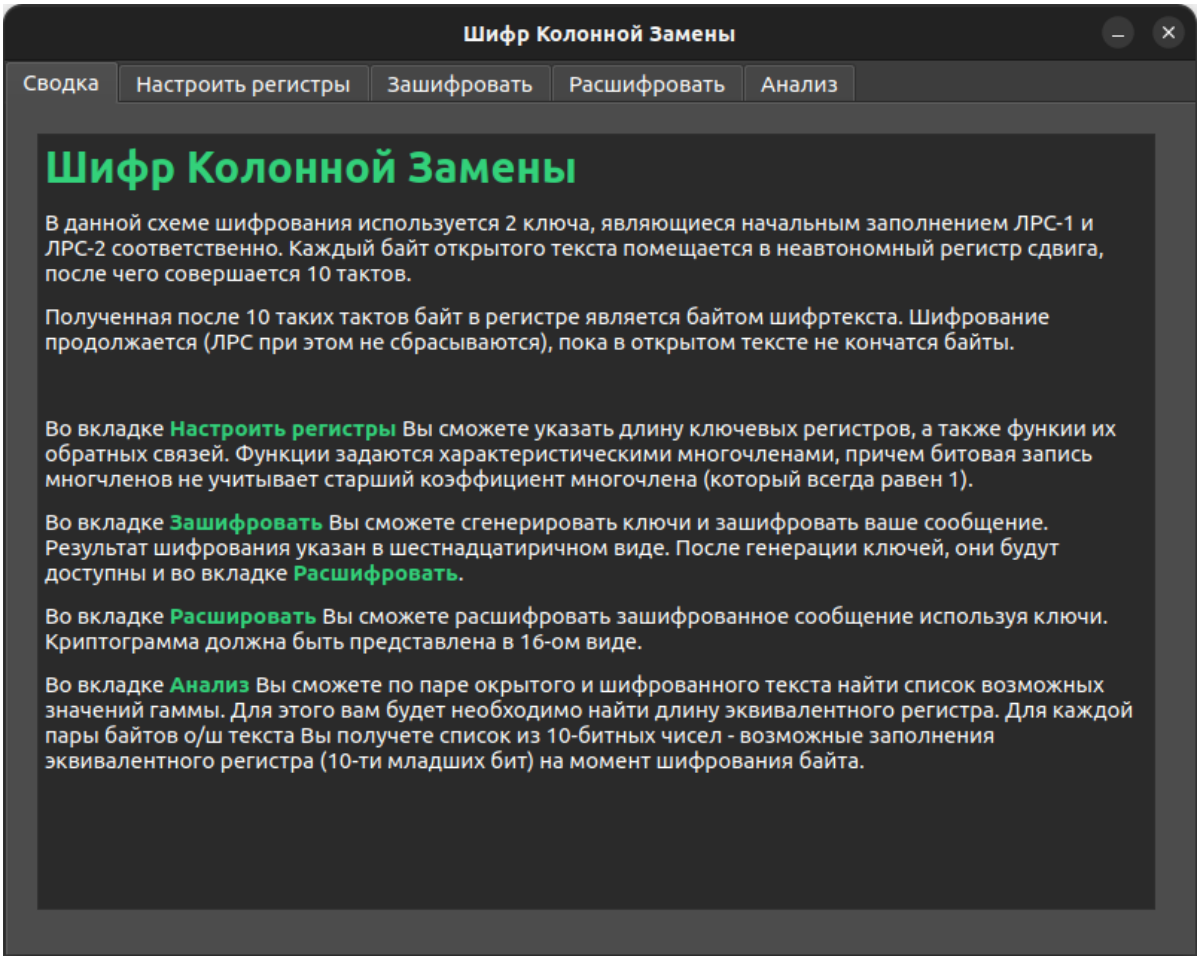
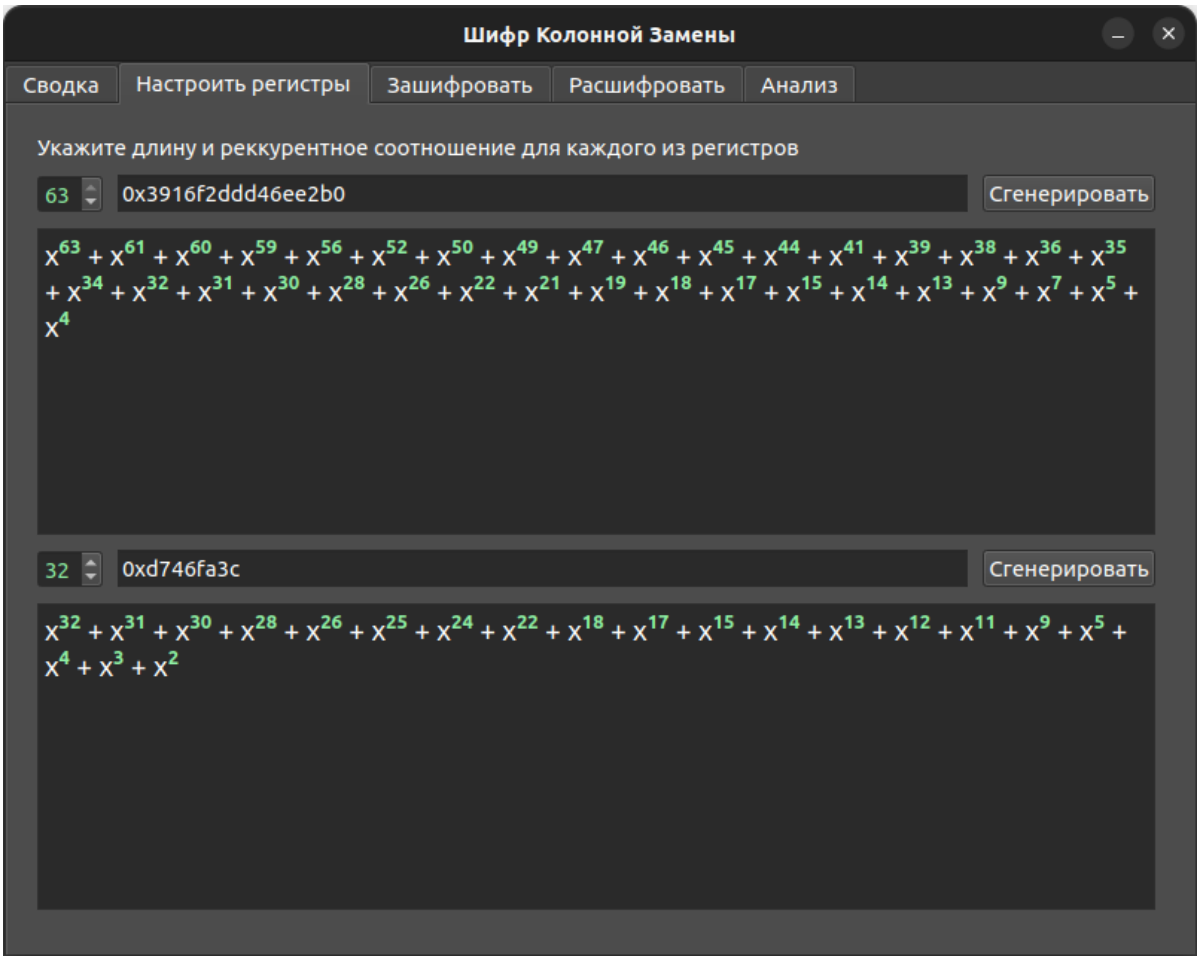
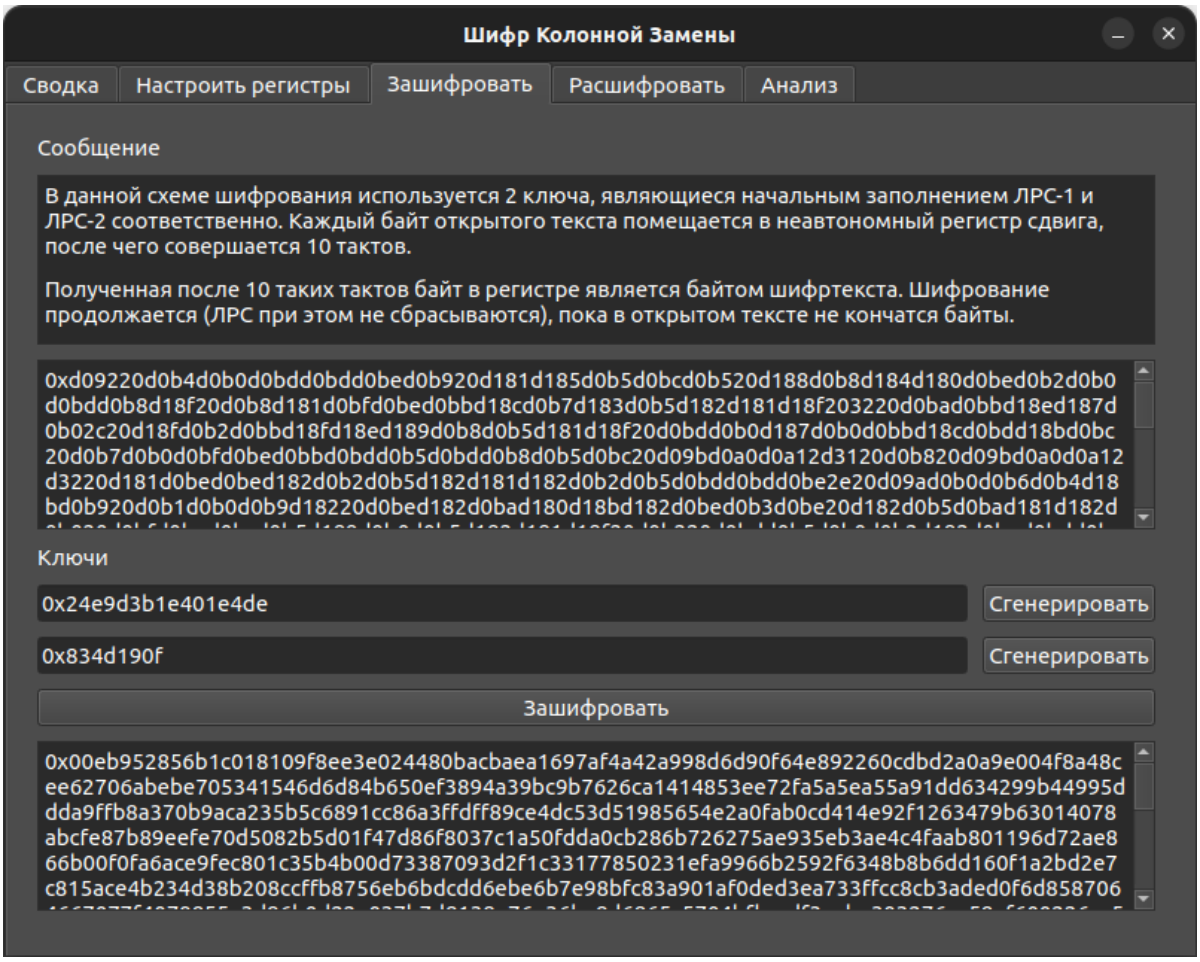
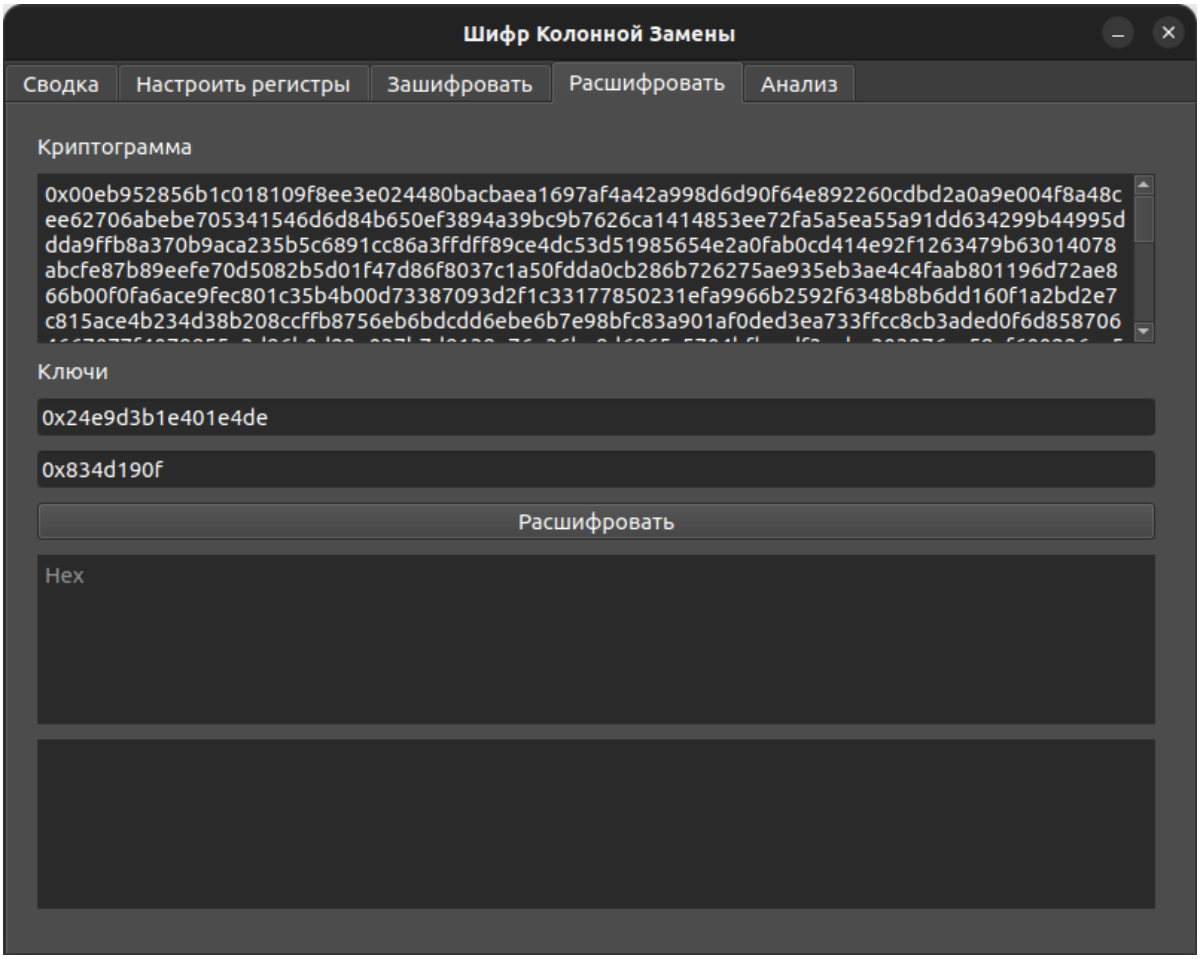
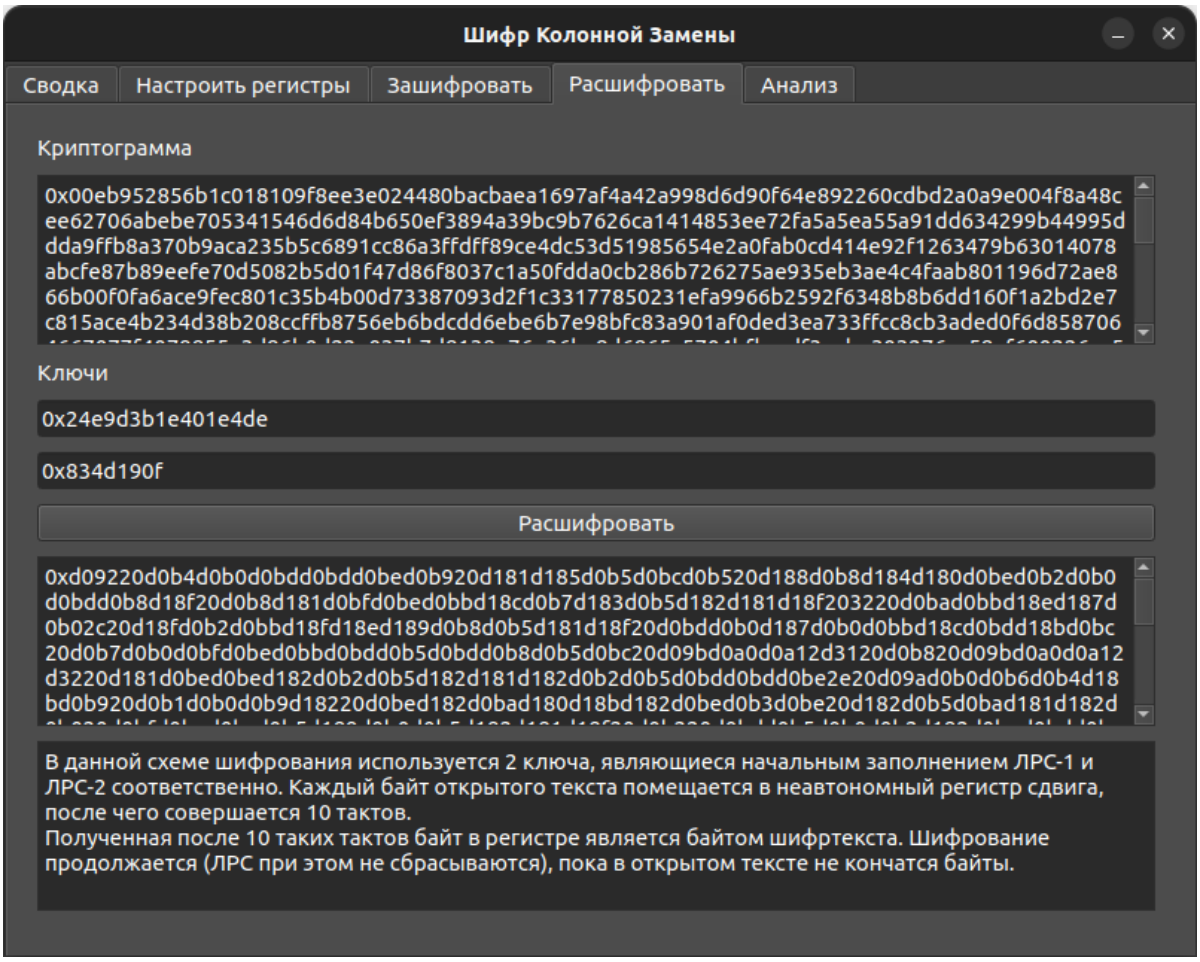
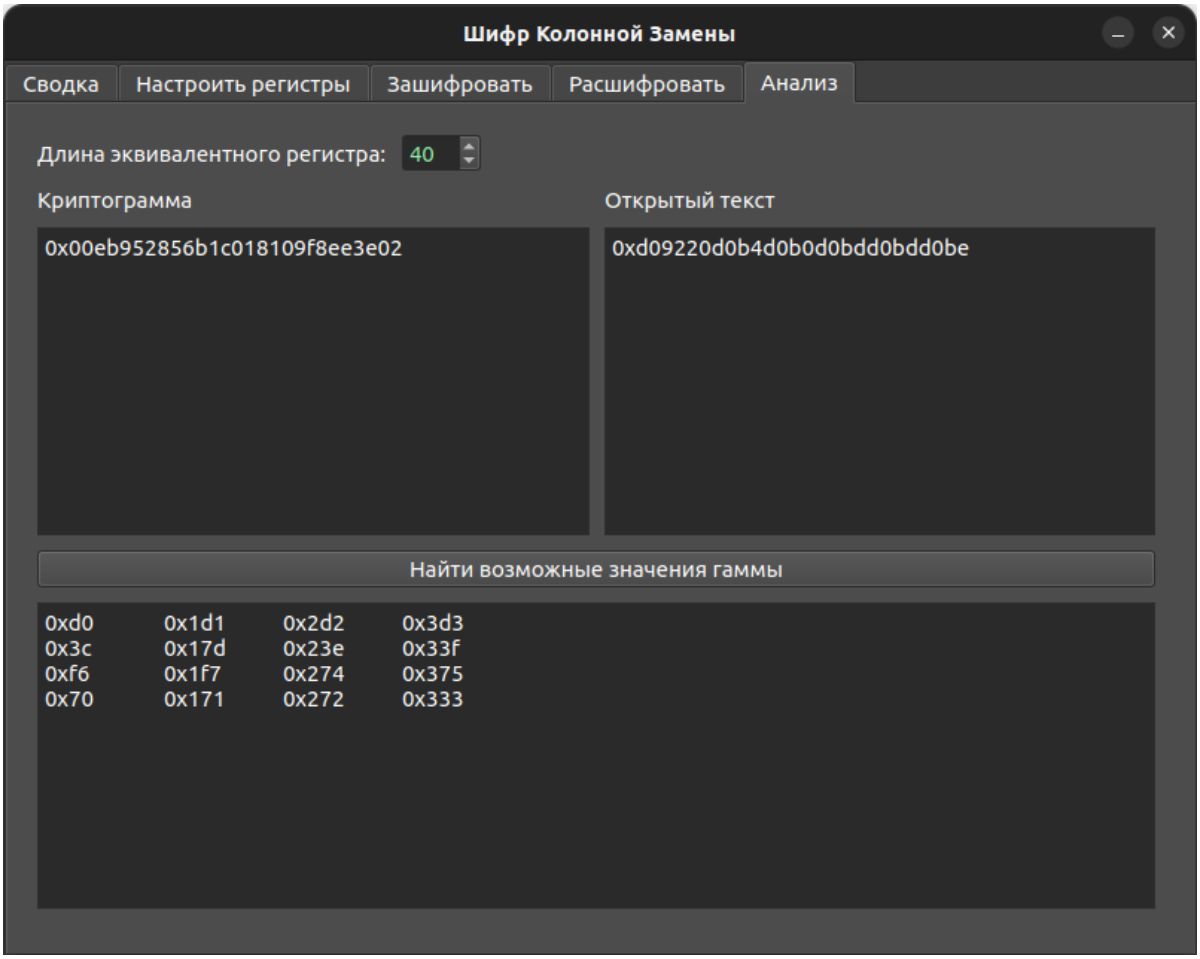

Шифр Колонной Замены
Сводка
Настроить регистры
Зашифровать
Расшифровать
Анализ
Шифр Колонной Замены
В данной схеме шифрования используется 2 ключа, являющиеся начальным заполнением ЛРС-1 и ЛРС-2 соответственно. Каждый байт открытого текста помещается в неавтономный регистр сдвига, после чего совершается 10 тактов.
Полученная после 10 таких тактов байт в регистре является байтом шифртекста. Шифрование продолжается (ЛРС при этом не сбрасываются), пока в открытом тексте не кончатся байты.
Во вкладке Настроить регистры Вы сможете указать длину ключевых регистров, а также функии их обратных связей. Функции задаются характеристическими многочленами, причем битовая запись многчленов не учитывает старший коэффициент многочлена (который всегда равен 1).
Во вкладке Зашифровать Вы сможете сгенерировать ключи и зашифровать ваше сообщение. Результат шифрования указан в шестнадцатиричном виде. После генерации ключей, они будут доступны и во вкладке Расшифровать.
Во вкладке Расшировать Вы сможете расшифровать зашифрованное сообщение используя ключи. Криптограмма должна быть представлена в 16-ом виде.
Во вкладке Анализ Вы сможете по паре окрытого и шифрованного текста найти список возможных значений гаммы. Для этого вам будет необходимо найти длину эквивалентного регистра. Для каждой пары байтов о/ш текста Вы получете список из 10-битных чисел - возможные заполнения эквивалентного регистра (10-ти младших бит) на момент шифрования байта.


Шифр Колонной Замены
Сводка
Настроить регистры
Зашифровать
Расшифровать
Анализ
Укажите длину и реккурентное соотношение для каждого из регистров
63
0x3916f2ddd46ee2b0
Сгенерировать
x63 + x61 + x60 + x59 + x56 + x52 + x50 + x49 + x47 + x46 + x45 + x44 + x41 + x39 + x38 + x36 + x35 + x34 + x32 + x31 + x30 + x28 + x26 + x22 + x21 + x19 + x18 + x17 + x15 + x14 + x13 + x9 + x7 + x5 + x4
32
0xd746fa3c
Сгенерировать
x32 + x31 + x30 + x28 + x26 + x25 + x24 + x22 + x18 + x17 + x15 + x14 + x13 + x12 + x11 + x9 + x5 + x4 + x3 + x2


Шифр Колонной Замены
Сводка
Настроить регистры
Зашифровать
Расшифровать
Анализ
Сообщение
В данной схеме шифрования используется 2 ключа, являющиеся начальным заполнением ЛРС-1 и ЛРС-2 соответственно. Каждый байт открытого текста помещается в неавтономный регистр сдвига, после чего совершается 10 тактов.
Полученная после 10 таких тактов байт в регистре является байтом шифртекста. Шифрование продолжается (ЛРС при этом не сбрасываются), пока в открытом тексте не кончатся байты.
0xd09220d0b4d0b0d0bdd0bdd0bed0b920d181d185d0b5d0bcd0b520d188d0b8d184d180d0bed0b2d0b0
d0bdd0b8d18f20d0b8d181d0bfd0bed0bbd18cd0b7d183d0b5d182d181d18f203220d0bad0bbd18ed187d
0b02c20d18fd0b2d0bbd18fd18ed189d0b8d0b5d181d18f20d0bdd0b0d187d0b0d0bbd18cd0bdd18bd0bc
20d0b7d0b0d0bfd0bed0bbd0bdd0b5d0bdd0b8d0b5d0bc20d09bd0a0d0a12d3120d0b820d09bd0a0d0a12
d3220d181d0bed0bed182d0b2d0b5d182d181d182d0b2d0b5d0bdd0bdd0be2e20d09ad0b0d0b6d0b4d18
bd0b920d0b1d0b0d0b9d18220d0bed182d0bad180d18bd182d0bed0b3d0be20d182d0b5d0bad181d182d
Ключи
0x24e9d3b1e401e4de
Сгенерировать
0x834d190f
Сгенерировать
Зашифровать
0x00eb952856b1c018109f8ee3e024480bacbaea1697af4a42a998d6d90f64e892260cdbd2a0a9e004f8a48c
ee62706abebe705341546d6d84b650ef3894a39bc9b7626ca1414853ee72fa5a5ea55a91dd634299b44995d
dda9ffb8a370b9aca235b5c6891cc86a3ffdff89ce4dc53d51985654e2a0fab0cd414e92f1263479b63014078
abcfe87b89eefe70d5082b5d01f47d86f8037c1a50fdda0cb286b726275ae935eb3ae4c4faab801196d72ae8
66b00f0fa6ace9fec801c35b4b00d73387093d2f1c33177850231efa9966b2592f6348b8b6dd160f1a2bd2e7
c815ace4b234d38b208ccffb8756eb6bdcdd6ebe6b7e98bfc83a901af0ded3ea733ffcc8cb3aded0f6d858706


Шифр Колонной Замены
Сводка
Настроить регистры
Зашифровать
Расшифровать
Анализ
Криптограмма
0x00eb952856b1c018109f8ee3e024480bacbaea1697af4a42a998d6d90f64e892260cdbd2a0a9e004f8a48c
ee62706abebe705341546d6d84b650ef3894a39bc9b7626ca1414853ee72fa5a5ea55a91dd634299b44995d
dda9ffb8a370b9aca235b5c6891cc86a3ffdff89ce4dc53d51985654e2a0fab0cd414e92f1263479b63014078
abcfe87b89eefe70d5082b5d01f47d86f8037c1a50fdda0cb286b726275ae935eb3ae4c4faab801196d72ae8
66b00f0fa6ace9fec801c35b4b00d73387093d2f1c33177850231efa9966b2592f6348b8b6dd160f1a2bd2e7
c815ace4b234d38b208ccffb8756eb6bdcdd6ebe6b7e98bfc83a901af0ded3ea733ffcc8cb3aded0f6d858706
Ключи
0x24e9d3b1e401e4de
0x834d190f
Расшифровать
Hex


Шифр Колонной Замены
Сводка
Настроить регистры
Зашифровать
Расшифровать
Анализ
Криптограмма
0x00eb952856b1c018109f8ee3e024480bacbaea1697af4a42a998d6d90f64e892260cdbd2a0a9e004f8a48c
ee62706abebe705341546d6d84b650ef3894a39bc9b7626ca1414853ee72fa5a5ea55a91dd634299b44995d
dda9ffb8a370b9aca235b5c6891cc86a3ffdff89ce4dc53d51985654e2a0fab0cd414e92f1263479b63014078
abcfe87b89eefe70d5082b5d01f47d86f8037c1a50fdda0cb286b726275ae935eb3ae4c4faab801196d72ae8
66b00f0fa6ace9fec801c35b4b00d73387093d2f1c33177850231efa9966b2592f6348b8b6dd160f1a2bd2e7
c815ace4b234d38b208ccffb8756eb6bdcdd6ebe6b7e98bfc83a901af0ded3ea733ffcc8cb3aded0f6d858706
Ключи
0x24e9d3b1e401e4de
0x834d190f
Расшифровать
0xd09220d0b4d0b0d0bdd0bdd0bed0b920d181d185d0b5d0bcd0b520d188d0b8d184d180d0bed0b2d0b0
d0bdd0b8d18f20d0b8d181d0bfd0bed0bbd18cd0b7d183d0b5d182d181d18f203220d0bad0bbd18ed187d
0b02c20d18fd0b2d0bbd18fd18ed189d0b8d0b5d181d18f20d0bdd0b0d187d0b0d0bbd18cd0bdd18bd0bc
20d0b7d0b0d0bfd0bed0bbd0bdd0b5d0bdd0b8d0b5d0bc20d09bd0a0d0a12d3120d0b820d09bd0a0d0a12
d3220d181d0bed0bed182d0b2d0b5d182d181d182d0b2d0b5d0bdd0bdd0be2e20d09ad0b0d0b6d0b4d18
bd0b920d0b1d0b0d0b9d18220d0bed182d0bad180d18bd182d0bed0b3d0be20d182d0b5d0bad181d182d
В данной схеме шифрования используется 2 ключа, являющиеся начальным заполнением ЛРС-1 и ЛРС-2 соответственно. Каждый байт открытого текста помещается в неавтономный регистр сдвига, после чего совершается 10 тактов.
Полученная после 10 таких тактов байт в регистре является байтом шифртекста. Шифрование продолжается (ЛРС при этом не сбрасываются), пока в открытом тексте не кончатся байты.


Шифр Колонной Замены
Сводка
Настроить регистры
Зашифровать
Расшифровать
Анализ
Длина эквивалентного регистра:
40
Криптограмма
0x00eb952856b1c018109f8ee3e02
Открытый текст
0xd09220d0b4d0b0d0bdd0bdd0be
Найти возможные значения гаммы
0xd0 0x1d1 0x2d2 0x3d3
0x3c 0x17d 0x23e 0x33f
0xf6 0x1f7 0x274 0x375
0x70 0x171 0x272 0x333