Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: ТИ (Теория информации)

ОТЧЕТ

по лабораторной работе № 2

Тема работы: Потоковое шифрование

Выполнил: гр. 951007 Воривода М.А.

Проверила: Болтак С.В.

Минск 2021

**СОДЕРЖАНИЕ**

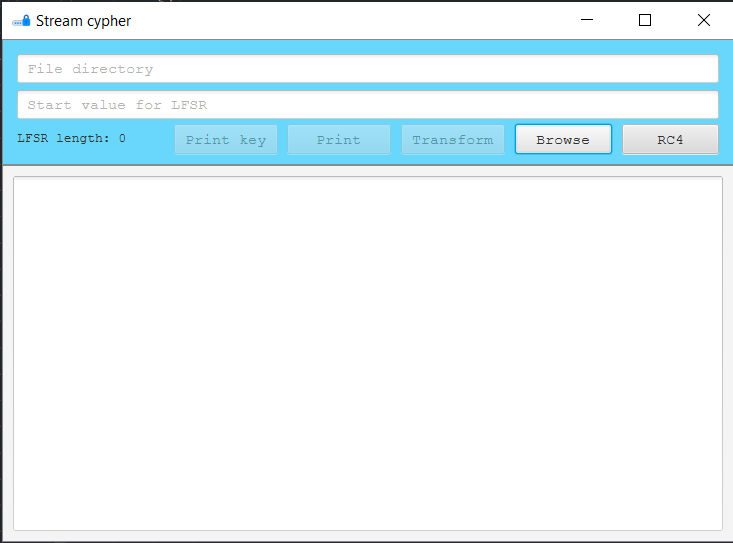
[1 SMOKE TEST 3](#_Toc66384686)

[2 ТАБЛИЦА И СКРИНШОТЫ ТЕСТОВ 6](#_Toc66384687)

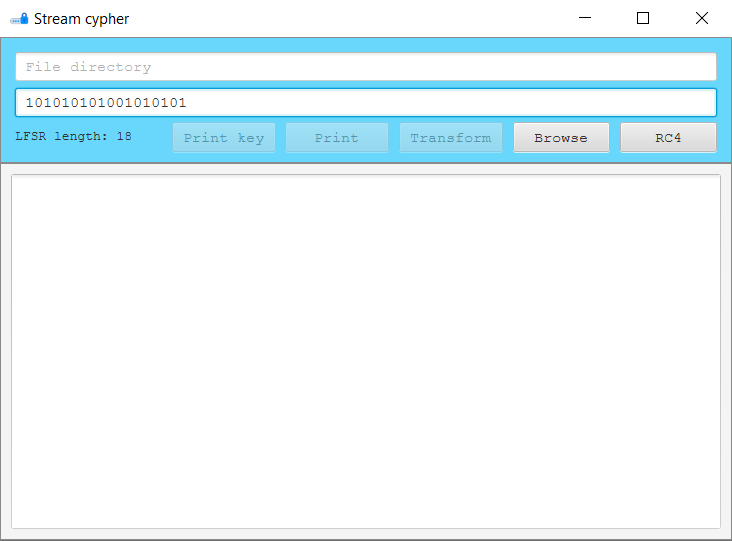
3 ОСНОВНОЙ ТЕСТ……………………………………………………………17

# SMOKE TEST

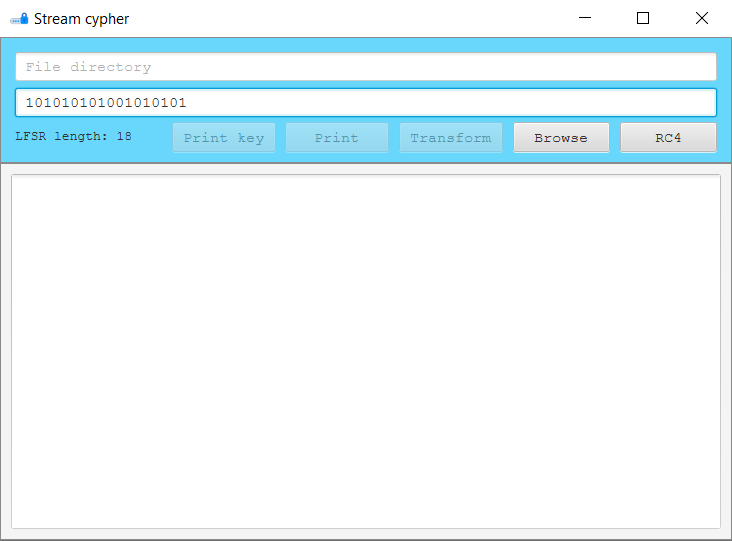
1. Запуск программы:

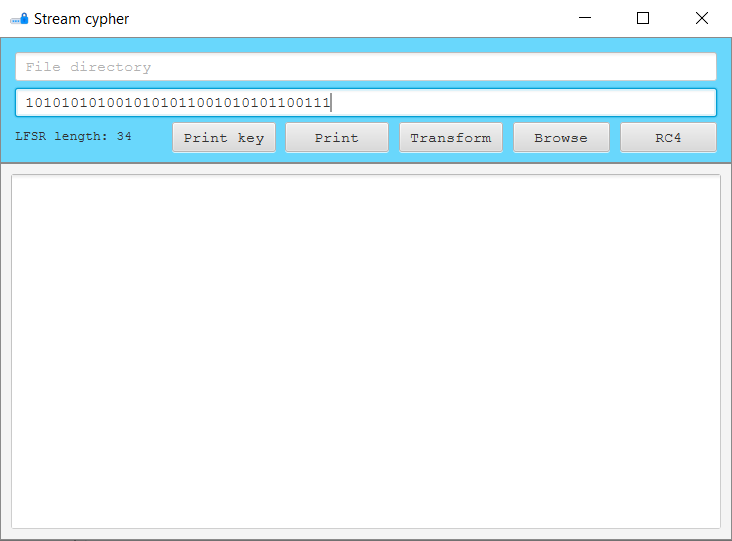


1. Проверка ключа:
   1. Должны быть только 0 и 1:

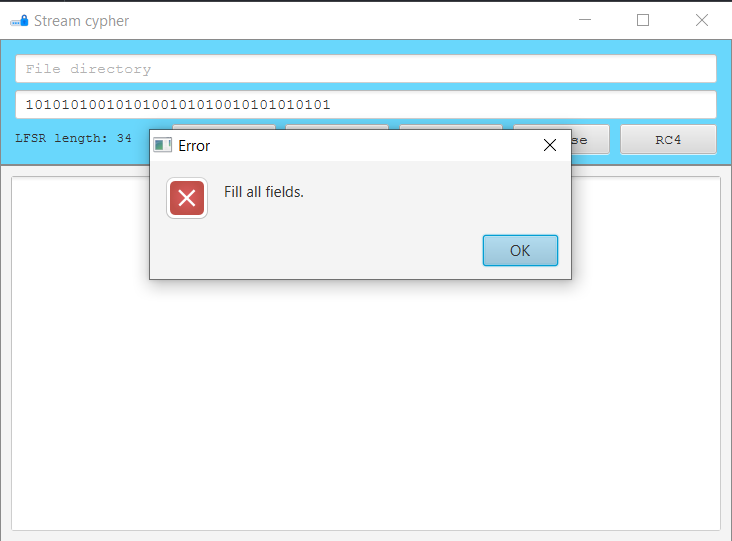


* 1. Длина должна быть равна 34:

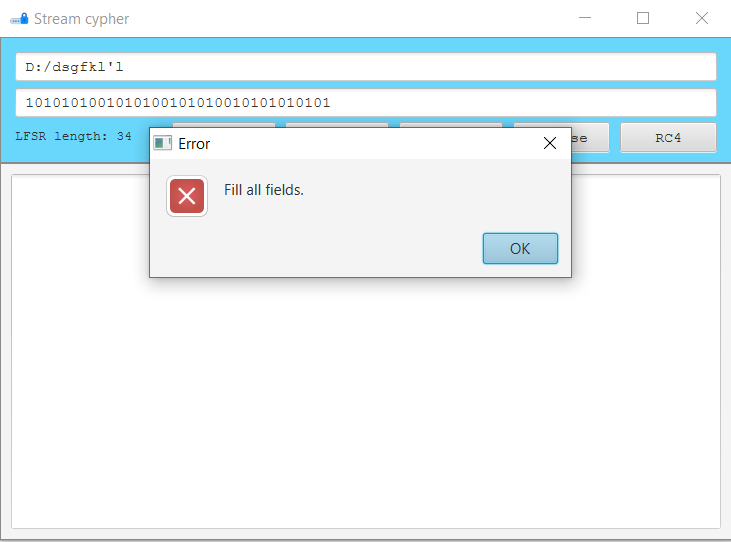




1. Выбор файла:
   1. Попытка зашифровать с пустым полем:



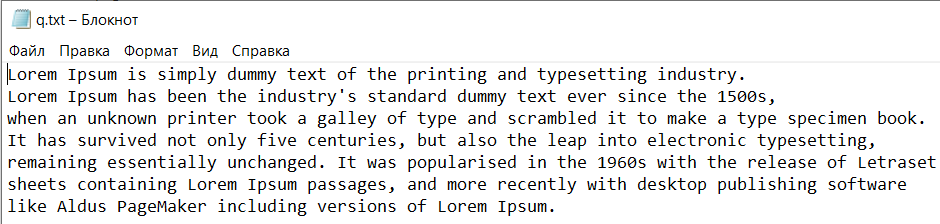
* 1. Попытка зашифровать несуществующий файл:



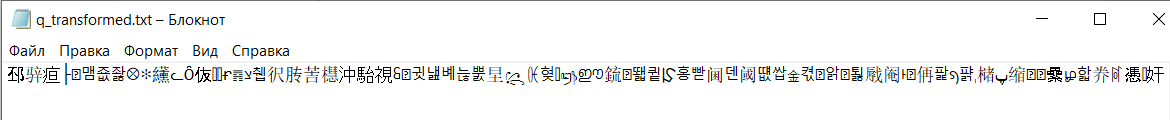
# 2 ТАБЛИЦА И СКРИНШОТЫ ТЕСТОВ

**Метод потокового шифрования с помощью LFSR**

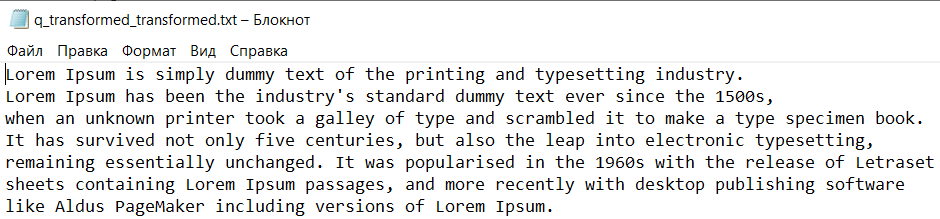
**Исходный текст:**



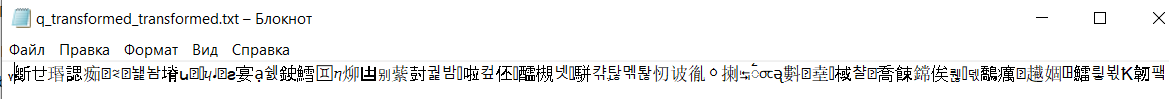
**Зашифрованный текст:**



**Расшифровка правильным ключом:**



**Расшифровка неправильным ключом:**



ݍ斲せ瑉諰㾒⪝놽놤塉ꭎ૛ⴗ♩ꙅ宴ạ쉜鉂鱈♊ⴄ㶯凷别䔝尌궕밤ᯀ啦컾伾ﶺ醽槻넷﫝駢캮ֶ탆멖퇂㣼诐㣧ㆁ揦⭾߱⳪ᶕ㪹㙓᯸棫챨喬餗鏛俟뤦᪵덳鷮癘䟌婟ꖸ鱩릫뵋Ꝁ韌퍀ꎻﱶ汙㘼ᓲᑡ덯畨廿ﲔ੥懊鍚唂꟏㪯䰂⌣붦ⶬﰏ┯ꨆ廮뇚㘏ꝃꌬ긴펰㞤₼ݼ힐됴拁賳﶐倚럛숎蔂䫑ฝ鍳鼬ṅ暑뤤≳勺∪铽ᘮ䋡١⵷彵솕甊琲ﵲ啜븰튕林ñ꺨쎘衻䡹숐蕟แᄟ쮙턬梳䎳닧匜ၯ覩乢刹錿ⴇ䝨濿푧Ⴤ뫕있㫢훘룠좕䵡盯풏糪⹸һ팲脎⣈俟㦛쿊䃮ᎇ錘巎硩ꟊԶ竝묋澑⻉㥔雦轤ꎛধ쳃榀搚ᚯ乌읧뎅㞴貎癧Ⴥρ혪鿽五࡭桲⒀毥鑤煭轷凵㘹쑛鬼훃䙖䫧㱕쓖裌科릺䰕櫟䛭胳컮豄鳒盁㧍莋꘏䪽ﳁࣜ쩯拴Ê퟉锴鹵

**Процесс шифрования:**

01001100(L) ^ 10101010 = 11100110(￦)

01101111(o) ^ 10100101 = 11001010(ￊ)

01110010(r) ^ 01001010 = 00111000(8)

01100101(e) ^ 10010101 = 11110000(￰)

01101101(m) ^ 01100111 = 00001010(

)

00100000( ) ^ 10011010 = 10111010(ﾺ)

01001001(I) ^ 10100000 = 11101001(￩)

01110000(p) ^ 00010011 = 01100011(c)

01110011(s) ^ 01101110 = 00011101()

01110101(u) ^ 00100000 = 01010101(U)

01101101(m) ^ 01000001 = 00101100(,)

00100000( ) ^ 00000101 = 00100101(%)

01101001(i) ^ 01100101 = 00001100()

01110011(s) ^ 00100100 = 01010111(W)

00100000( ) ^ 11001001 = 11101001(￩)

01110011(s) ^ 01011000 = 00101011(+)

01101001(i) ^ 00100100 = 01001101(M)

01101101(m) ^ 10110000 = 11011101(￝)

01110000(p) ^ 11111001 = 10001001(ﾉ)

01101100(l) ^ 11100011 = 10001111(ﾏ)

01111001(y) ^ 11000001 = 10111000(ﾸ)

00100000( ) ^ 00101001 = 00001001( )

01100100(d) ^ 11011101 = 10111001(ﾹ)

01110101(u) ^ 00011110 = 01101011(k)

01101101(m) ^ 01001000 = 00100101(%)

01101101(m) ^ 10000001 = 11101100(￬)

01111001(y) ^ 11100001 = 10011000(ﾘ)

00100000( ) ^ 10001010 = 10101010(ﾪ)

01110100(t) ^ 00010000 = 01100100(d)

01100101(e) ^ 01101111 = 00001010(

)

01111000(x) ^ 00101100 = 01010100(T)

01110100(t) ^ 11000101 = 10110001(ﾱ)

00100000( ) ^ 10011110 = 10111110(ﾾ)

01101111(o) ^ 00111110 = 01010001(Q)

01100110(f) ^ 01111100 = 00011010()

00100000( ) ^ 00101101 = 00001101()

01110100(t) ^ 10100100 = 11010000(￐)

01101000(h) ^ 01100111 = 00001111()

01100101(e) ^ 11001001 = 10101100(ﾬ)

00100000( ) ^ 00110011 = 00010011()

01110000(p) ^ 11111000 = 10001000(ﾈ)

01110010(r) ^ 01110001 = 00000011()

01101001(i) ^ 01100000 = 00001001( )

01101110(n) ^ 00000011 = 01101101(m)

01110100(t) ^ 10101011 = 11011111(￟)

01101001(i) ^ 11110101 = 10011100(ﾜ)

01101110(n) ^ 00110000 = 01011110(^)

01100111(g) ^ 01010110 = 00110001(1)

00100000( ) ^ 11001110 = 11101110(￮)

01100001(a) ^ 00011111 = 01111110(~)

01101110(n) ^ 11111000 = 10010110(ﾖ)

01100100(d) ^ 11100110 = 10000010(ﾂ)

00100000( ) ^ 11100101 = 11000101(ￅ)

01110100(t) ^ 11001101 = 10111001(ﾹ)

01111001(y) ^ 10000101 = 11111100(￼)

01110000(p) ^ 10111101 = 11001101(ￍ)

01100101(e) ^ 00000011 = 01100110(f)

01101110(n) ^ 11011110 = 10110000(ﾰ)

01100100(d) ^ 11100111 = 10000011(ﾃ)

01100001(a) ^ 00011110 = 01111111()

01110010(r) ^ 01000000 = 00110010(2)

01100100(d) ^ 00101000 = 01001100(L)

00100000( ) ^ 11010000 = 11110000(￰)

01100100(d) ^ 00111100 = 01011000(X)

01110101(u) ^ 01100001 = 00010100()

01101101(m) ^ 11101111 = 10000010(ﾂ)

01101101(m) ^ 00101000 = 01000101(E)

01111001(y) ^ 10001100 = 11110101(￵)

00100000( ) ^ 10101011 = 10001011(ﾋ)

01110100(t) ^ 11001000 = 10111100(ﾼ)

01100101(e) ^ 00101101 = 01001000(H)

01111000(x) ^ 10000011 = 11111011(￻)

01110100(t) ^ 01011111 = 00101011(+)

00100000( ) ^ 01000110 = 01100110(f)

01100101(e) ^ 11110111 = 10010010(ﾒ)

01110110(v) ^ 10001000 = 11111110()

01100101(e) ^ 11011001 = 10111100(ﾼ)

01110010(r) ^ 00100111 = 01010101(U)

00100000( ) ^ 11100000 = 11000000(￀)

01110011(s) ^ 01111100 = 00001111()

01101001(i) ^ 11011000 = 10110001(ﾱ)

01101110(n) ^ 01101000 = 00000110()

01100011(c) ^ 01101100 = 00001111()

01100101(e) ^ 10101001 = 11001100(ￌ)

00100000( ) ^ 01000001 = 01100001(a)

01110100(t) ^ 01011001 = 00101101(-)

01101000(h) ^ 11100111 = 10001111(ﾏ)

01100101(e) ^ 00000011 = 01100110(f)

00100000( ) ^ 01011000 = 01111000(x)

00110001(1) ^ 01111110 = 01001111(O)

00110101(5) ^ 10010010 = 10100111(ﾧ)

00110000(0) ^ 10001011 = 10111011(ﾻ)

00110000(0) ^ 11110000 = 11000000(￀)

01110011(s) ^ 01001010 = 00111001(9)

00101100(,) ^ 10111010 = 10010110(ﾖ)

00100000( ) ^ 10010110 = 10110110(ﾶ)

00001101() ^ 10000011 = 10001110(ﾎ)

00001010(

) ^ 01010111 = 01011101(])

01110111(w) ^ 00101110 = 01011001(Y)

01101000(h) ^ 01111111 = 00010111()

01100101(e) ^ 10110011 = 11010110(ￖ)

01101110(n) ^ 01100100 = 00001010(

)

00100000( ) ^ 11101001 = 11001001(￉)

01100001(a) ^ 11001101 = 10101100(ﾬ)

01101110(n) ^ 11111001 = 10010111(ﾗ)

00100000( ) ^ 00000001 = 00100001(!)

01110101(u) ^ 11100100 = 10010001(ﾑ)

01101110(n) ^ 01010010 = 00111100(<)

01101011(k) ^ 10001001 = 11100010(￢)

01101110(n) ^ 00010100 = 01111010(z)

01101111(o) ^ 00011001 = 01110110(v)

01110111(w) ^ 01000111 = 00110000(0)

01101110(n) ^ 11110110 = 10011000(ﾘ)

00100000( ) ^ 01000110 = 01100110(f)

01110000(p) ^ 01001001 = 00111001(9)

……………………………………………………………………………………………

**Процесс генерации ключа**

Полином: x^34 + x^15 + x^14 + x + 1

Начальное состояние: 1111111111111111111111111111111111

После такта №1:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)111111111111(0)

После такта №2:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)111111111110(1)

После такта №3:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)111111111101(0)

После такта №4:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)111111111010(1)

После такта №5:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)111111110101(0)

После такта №6:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)111111101010(1)

После такта №7:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)111111010101(0)

После такта №8:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)111110101010(1)

После такта №9:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)111101010101(0)

После такта №10:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)111010101010(1)

После такта №11:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)110101010101(0)

После такта №12:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)101010101010(1)

После такта №13:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(1)010101010101(0)

После такта №14:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(1)(0)101010101010(0)

После такта №15:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111111(0)(1)010101010100(0)

После такта №16:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111110(1)(0)101010101000(0)

После такта №17:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111101(0)(1)010101010000(0)

После такта №18:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111111010(1)(0)101010100000(0)

После такта №19:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111110101(0)(1)010101000000(0)

После такта №20:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111101010(1)(0)101010000000(0)

После такта №21:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111111010101(0)(1)010100000000(0)

После такта №22:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111110101010(1)(0)101000000000(0)

После такта №23:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111101010101(0)(1)010000000000(0)

После такта №24:

Сгенерированный ключ: 1

Состояние регистра: (1)111111111010101010(1)(0)100000000000(0)

После такта №25:

Сгенерированный ключ: 1

Состояние регистра: (1)111111110101010101(0)(1)000000000000(0)

После такта №26:

Сгенерированный ключ: 1

Состояние регистра: (1)111111101010101010(1)(0)000000000000(0)

После такта №27:

Сгенерированный ключ: 1

Состояние регистра: (1)111111010101010101(0)(0)000000000000(1)

После такта №28:

Сгенерированный ключ: 1

Состояние регистра: (1)111110101010101010(0)(0)000000000001(0)

После такта №29:

Сгенерированный ключ: 1

Состояние регистра: (1)111101010101010100(0)(0)000000000010(1)

После такта №30:

Сгенерированный ключ: 1

Состояние регистра: (1)111010101010101000(0)(0)000000000101(0)

После такта №31:

Сгенерированный ключ: 1

Состояние регистра: (1)110101010101010000(0)(0)000000001010(1)

После такта №32:

Сгенерированный ключ: 1

Состояние регистра: (1)101010101010100000(0)(0)000000010101(0)

После такта №33:

Сгенерированный ключ: 1

Состояние регистра: (1)010101010101000000(0)(0)000000101010(1)

После такта №34:

Сгенерированный ключ: 1

Состояние регистра: (0)101010101010000000(0)(0)000001010101(0)

После такта №35:

Сгенерированный ключ: 0

Состояние регистра: (1)010101010100000000(0)(0)000010101010(0)

После такта №36:

Сгенерированный ключ: 1

Состояние регистра: (0)101010101000000000(0)(0)000101010100(1)

После такта №37:

Сгенерированный ключ: 0

Состояние регистра: (1)010101010000000000(0)(0)001010101001(1)

После такта №38:

Сгенерированный ключ: 1

Состояние регистра: (0)101010100000000000(0)(0)010101010011(0)

После такта №39:

Сгенерированный ключ: 0

Состояние регистра: (1)010101000000000000(0)(0)101010100110(0)

После такта №40:

Сгенерированный ключ: 1

Состояние регистра: (0)101010000000000000(0)(1)010101001100(0)

После такта №41:

Сгенерированный ключ: 0

Состояние регистра: (1)010100000000000000(1)(0)101010011000(1)

После такта №42:

Сгенерированный ключ: 1

Состояние регистра: (0)101000000000000001(0)(1)010100110001(1)

После такта №43:

Сгенерированный ключ: 0

Состояние регистра: (1)010000000000000010(1)(0)101001100011(0)

После такта №44:

Сгенерированный ключ: 1

Состояние регистра: (0)100000000000000101(0)(1)010011000110(0)

После такта №45:

Сгенерированный ключ: 0

Состояние регистра: (1)000000000000001010(1)(0)100110001100(1)

После такта №46:

Сгенерированный ключ: 1

Состояние регистра: (0)000000000000010101(0)(1)001100011001(1)

После такта №47:

Сгенерированный ключ: 0

Состояние регистра: (0)000000000000101010(1)(0)011000110011(0)

После такта №48:

Сгенерированный ключ: 0

Состояние регистра: (0)000000000001010101(0)(0)110001100110(0)

После такта №49:

Сгенерированный ключ: 0

Состояние регистра: (0)000000000010101010(0)(1)100011001100(1)

После такта №50:

Сгенерированный ключ: 0

Состояние регистра: (0)000000000101010100(1)(1)000110011001(1)

После такта №51:

Сгенерированный ключ: 0

Состояние регистра: (0)000000001010101001(1)(0)001100110011(0)

После такта №52:

Сгенерированный ключ: 0

Состояние регистра: (0)000000010101010011(0)(0)011001100110(0)

После такта №53:

Сгенерированный ключ: 0

Состояние регистра: (0)000000101010100110(0)(0)110011001100(0)

После такта №54:

Сгенерированный ключ: 0

Состояние регистра: (0)000001010101001100(0)(1)100110011000(1)

Полный ключ:

111111111111111111111111111111111111010101010101000000

**Метод потокового шифрования RC4**

**Ключ (в байтах):**

[104, 101, 108, 108, 111, 119, 111, 114, 108, 100]

**Исходный текст:**

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

**Зашифрованный текст:**

���}����q��↹4��H:u�s�3n�B�� ?�ˀ[��Փ\*�C������Z��,�7�Q��MG����H�Mq�� �sڰC�c�7�8{��,�!�0bZ�r�~�h���ns8�qY���n�I�

%v]���I�\\_�%EG�\X�W�qU�u~X[���ȂO+�{�R`(��Ū2c����?�]���K�B���k�����}�?l� �s�=~j���u�b����ˇ��YP�&<��d����)��z5�9������Z�J[�8��đ8�M�E�-,<4})f�J%��S�Sݵ���B�p�����F����ꧺ��`�G��o��'��%��]�;����N}��+p�N{�s(��Ǒ���N�lotz�T� R拼�U|

���~?J7%��^�#/�n�k#�3D�6��Yצ�c�aF4��5�����7f�,co j����?Z5�/���^��8�S�e�r�z�y#5i+���[��U7N��o\_�I�9[����]��8�Q-�r��H��;�d}ίB�'|�V����f�AyTMJ6�э�RJ�E�Kk)�ޠ�WRܧ�

**Расшифровка правильным ключом:**

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

**Расшифровка неправильным ключом:**

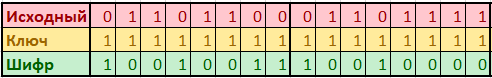
**Ключ (в байтах):** [100, 108, 114, 111, 119, 111, 108, 108, 101, 104]

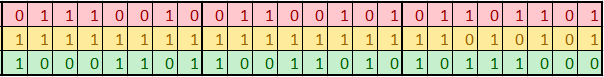
��f�7Jv�'��}���gLnJ��2e��F��+p��и��'7 �EH=����������/��3S%�JxU]%�[�`�lLַ��'i�<�܋�}��$V�]�����P!{l<�D� 1���I7ӂ�0Z[+�H���1�;���U��lVOAZ�P Eʬ\L!7\_B�Yq�xxC��r�����Ҁ�v�����#wI��रq�Kk�{�@è��>�{�9\_�)��j�\`�����L��b�F�Åk��>��ԃn���2�=Uћ���>�,�T���<�:���USN�#�T����P��0w<~���lu�pdE�%���5#���������{4�mvFAmԒ��ۆ���~S�ܽ���'7��u&�B�a�feZW�ڀ�0M����Fam�5�&\*&��@�,�J7� Fo�B���1v;L2

nZG�}�\* ''����D��Xgs�.�;!� ��o�Ohx��(�;F3i�UE1ē�@���Þ܉Rf`�����������K�of<.�$�%���R6��J�a�����L1��I��K

**3 ОСНОВНОЙ ТЕСТ**

Ручной расчёт:





Программный расчёт:

