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

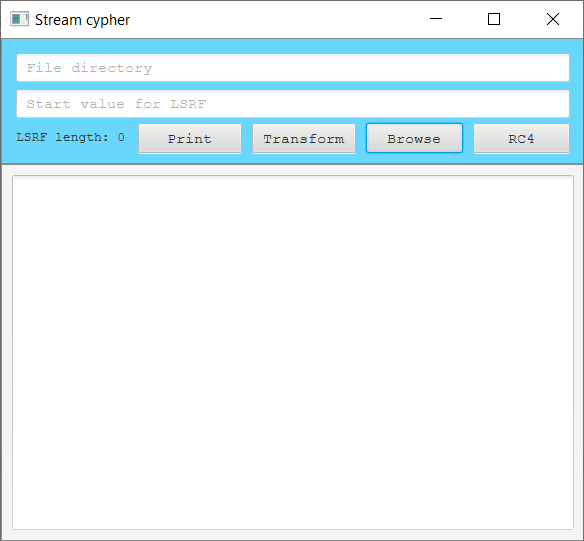
Содержание

[1 Smoke test 3](#_Toc23786492)

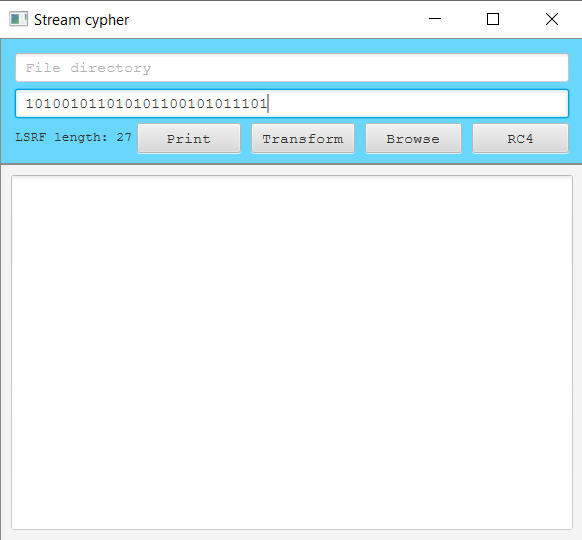
2 Таблица и скриншоты тестов..…………………………………………………9

# SMOKE TEST

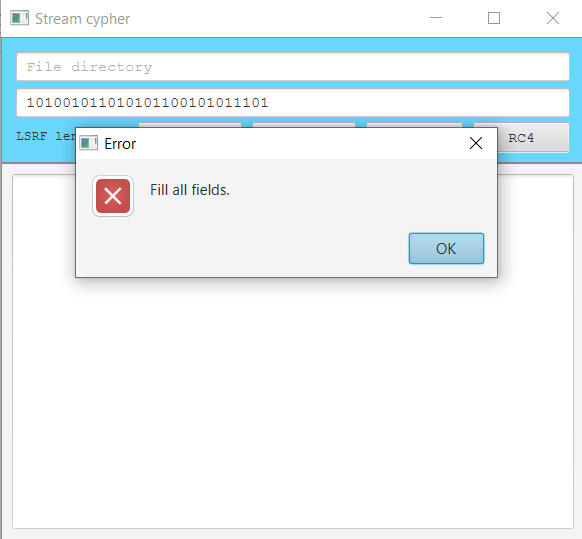
1. Запуск программы:



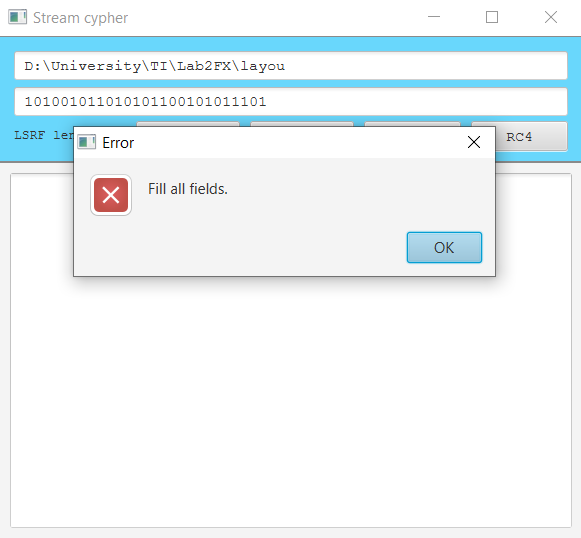
1. Проверка ключа – должны быть только 0 и 1:



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



* 1. Попытка зашифровать несуществующий файл:



# 2 ТАБЛИЦА И СКРИНШОТЫ ТЕСТОВ

**Метод потокового шифрования с помощью LSRF**

**Пример генерации ключа:**

Полином: a^27 + a^1 + 1

Начальное состояние: 111010011110100101010101011

После такта №1:

Сгенерированный ключ: 1

Состояние регистра: 110100111101001010101010110

После такта №2:

Сгенерированный ключ: 1

Состояние регистра: 101001111010010101010101101

После такта №3:

Сгенерированный ключ: 1

Состояние регистра: 010011110100101010101011010

После такта №4:

Сгенерированный ключ: 0

Состояние регистра: 100111101001010101010110100

После такта №5:

Сгенерированный ключ: 1

Состояние регистра: 001111010010101010101101001

После такта №6:

Сгенерированный ключ: 0

Состояние регистра: 011110100101010101011010011

После такта №7:

Сгенерированный ключ: 0

Состояние регистра: 111101001010101010110100111

После такта №8:

Сгенерированный ключ: 1

Состояние регистра: 111010010101010101101001110

После такта №9:

Сгенерированный ключ: 1

Состояние регистра: 110100101010101011010011101

После такта №10:

Сгенерированный ключ: 1

Состояние регистра: 101001010101010110100111010

После такта №11:

Сгенерированный ключ: 1

Состояние регистра: 010010101010101101001110101

После такта №12:

Сгенерированный ключ: 0

Состояние регистра: 100101010101011010011101011

После такта №13:

Сгенерированный ключ: 1

Состояние регистра: 001010101010110100111010110

После такта №14:

Сгенерированный ключ: 0

Состояние регистра: 010101010101101001110101100

После такта №15:

Сгенерированный ключ: 0

Состояние регистра: 101010101011010011101011000

После такта №16:

Сгенерированный ключ: 1

Состояние регистра: 010101010110100111010110001

После такта №17:

Сгенерированный ключ: 0

Состояние регистра: 101010101101001110101100011

После такта №18:

Сгенерированный ключ: 1

Состояние регистра: 010101011010011101011000110

После такта №19:

Сгенерированный ключ: 0

Состояние регистра: 101010110100111010110001100

После такта №20:

Сгенерированный ключ: 1

Состояние регистра: 010101101001110101100011001

После такта №21:

Сгенерированный ключ: 0

Состояние регистра: 101011010011101011000110011

После такта №22:

Сгенерированный ключ: 1

Состояние регистра: 010110100111010110001100110

После такта №23:

Сгенерированный ключ: 0

Состояние регистра: 101101001110101100011001100

После такта №24:

Сгенерированный ключ: 1

Состояние регистра: 011010011101011000110011001

После такта №25:

Сгенерированный ключ: 0

Состояние регистра: 110100111010110001100110011

После такта №26:

Сгенерированный ключ: 1

Состояние регистра: 101001110101100011001100110

После такта №27:

Сгенерированный ключ: 1

Состояние регистра: 010011101011000110011001101

После такта №28:

Сгенерированный ключ: 0

Состояние регистра: 100111010110001100110011011

После такта №29:

Сгенерированный ключ: 1

Состояние регистра: 001110101100011001100110110

После такта №30:

Сгенерированный ключ: 0

Состояние регистра: 011101011000110011001101100

После такта №31:

Сгенерированный ключ: 0

Состояние регистра: 111010110001100110011011000

После такта №32:

Сгенерированный ключ: 1

Состояние регистра: 110101100011001100110110001

После такта №33:

Сгенерированный ключ: 1

Состояние регистра: 101011000110011001101100010

После такта №34:

Сгенерированный ключ: 1

Состояние регистра: 010110001100110011011000101

После такта №35:

Сгенерированный ключ: 0

Состояние регистра: 101100011001100110110001011

После такта №36:

Сгенерированный ключ: 1

Состояние регистра: 011000110011001101100010110

После такта №37:

Сгенерированный ключ: 0

Состояние регистра: 110001100110011011000101100

После такта №38:

Сгенерированный ключ: 1

Состояние регистра: 100011001100110110001011001

После такта №39:

Сгенерированный ключ: 1

Состояние регистра: 000110011001101100010110010

После такта №40:

Сгенерированный ключ: 0

Состояние регистра: 001100110011011000101100100

После такта №41:

Сгенерированный ключ: 0

Состояние регистра: 011001100110110001011001000

После такта №42:

Сгенерированный ключ: 0

Состояние регистра: 110011001101100010110010000

После такта №43:

Сгенерированный ключ: 1

Состояние регистра: 100110011011000101100100001

После такта №44:

Сгенерированный ключ: 1

Состояние регистра: 001100110110001011001000010

После такта №45:

Сгенерированный ключ: 0

Состояние регистра: 011001101100010110010000100

После такта №46:

Сгенерированный ключ: 0

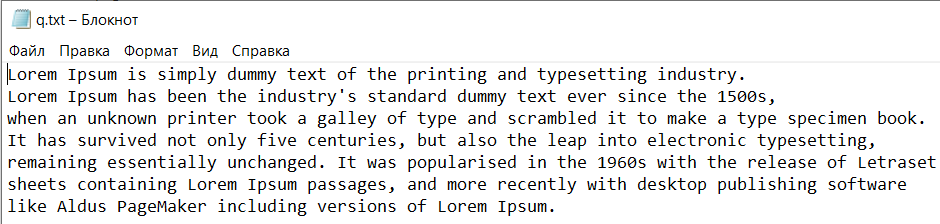
Состояние регистра: 110011011000101100100001000

После такта №47:

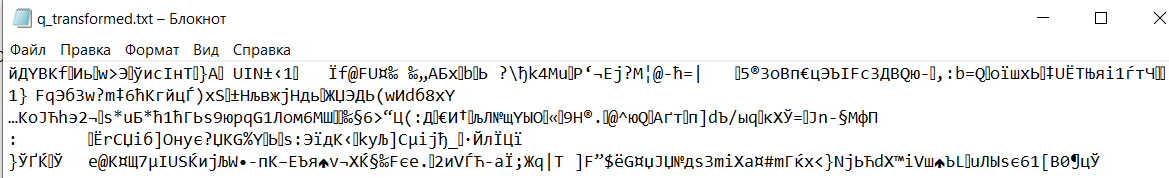
Сгенерированный ключ: 1

Состояние регистра: 100110110001011001000010001

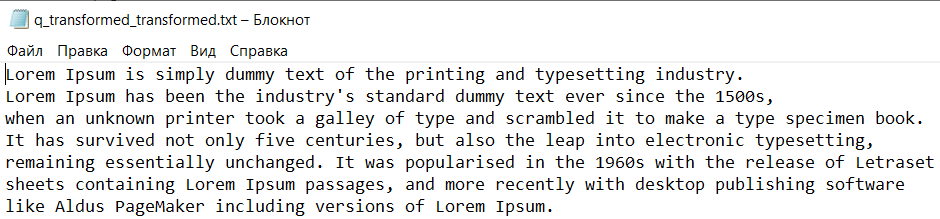
**Исходный текст:**



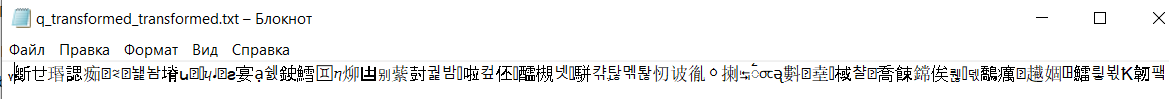
**Зашифрованный текст:**



**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) ^ 10100100 = 11101000(￨)

01101111(o) ^ 11000011 = 10101100(ﾬ)

01110010(r) ^ 11101011 = 10011001(ﾙ)

01100101(e) ^ 10100111 = 11000010(ￂ)

01101101(m) ^ 00010000 = 01111101(})

00100000( ) ^ 01010110 = 01110110(v)

01001001(I) ^ 01011000 = 00010001()

01110000(p) ^ 10111100 = 11001100(ￌ)

01110011(s) ^ 00001100 = 01111111()

01110101(u) ^ 10001101 = 11111000(￸)

01101101(m) ^ 11100101 = 10001000(ﾈ)

00100000( ) ^ 00000001 = 00100001(!)

01101001(i) ^ 00011110 = 01110111(w)

01110011(s) ^ 11010111 = 10100100(ﾤ)

00100000( ) ^ 00111111 = 00011111()

01110011(s) ^ 11000010 = 10110001(ﾱ)

01101001(i) ^ 10010011 = 11111010(￺)

01101101(m) ^ 01000101 = 00101000(()

01110000(p) ^ 01010000 = 00100000( )

01101100(l) ^ 01100011 = 00001111()

01111001(y) ^ 10110000 = 11001001(￉)

00100000( ) ^ 11001100 = 11101100(￬)

01100100(d) ^ 00001000 = 01101100(l)

01110101(u) ^ 01011011 = 00101110(.)

01101101(m) ^ 11101110 = 10000011(ﾃ)

01101101(m) ^ 11111110 = 10010011(ﾓ)

01111001(y) ^ 00001101 = 01110100(t)

00100000( ) ^ 10101001 = 10001001(ﾉ)

01110100(t) ^ 01101010 = 00011110()

01100101(e) ^ 10000001 = 11100100(￤)

01111000(x) ^ 00100110 = 01011110(^)

01110100(t) ^ 00110110 = 01000010(B)

00100000( ) ^ 01100000 = 01000000(@)

01101111(o) ^ 00111000 = 01010111(W)

01100110(f) ^ 10000100 = 11100010(￢)

00100000( ) ^ 10001000 = 10101000(ﾨ)

01110100(t) ^ 00000101 = 01110001(q)

И т.д.

**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