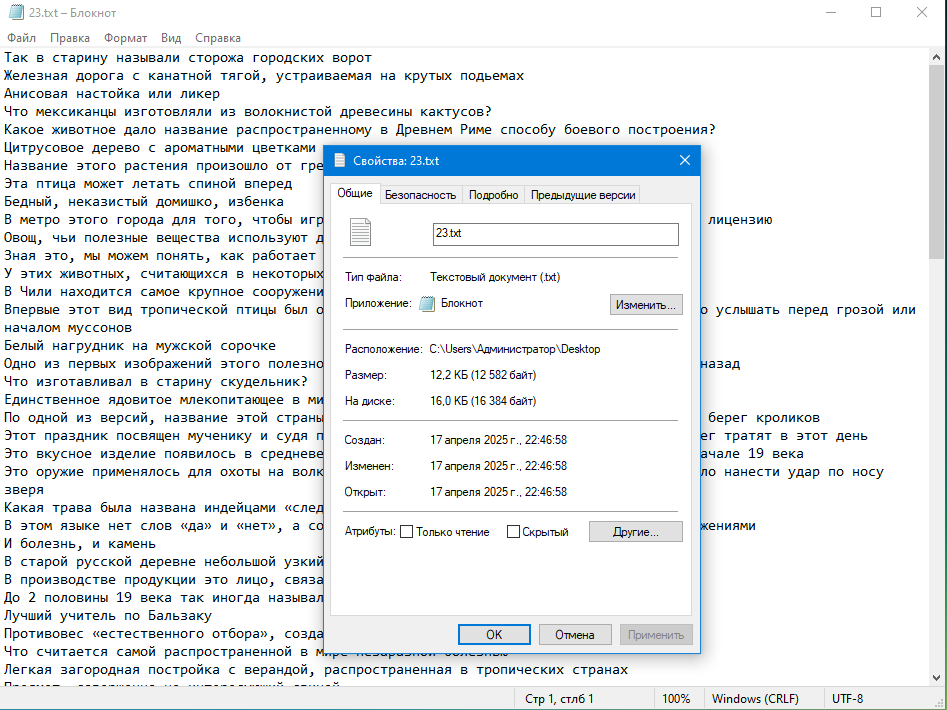


Рис. 15 – Результат дешифрования

Критические ситуации

**Исходные данные:**

p = 999 (Ошибка, вызванная невыполнением 2 условий)

q = -

b = -

**Ключи:**

Открытый: (n, b) => -

Закрытый: (p, q) => -

**Исходный текст:**

-

**Зашифрованный текст:**

-

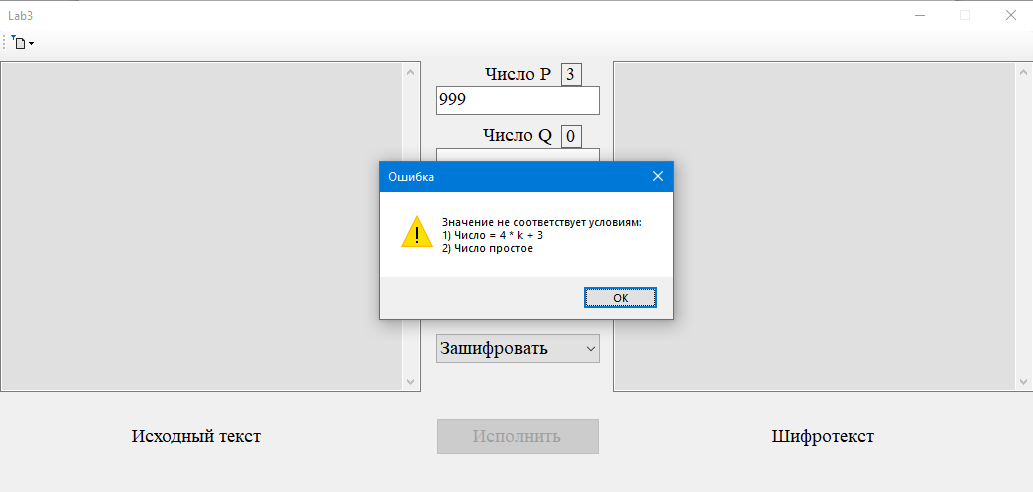


Рис. 16 – Критическая ситуация 1

**Исходные данные:**

p = 4091

q = 21611

(n = 88410601)

b = 5151515151 (Ошибка, вызванная тем, что b >= n)

**Пометка:**

Если b >= n, то программа автоматически заменяет b на значение n-1, так как оно не выходит за обозначенные пределы: 0<=b<n.

В данном случае замена будет на 88410600.

**Ключи:**

Открытый: (n, b) => (88410601, 88410600)

Закрытый: (p, q) => (4091, 21611)

**Исходный текст:**

-

**Зашифрованный текст:**

-

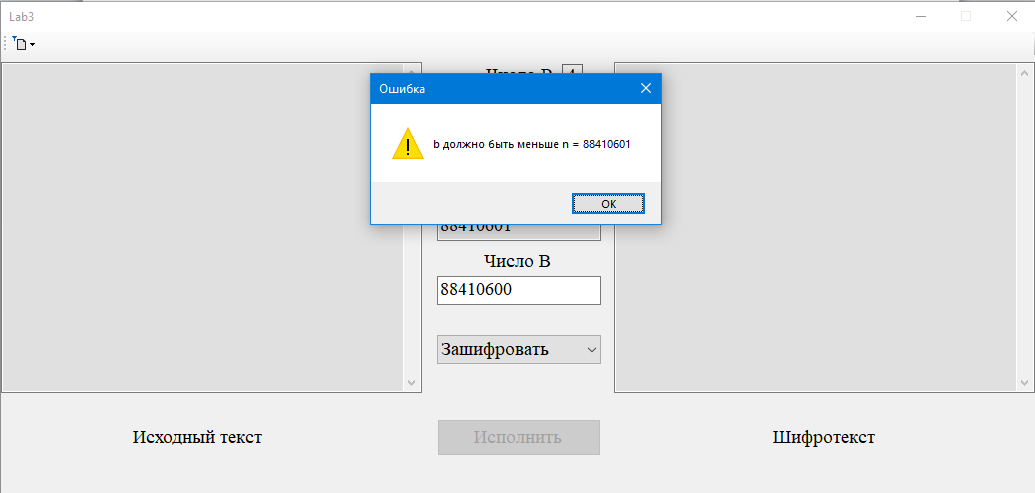


Рис. 17 – Критическая ситуация 2

**Исходные данные:**

p = 4091

q = 21611

(n = 88410601)

b = 515151

**Ключи:**

Открытый: (n, b) => (88410601, 515151)

Закрытый: (p, q) => (4091, 21611)

**Исходный текст:**

208 191 209 145 209 130 209 128 32 208 191 208 181 209 128 208 178 209 139 208 185

**Зашифрованный текст:**

- (Ошибка, вызванная сохранением в файл никаких данных)

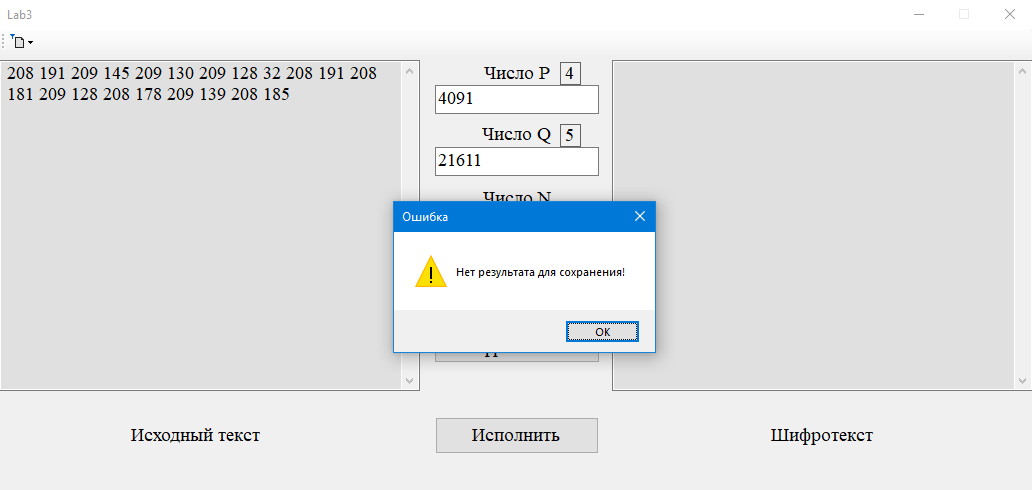


Рис. 17 – Критическая ситуация 3