

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ СИСТЕМЫ ШИФРОВАНИЯ НА ОСНОВЕ ОДНОРАЗОВЫХ БЛОКНЕТОВ

Щебетов Андрей Сергеевич

11 класс ЧОУ СОШ «Ломоносовская школа» (г. Москва)

Презентация на конференции «Интел-Авангард»

23 февраля 2018 года

ЦЕЛИ И ЗАДАЧИ ПРОЕКТА

- *Практическая реализация работоспособного прототипа системы шифрования, использующей одноразовые блокноты*
- *Сочетание шифрования одноразовыми блокнотами с кодовыми таблицами и супершифрованием*
- *Практическая проверка 3 предложенных протоколов обмена кодовыми таблицами, одноразовыми блокнотами и сообщениями*
- *Понимание из каких блоков и элементов и на какой программной и аппаратной базе может быть реализован такой прототип*
- *Проверка пяти ГСЧ для генерации кодовых таблиц и одноразовых блокнотов*
- *Основной приоритет – обеспечение информационной, программной и аппаратной безопасности*
- *Простота и наглядность созданного прототипа и возможности прямой проверки правильности работы системы на каждом шаге*
- *Обеспечение физической безопасности системы и наличие «достоверного отрицания»*
- *Намеренное упрощение:*
 - *Наглядные арифметические операции взятия по модулю (вместо побитового XOR)*
 - *Собственный алфавит из 256 символов (вместо 55295 несуррогатных символов UTF-16)*
 - *Уменьшенная степень автоматизации (ручная отправка ZIP-контейнеров из почтового клиента)*
 - *Консольная реализация*

Задачей проекта являлась построение прототипа системы обмена сообщениями с помощью одноразового блокнота, кодовых таблиц и супершифрования

ШЕСТЬ ПРИНЦИПОВ КЕРКГОФФА

- **Физическая и математическая стойкость:** «Система должна быть физически, если не математически, невскрываемой»
- **Открытость алгоритма:** «Нужно, чтобы не требовалось сохранение системы в тайне; попадание системы в руки врага не должно причинять неудобств»
- **Возможность выбора и обмена ключами:** «Хранение и передача ключа должны быть осуществимы без помощи бумажных записей; корреспонденты должны располагать возможностью менять ключ по своему усмотрению»
- **Пригодность для каналов связи:** «Система должна быть пригодной для сообщения через телеграф»
- **Компактность:** «Система должна быть легко переносимой, работа с ней не должна требовать участия нескольких лиц одновременно»
- **Простота:** «Наконец, от системы требуется, учитывая возможные обстоятельства её применения, чтобы она была проста в использовании, не требовала значительного умственного напряжения или соблюдения большого количества правил»

При построении прототипа и написании программ мы старались придерживаться шести принципов Керкгоффса

ОПИСАНИЕ ОДНОРАЗОВОГО БЛОКНОТА (ONE-TIME PAD или ОТП)

- Пример: алфавит из 50 символов

"	0	Д	5	И	10	Н	15	Т	20	Ч	25	Ь	30	1	35	6	40	.	45
А	1	Е	6	Й	11	О	16	У	21	Ш	26	Э	31	2	36	7	41	?	46
Б	2	Ё	7	К	12	П	17	Ф	22	Щ	27	Ю	32	3	37	8	42	-	47
В	3	Ж	8	Л	13	Р	18	Х	23	Ъ	28	Я	33	4	38	9	43	:	48
Г	4	З	9	М	14	С	19	Ц	24	Ы	29	0	34	5	39	!	44		49

- Пример: шифрование одноразовым блокнотом полученным от ГСЧ

Текст	Д	О	В	С	Т	Р	Е	Ч	И	В	В	О	Р	О	Н	О	В	О	!			
Код текста	5	16	49	3	19	20	18	6	25	10	49	3	49	3	16	18	16	15	16	3	16	44
Текст ГСЧ	З	Ш	А	Х	П	Р	:	0	6	Э	Т	4	8	Ь	0	Ж	Ц	2	И	Ф		М
Код от ГСЧ	9	26	1	23	17	18	48	34	40	31	20	38	42	30	34	8	24	36	10	22	49	14
Шифротекст	М	8	"	Ш	2	4	О	6	Н	7	С	7	7	Я	"	Ш	6	А	Ш	Ч	Н	Ж
Код шифротекста	14	42	0	26	36	38	16	40	15	41	19	41	41	33	0	26	40	1	26	25	15	8

Шифрование одноразовым блокнотом заключается в накладывании на открытый текст случайного ключа той же или большей длины

НЕМНОГО ИСТОРИИ

- 1882** *Изобретатель – американский банкир Франк Миллер (1882)*
- 1919** *US Patent 1,310,719 «Секретная сигнальная система» Гильберта Вернама («шифр Вернам»)*
- 1922** *Джозеф Мабурн (США) предположил, что если пользоваться абсолютно случайным ключом и использовать его только один раз, то криптоанализ системы не даст результатов.*
- 1923** *Германский МИД переходит на использование одноразовых блокнотов*
- 1927** *СССР переходит на использование одноразовых блокнотов*
- 1930-е** *Военные, разведка и спецслужбы по всему миру широко используют одноразовые блокноты*
- 1941** *Владимир Александрович Котельников (СССР) доказал, что системы шифрования с одноразовыми ключами (или одноразовыми блокнотами) являются абсолютно стойкими*
- 1941** *В США запущена военная голосовая система на основе одноразового блокнота (SIGSALY)*
- 1943** *В США запущен сверхсекретный проект Venona для расшифровки перехваченных советских сообщений*
- 1945** *Клод Шеннон (США) пришел к тем же выводам, что и Котельников*
- 1949** *Клод Шеннон (США) опубликовал работу «Теория связи в секретных системах»*
- 1950-е** *«Номерные радиостанции» начинают вещать по всему миру*
- 1970** *Стивен Визнер (США) предлагает идею квантовой криптографии*
- 1982** *Доклад Чарльза Беннета (Канада) с др. «Квантовая криптография II: как безопасно снова использовать одноразовый блокнот даже если $P=NP$ »*
- 1984** *Опубликован BB84 – первый протокол квантовой криптографии и квантового распределения ключей, тесно связанный с использованием одноразовых блокнотов*
- 2015** *АНБ США объявило о переходе к пост-квантовой криптографии в течение 10 лет*

В 1941 году Котельников и в 1945 году Шеннон доказали абсолютную криптостойкость одноразовых блокнотов

АБСОЛЮТНО СТОЙКИЙ ШИФР

- *Котельников в 1941 и Шеннон в 1945 году доказали, что шифр является абсолютно стойким, если соблюдаются следующие условия:*

(1) Секретность: «Ключ секретен — известен только легитимным пользователям»

(2) Превышение длины ключа над длиной сообщения: «Длина ключа в битах не меньше длины сообщения»

(3) Случайность: «Ключ случаен»

(4) Одноразовость: «Ключ используется только один раз»

Котельников и Шеннон сформулировали требования к абсолютно стойкому шифру, которым удовлетворяет только одноразовый блокнот

ПРЕИМУЩЕСТВА ОДНОРАЗОВЫХ БЛОКНЕТОВ

- *Абсолютная криптостойкость* – невозможность расшифровки сообщения после его перехвата противником никакими методами, даже если противник обладает неограниченным вычислительным ресурсом
- *Степенной рост трудности* порядка A^M для лобовой «атаки грубой силой» при росте длины сообщения, в то время как у традиционных схем шифрования трудность постоянна и равна A^P (где A – длина алфавита, P – длина пароля, M – длина сообщения)
- *Абсолютная энтропия* – равная вероятность любого возможного варианта открытого текста той же длины
- *Невосстанавливаемость сообщений* – даже физический доступ противника к одноразовому блокноту, у которого уничтожены предыдущие «страницы», не позволяет восстановить прошлые сообщения (так называемая «совершенная секретность в будущем»)
- *Возможность использования в системах супершифрования* в качестве одного из слоев шифрования или системы шифрования длинного пароля
- *Открытая передача сообщений* – сообщения можно свободно передавать по любым открытым сетям
- *Полная возможность «правдоподобного отрицания»* в случае компрометации пользователя
- *Быстрота шифрования* – шифрование с помощью одноразового блокнота требует значительно меньше операций, чем при помощи традиционных шифров (например, DES, AES или RSA)

Одноразовые блокноты имеют целый ряд важных преимуществ, включая абсолютную криптостойкость и энтропию сообщений

НЕДОСТАТКИ ОДНОРАЗОВЫХ БЛОКНЕТОВ

- *Требование полной случайности* – труднодостижимое на практике, так как нет хороших генераторов случайных чисел
- *Требование абсолютной одноразовости* – невозможности полного уничтожения всех копий блокнота после использования (касается остаточной информации на носителях данных)
- *Требования безопасного распределения ключей* – невозможно быстрое осуществление в необходимых объемах (требуется физическая доставка или использование других менее криптостойких методов шифрования блокнотов для доставки по сетям)
- *Требование аутентификации отправителя* – необходимость дополнительной и менее стойкой системы для аутентификации отправителя
- *Большая длина* – традиционная криптография сокращает размер секрета до размера ключа, в то время как одноразовый блокнот требует их равенства
- *Непрактичность для аудио и видео* – традиционная криптография успешно шифрует большие куски информации (аудио, видео, VPN и Интернет-соединения) и использование одноразовых блокнотов непрактично для этих целей
- *Проблема распределения ключей* – одноразовый блокнот не решает основную проблему современной криптографии – безопасное распределение ключей, а только усложняет ее
- *Ненужная более высокая криптостойкость* – одноразовый блокнот решает проблему повышения криптостойкости шифров, которая и так достаточно высока.

При традиционном взгляде на шифрование одноразовые блокноты имеют целый ряд недостатков

КВАНТОВАЯ КРИПТОГРАФИЯ И БУДУЩЕЕ ОДНОРАЗОВЫХ БЛОКНЕТОВ

- *Сумасшедшая идея использовать квантовые состояния фотона для маркировки денег (1970-е годы, «Сопряженное кодирование», Стивен Визнер)*
- *«Квантовая криптография II: как безопасно использовать снова одноразовый блокнот даже если $P=NP$ » (1982 год, Жиль Brassar и Сет Брейдбарт)*
- *Квантовое распределение ключей (протокол BB84, 1984, Жиль Brassar и Сет Брейдбарт)*
- *Квантовая криптография основана на законах квантовой механики, а не на трудностях решения математических проблем*
- *При использовании канала передачи, основанном на квантовом состоянии фотонов, перехват данных и прослушивание становится невозможным, поскольку неизбежно ведет к обнаружению и безвозвратному изменению перехваченных данных.*
- *Верифицированный одноразовый блокнот (или ключ), полученный по такому каналу, может использоваться снова и снова для шифрования сообщений пока не выяснится, что он перехвачен противником.*
- *При обнаружении перехвата, блокнот (или ключ) заменяется на другой, до тех пор, пока не обеспечивается и подтверждается его верифицированное получение.*
- *Квантовая криптография тесно связана с идеей использования одноразовых блокнотов, как наиболее естественного способа существования ключей и шифрования сообщений.*
- *Квантовая криптография быстро развивается и начинает влиять на традиционные методы шифрования*

Квантовая криптография тесно связана с шифрованием одноразовыми блокнотами и решает раз и навсегда проблему их безопасного распространения

СУПЕРШИФРОВАНИЕ

- Эффективное удлинение ключей при каскадном шифровании
- Последовательное использование нескольких алгоритмов (например, 16 раз AES или AES-Serpent-Twofish)
- Достаточно хорошо изучено при переходе от DES к 3DES
- В 2014 году международной группой математиков было показано, что при каскадном шифровании эффективное удлинение ключа определяется формулой:

$$2^{\left(k + \min\left\{k * \left(\frac{L-2}{2}\right); \frac{n(L-2)}{L}\right\}\right)} \Rightarrow \text{max} \equiv 2^{(k+n)}, L \rightarrow \infty$$

K – длина ключа, *n* – длина блока, *L* – количество раундов шифрования

Прирост криптостойкости и эффективной длины ключа с увеличением раундов шифрования для симметричного блочного шифра с размером блока *n*=128

n=128	Количество раундов шифрования									
	2	4	16	32	64	128	256	512	1024	2048
64	0	64.0	112.0	120.0	124.0	126.0	127.0	127.5	127.8	127.9
128	0	64.0	112.0	120.0	124.0	126.0	127.0	127.5	127.8	127.9
192	0	64.0	112.0	120.0	124.0	126.0	127.0	127.5	127.8	127.9
256	0	64.0	112.0	120.0	124.0	126.0	127.0	127.5	127.8	127.9
320	0	64.0	112.0	120.0	124.0	126.0	127.0	127.5	127.8	127.9
384	0	64.0	112.0	120.0	124.0	126.0	127.0	127.5	127.8	127.9
448	0	64.0	112.0	120.0	124.0	126.0	127.0	127.5	127.8	127.9
512	0	64.0	112.0	120.0	124.0	126.0	127.0	127.5	127.8	127.9

Применение каскадного шифрования позволяет эффективно удлинить ключ и увеличить его криптостойкость

ТЕХНОЛОГИИ И АЛГОРИТМЫ

- **Платформа:** *Microsoft .NET Framework 4.7*
- **Язык программирования:** *C# 7.0*
- **IDE:** *Microsoft Visual Studio Professional 2017*
- **Модули:**
 - *Стандартные модули C# 7.0*
 - *System.Security.Cryptography*
 - *System.XML*
- **Внешние модули:**
 - *Ionic.ZIP (шифрованные ZIP-контейнеры)*
- **ГПСЧ:**
 - *System.Random (встроенный)*
 - *System.Random Thread-Safe (встроенный с использованием ThreadLocal<T>)*
 - *RNGCryptoServiceProvider (встроенный, удовлетворяет требованиям FIPS к ГСЧ)*
 - *PCG (внешний модуль на C# и отдельная реализация на C++, близок к требованиям FIPS к ГСЧ)*
 - *MT19937 (Mersenne Twister, внешний модуль на C# и отдельная реализация на Python)*
- **Хранение ключей RSA:** *встроенный в Windows криптоконтейнер MachineKeyStore*
- **Кодовые таблицы:** *собственный алфавит из 256 символов*
- **Физическая стойкость:** *TrueCrypt 7.1a*

Построенный прототип опирался на набор из целого ряда технологий и алгоритмов

РЕАЛИЗАЦИЯ ПРОТОТИПА

- **Функциональность:**
 - Создание профилей администраторов и пользователей
 - Генерация случайных кодовых таблиц и одноразовых блокнотов (пять ГСЧ)
 - Шифрование сообщений
 - Расшифровка сообщений
- ГСЧ отличались по качеству и скорости работы

OTP Admin

- Профили пользователей
- Пары RSA-ключей для каждого пользователя

OTP Generator

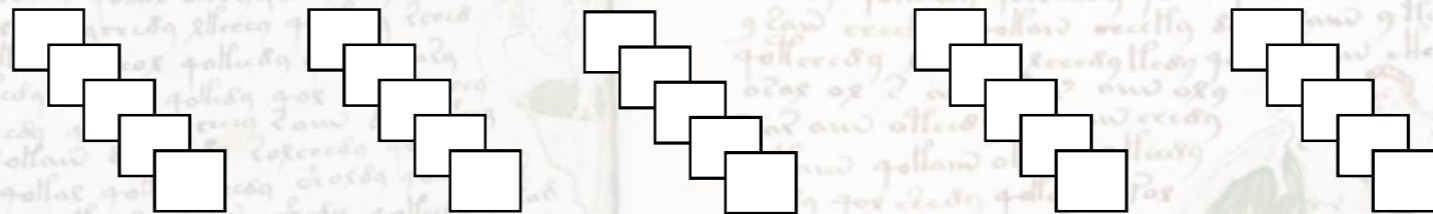
- Создание кодовых книг (алфавит+RNG)
- Создание одноразовых блокнотов (КК + RNG)
- Шифрование (DES + RSA) для безопасного хранения

OTP Encoder

- Шифрование сообщений (OTP)

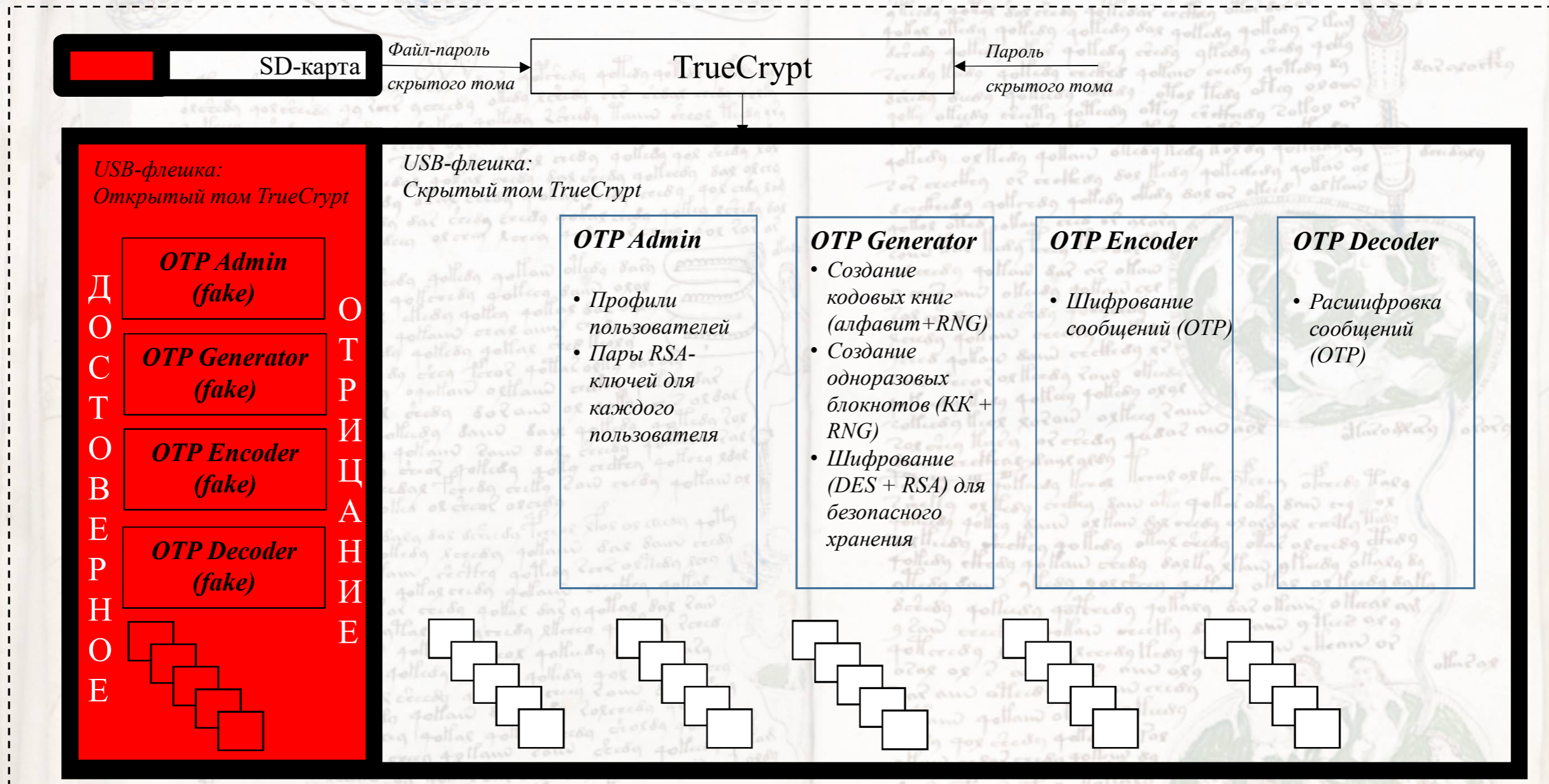
OTP Decoder

- Расшифровка сообщений (OTP)



Прототип был написан на С# в виде 4 отдельных программ-модулей, каждая из которых исполняла свою выделенную задачу

РЕАЛИЗАЦИЯ ПРОТОТИПА: ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ



Все программы расположены на скрытом томе TrueCrypt, который не может быть обнаружен никакими существующими методами

OTP ADMIN: СОЗДАНИЕ ПРОФИЛЕЙ ПОЛЬЗОВАТЕЛЕЙ

```
C:\development\9105 OTP Admin Test\Release\9105 OTP Admin.exe
Copyright © 2017 Andrey S. Shchebetov
Copyright © 2017 Андрей Щебетов

THIS IS USER PROFILE AND RSA PASSWORDS GENERATOR
ЭТО ГЕНЕРАТОР ПОЛЬЗОВАТЕЛЕЙ И ПАРОЛЕЙ RSA

Please, enter your user name using basic latin, numbers and special characters only (A-Z, a-z, 0-9, !-~):
Пожалуйста, введите ваше имя пользователя используя только базовую латиницу, цифры и специальные символы (A-Z, a-z, 0-9, !-~):
001

Please, enter your login using basic latin, numbers and special characters only (A-Z, a-z, 0-9, !-~):
Пожалуйста, введите ваш логин используя только базовую латиницу, цифры и специальные символы (A-Z, a-z, 0-9, !-~):
****

Welcome! Your entered correct admin username and login!
Добро пожаловать! Вы ввели правильное имя пользователя и логин для администратора!

Please, enter your access password using basic latin, numbers and special characters only (A-Z, a-z, 0-9, !-~):
Пожалуйста, введите ваш пароль пользователя используя только базовую латиницу, цифры и специальные символы (A-Z, a-z, 0-9, !-~):
*****

Your password is correct!
Вы ввели правильный пароль!

Please, select what you would like to do:
[1] Create new admin profile
[2] Create a pair of new public and private RSA keys for admin
[3] Create a new user profile to connect with
[4] Unprotect and save existing user profile
[5] Protect and save existing user profile
[6] Finish work and exit
Please, make your choice (enter 1, 2, 3, 4, 5 or 6 only)!

Пожалуйста, выберите что вы хотели бы сделать:
[1] Создать новый профиль администратора
[2] Создать пару новых RSA ключей для существующего администратора
[3] Создать новый профиль пользователя для связи
[4] Распаролить и сохранить профиль пользователя
[5] Запаролить и сохранить профиль пользователя
[5] Закончить работу и выйти из программы
```

- Создание профилей администраторов и пользователей
- Создание ключей RSA для администраторов
- Хранение ключей RSA в криптоконтейнерах Machine Key Store на компьютере
- Создание профилей пользователей
- Хранение всех профилей только в виде XML-файлов с зашифрованной или запароленной информацией

OTP Admin позволял создавать профили администраторов и пользователей системы, а также их RSA ключи

ПРОФИЛИ АДМИНИСТРАТОРА И ПОЛЬЗОВАТЕЛЕЙ

```
C:\Users\re200\Source\Repos\1015-Palindromes\9105 Login Password Generator\bin\Release\Admins\adminuser_001.xml - Notepad...
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
adminuser_001.xml
1 <?xml version="1.0" encoding="utf-8" ?>
2 <Admins>
3 <Admin>
4 <Username>001</Username>
5 <Name>
6 m+f7NkciBwXwL6KEx71XYU3AzstH4mBhR+yYRD0IMy1BFqdBFpBBm71N0yeL82ZpkoKhFa2h0oE1j2tLs3WT1cZfVNOYrb
7 AjabsMLD41HYqwgEOneTy+YPqCGGD9EPPP4u/DIwD/HVEJq9hgQFz/HX66nYKMA1mUH01L7sBF7KE=</Name>
8 <Surname>
9 PinLFaCmindayBoK8ofEh1X0FRHv6ieIPP20kWoB5QhOqQ3Wj4WBAc/Udmbao29ypgz3MFGF5N1Nnix1NVAKDfyHLV7HH
10 RW9Qyp3hqQsOFB+dGQ7msHnkC4J+kpvd7dNKOS49iJPLWSAgFIoiwszSgV2RV/ldPofKIPlKbZyUQ=</Surname>
11 <Email>
12 CnMKxmzV2NEu4sTaPM74vKeTUAK+C1AY49/EnePoH93LTczH9Yucjwlaa4S7yKX9W1EbHKEdwc/uCYCSXGIghCKnVmXdLX
13 F/5hq2edtr0beRQdrGdX5aP2qN1PTGNg4KZC9S9K8djY7m+UactfHsK6sLrcQ9RWvF+WQNWVsQXEY=</Email>
14 <Login>
15 fOd3ulqtZhlHtTrMHxRONFe0PXW9pXFt5CUuVL0npd8=:3rTZummYct0JmPfLnLGTdZyKDFHRFG8GvNjLtvfFwCs=
16 </Login>
17 <Password>
18 sXaNn1jD91/aMH2YlRy5XDd1PdU8dCKr/a96FKfQ8Es=:9+MutJ8XZqj0ErznD6bUcan5CS1yMHSQMN6ENh0uLU8=
19 </Password>
20 <RSAKeyValue>
21 <Modulus>
22 z/xImpGuc219eenDasSdT+QTQc5kZ7zJ0uoFkHBGBLtg5vmdY3C7uf+6Ex43SPe1QMLxtngNOuX6EO2IOdKSHmv6fmY1
23 sBz0e1w5PxZVavUocB4NwQ0cm9fg71u+BcpR/IwEVdwrTR1yBwA6QnmY+oACFd/aa9Nn5pW6dMMmMbE=</Modulus>
24 <Exponent>AQAB</Exponent>
25 </RSAKeyValue>
26 <Comment>
27 CnMKxmzV2NEu4sTaPM74vKeTUAK+C1AY49/EnePoH93LTczH9Yucjwlaa4S7yKX9W1EbHKEdwc/uCYCSXGIghCKnVmXdLX
28 F/5hq2edtr0beRQdrGdX5aP2qN1PTGNg4KZC9S9K8djY7m+UactfHsK6sLrcQ9RWvF+WQNWVsQXEY=</Comment>
29 </Admin>
30 </Admins>
```

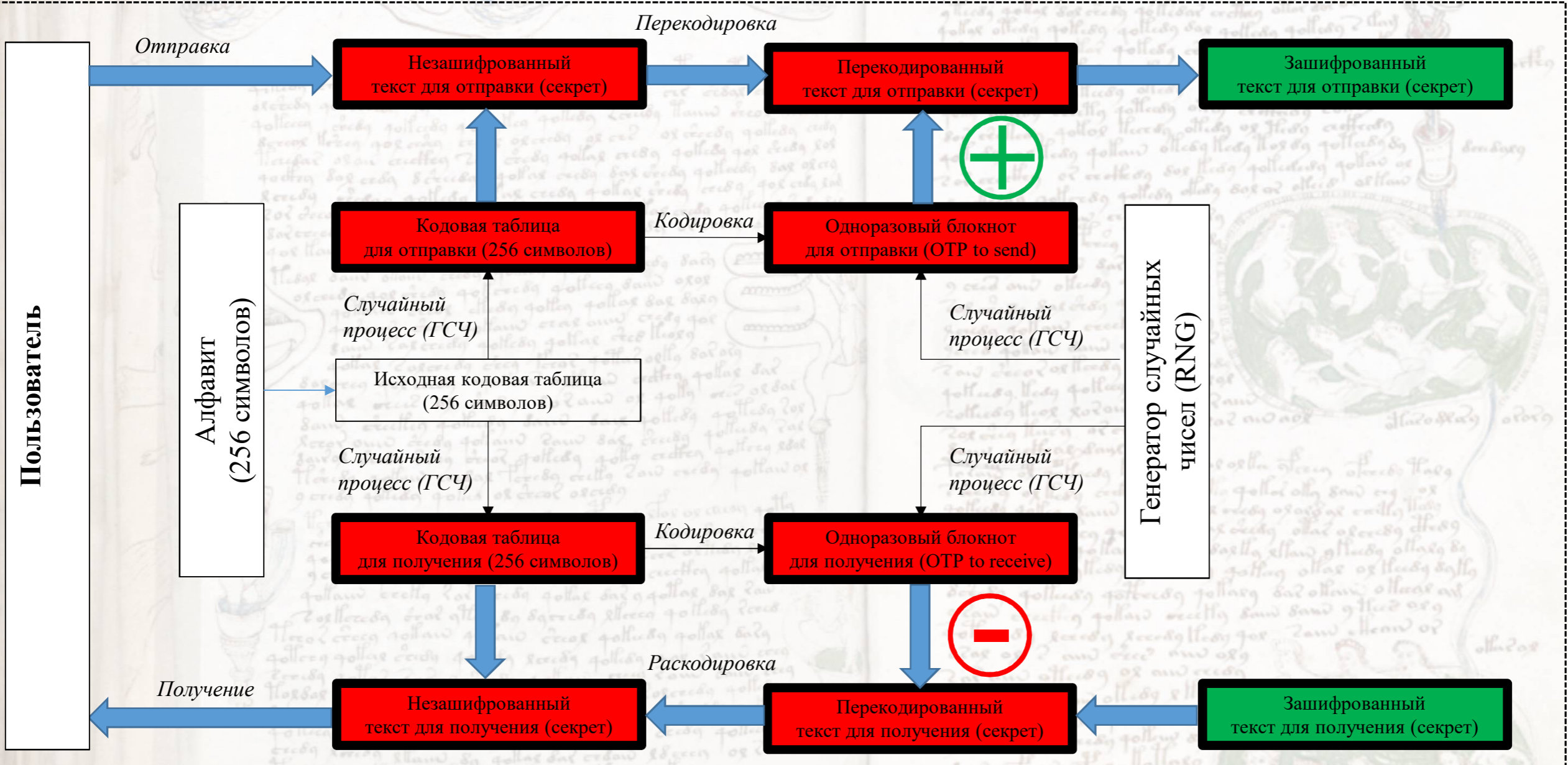
- Вход в систему и все ее программы без существующего профиля администратора невозможен
- Все данные либо хэшируются либо запаролены
- При каждом входе вся введенная информация сравнивается с хранящейся в XML-профиле
- Каждый администратор, вошедший в систему, может создавать новые профили администраторов и пользователей
- Можно изменять пары RSA-паролей, хранящиеся в специальных контейнерах, встроенных в Windows

- Каждый администратор может создавать профили своих пользователей, чтобы обмениваться с ними сообщениями

```
C:\Users\re200\Source\Repos\1015-Palindromes\9105 Login Password Generator\bin\Release\Users\user_001_021.xml - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
user_001_021.xml
1 <?xml version="1.0" encoding="utf-8" ?>
2 <Users>
3 <User>
4 <Username>021</Username>
5 <Name>owYVydQK2SG3c7NFgiH907GNja+Z6raA43+8662f/X3c8drdGZVJnd2rQ9DSa+LeRmFBGbf12zJYxJxJovVEX/VFNIDCqWCDJ3+8sEtA00EW3RmfPLELVgG+r9PoGa3wnjFYw+0ZhcM5Y/boungf4kArZZKDVz40+pJ+GoZwW=</Name>
6 <Surname>N018sAyRtIRRjGSD00EZiorULjzMeQiSt2A08TAbjMz2XknZytQE3V3v666kMZ3aBQ66KXaVy3/DQKFWLAHS7ERhZ7J4zUQ6r3o2F944Kp1XYezAVgOpa/kFusGI4tKqiSPNYBVvSYPkiS1p7HKQAw4IEsYi+Qs06GP4qENxow=</Surname>
7 <Email>NZjtds9IQpRmlmwOvGxXhYrFxBQmoyALvKpCOWt6CI7JDU/7wAH1/ru1Cs6EKehOKYyIkczYU0tGVNXovEB3qys4sMc/xCDY+/IdIBDRA9vU75w41Fg44mcNfj5MkpqQchMZgRUq/OmPsP3sbNio7s9aq9QB9q5heMCw9S8o=</Email>
8 <RSAKeyValue>
9 <Modulus>wsnYZj4jtGU3Zjx1RkGgDAPRde1dIBxCEfJ4+kmFXJwpS8TWhtZu2SV8z5pSK2ERyh105i82ug3d7Mx0fTmuD3aFh/Lxibo79rKyIRXqalfTo9cfm6mj49IkavCKq0TeV7tK8F95A0arD5gv/rXGQZYBd2eH7uTZk1orkbpgk=</Modulus>
10 <Exponent>AQAB</Exponent>
11 </RSAKeyValue>
12 <Comments>B0wreJwmp2QqCM9PEXpA13UnN5L5KxBqTEZE3w+EJE5JS+jcL9XoGE+2YOS1EhTpjL2qavwQtJtGVdXNwXPaROH0P0PqAYv9v01r+Y0yLEk66ShPHUttAgpBdL1RcvvkaeWKRtJRdV72Awg38nmMoXdsj/w01nNkm6NCgS01=</Comments>
13 <CreatedBy>001</CreatedBy>
14 <DateTime>08-Feb-2018 16:39:49</DateTime>
15 </User>
16 </Users>
```

Вся информация об администраторах и пользователях хранится в XML-файлах с захешированной или запароленной информацией

ОБЩАЯ СХЕМА ШИФРОВАНИЯ ОДНОРАЗОВЫМ БЛОКНОТОМ



Общая схема шифрования одноразовым блокнотом зависит от нескольких случайных процессов, генерируемых набором ГСЧ

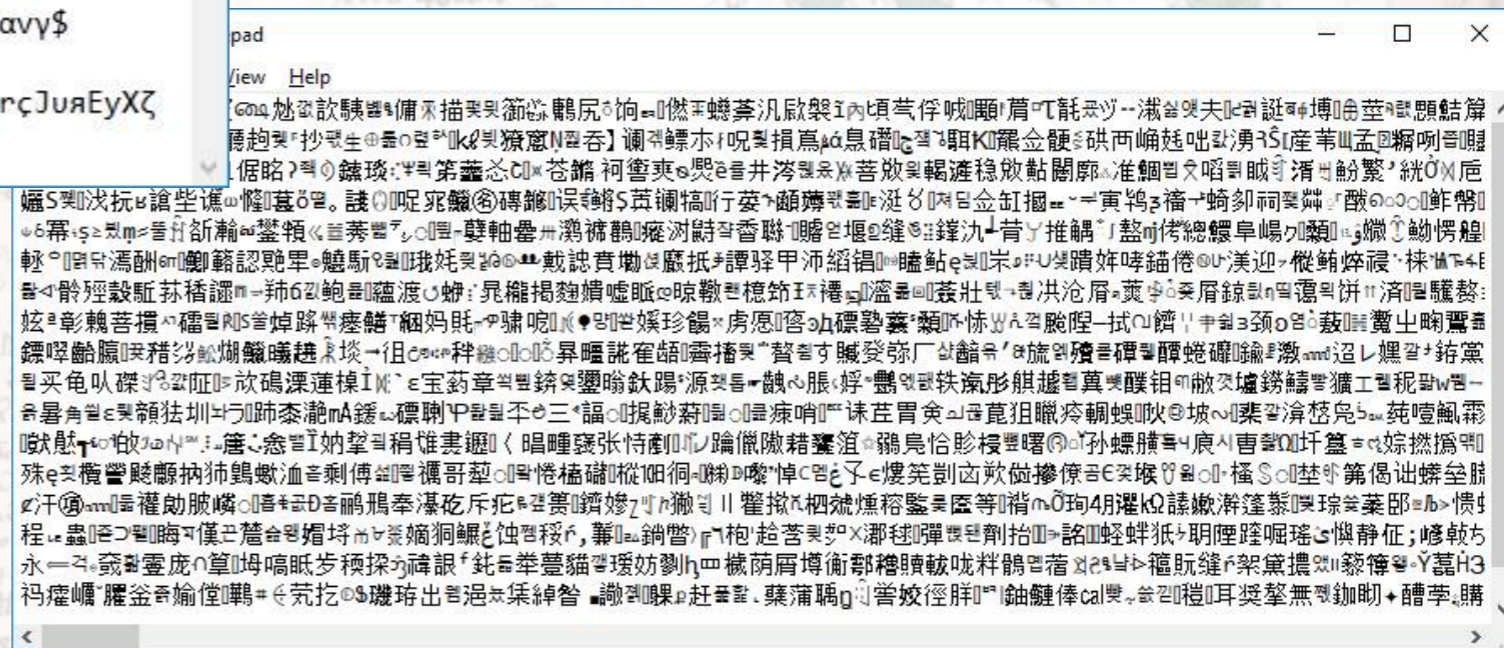
КОДОВЫЕ ТАБЛИЦЫ

```
001_002.code - Notepad
File Edit Format View Help
XδXα-ÿρυ»κĔτqy&ÛησκελτtÛъэÏVοβÂΠΨξΓSшмАĔщiĀ±æφРАнтχЙеZВ(еьЖÙ
ĔFYΠρωчLuvz=ĔĬEφ$5μ]I*GH#/0иц)Xr-fЯpé~0Л
[юАÿÇÆвDè09Ψ6ЫΛÛМУxĕM^cîTODЄ,НÛГнКпQФĔλ{\IЗчсgШUЭЦ"ψdжRb&β408PЮлВbБ' à
%M;_ИJ.2ÄÔτΣ öoδxэo>çOCkEα:YjNбωгPΔW< i3γymn7Bbÿ}яйξē1NФ`СКσνE+ΞTÖ|K!
Ωa1Zñi@ēç?āĴ
```

```
002_001.code - Notepad
File Edit Format View Help
|;лВМiШ/‰Ĕp3[жа0æĔ»+OZьYōhSLXàsхâ\λ7ьπ±CĔч1úaiMκ=Woσ3ubэB^wΦ
{z>гθь5HεозтVAKX?ЖУТδĀiΠ|]μс<ЭМ. вΨ ДĬИГCFŎIB"АÿδeуЙскФGHĕ`jbtЩD6avy$
ëCd$QпхЕШйАÛPфБнĕÄЧц'_нĔÛIw12Pы8PNГ( UӨHĕxЮЭрфÛ
%)9KΘςTΠ@gZĬoÿяvηNцб#φEЫЮ*ит&YÛВ,рлām~Лôé:4екĔψ-ξÿτΔmèΣ}Ωцβ!KqюςJюяЕуXζ
RTд
```

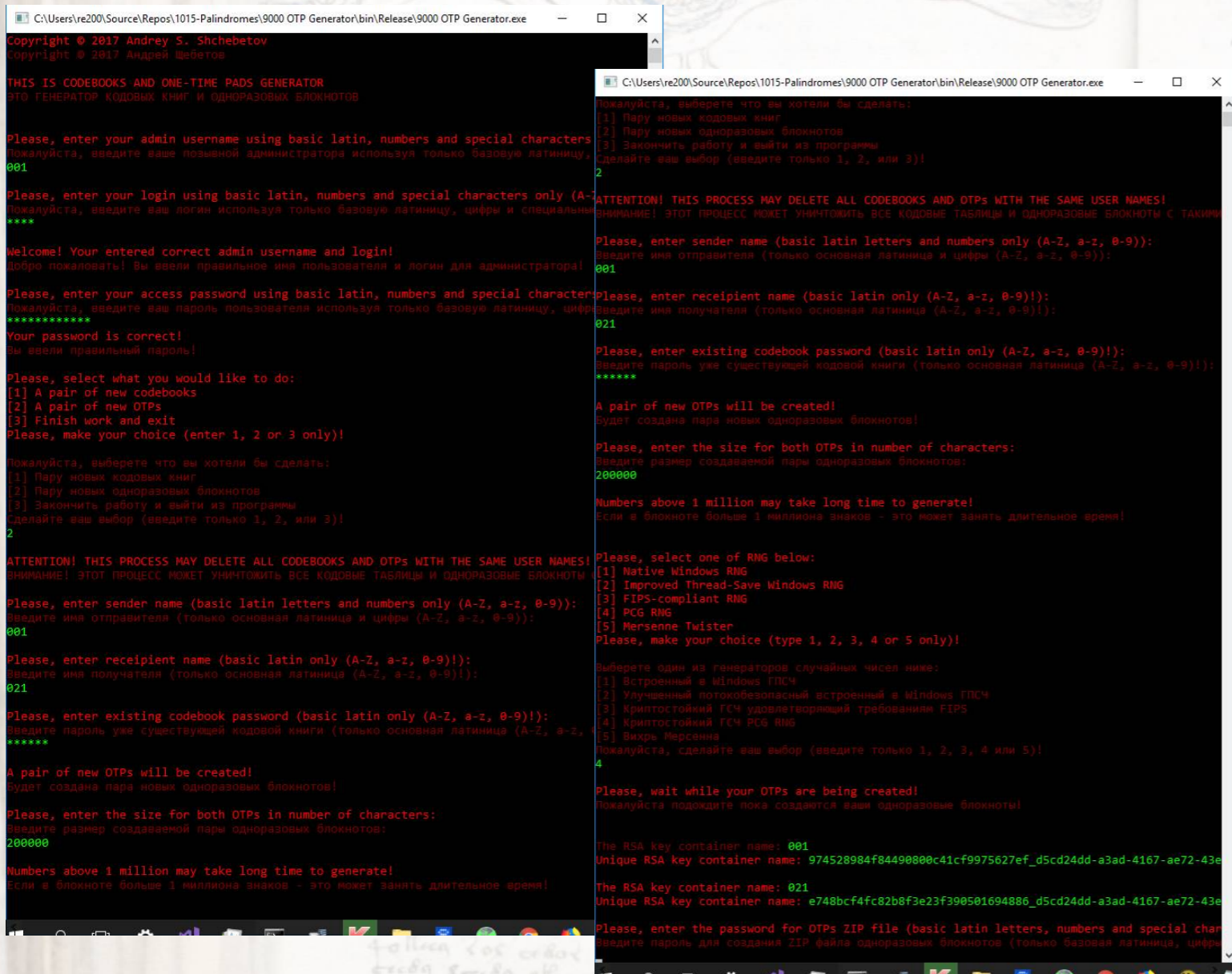
- Примерный вид пары кодовых таблиц на основе собственного алфавита из 256 символов
- 256 совпадает с цифровым значением байтов (0-255)
- Позволяет писать на русском, английском, немецком, французском и греческом языках
- Символы полностью перепутаны, нет никакого порядка
- Смена кодовой таблицы эквивалентна смене шифра

- Вид зашифрованного текста при использовании алфавита из 55295 одиночных («несуррогатных») символов UTF-16
- Большой алфавит труднее расшифровать, но требуется больше памяти
- Проверялись также сокращенные варианты (например, Base64 или алфавит из 50 символов)



Кодовые таблицы были основаны на собственном алфавите из 256 символов, который может быть расширен до 55295 одиночных символов UTF-16

OTP GENERATOR: ГЕНЕРАЦИЯ ТАБЛИЦ И ОДНОРАЗОВЫХ БЛОКНЕТОВ



The screenshot shows the OTP Generator application running in a Windows command prompt. The interface is in Russian and prompts the user for an admin username, login, access password, sender name, recipient name, and existing codebook password. It then offers options to generate new codebooks or OTPs, and prompts for the size of the OTPs and the choice of RNG (Native Windows RNG, Improved Thread-Save Windows RNG, FIPS-compliant RNG, PCG RNG, Mersenne Twister). The application displays the unique RSA key container names for the generated OTPs and prompts for a password for the ZIP file.

- Генерация кодовых таблиц (для каждой пары пользователей одна «на отправку» и одна «на получение»)
- Генерация одноразовых блокнотов (для каждой пары пользователей один «на отправку» и один «на получение»)
- Пять встроенных ГПСЧ, один из которых удовлетворяет требованиям FIPS и один (PCG) – близок к ним
- ГСЧ отличались качеством и скоростью работы
- Сохранение кодовых таблиц и одноразовых блокнотов в запароленных контейнерах на скрытом томе TrueCrypt

OTP Generator позволял генерировать кодовые таблицы и одноразовые блокноты с использованием 5 генераторов псевдослучайных чисел

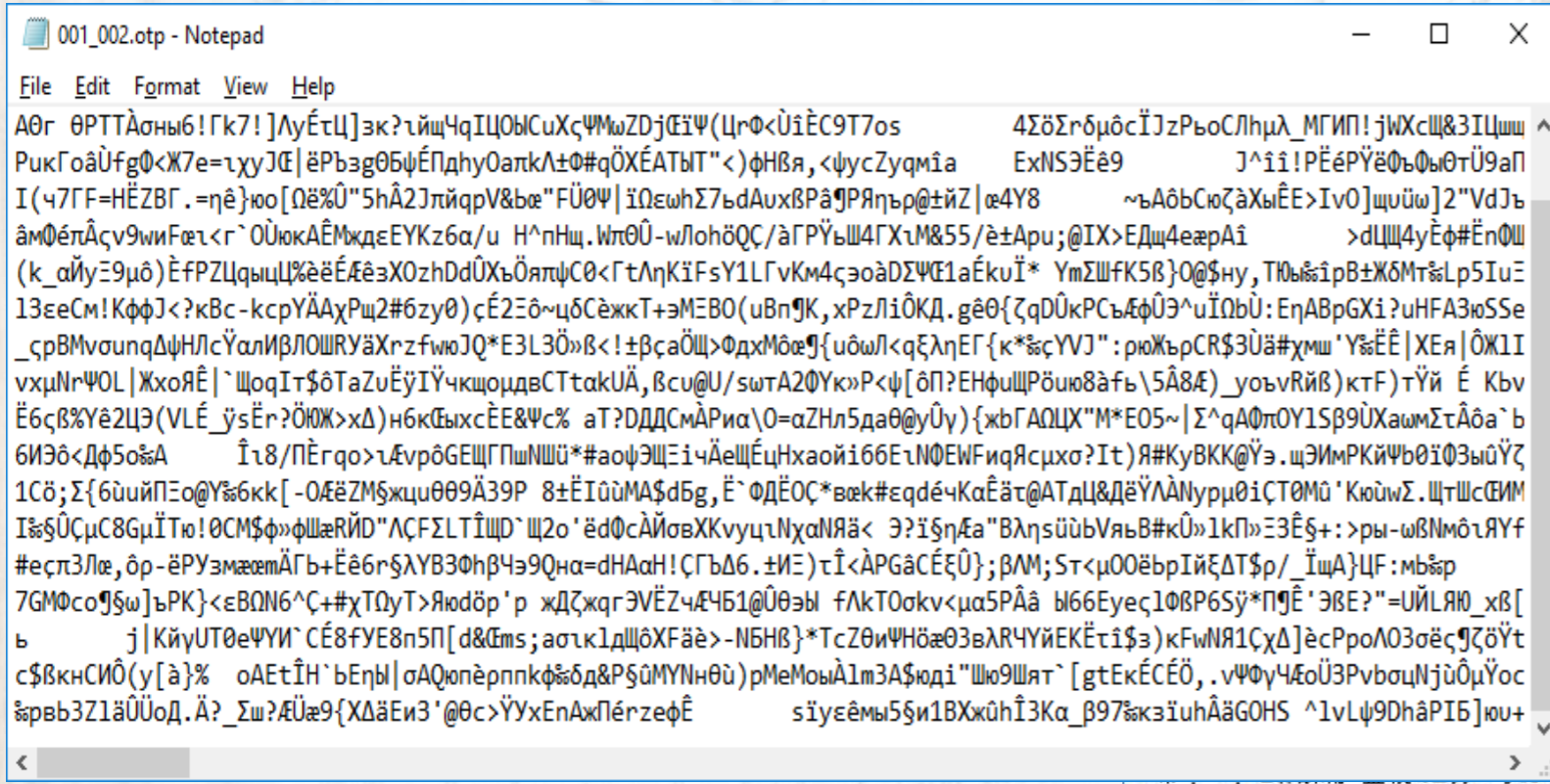
ОДНОРАЗОВЫЙ БЛОКНОТ ПОСЛЕ КОДИРОВКИ



- *Случайный набор символов без каких-либо привязанных цифровых значений*
- *Возможность замены на новый блокнот в любой момент*
- *Возможность «периспользования» блокнота при замене кодовой таблицы*
- *Хранение и пересылка только в запароленном AES-контейнере*
- *Использование — кодовой вмести с кодовой таблицей — никогда в одиночку*

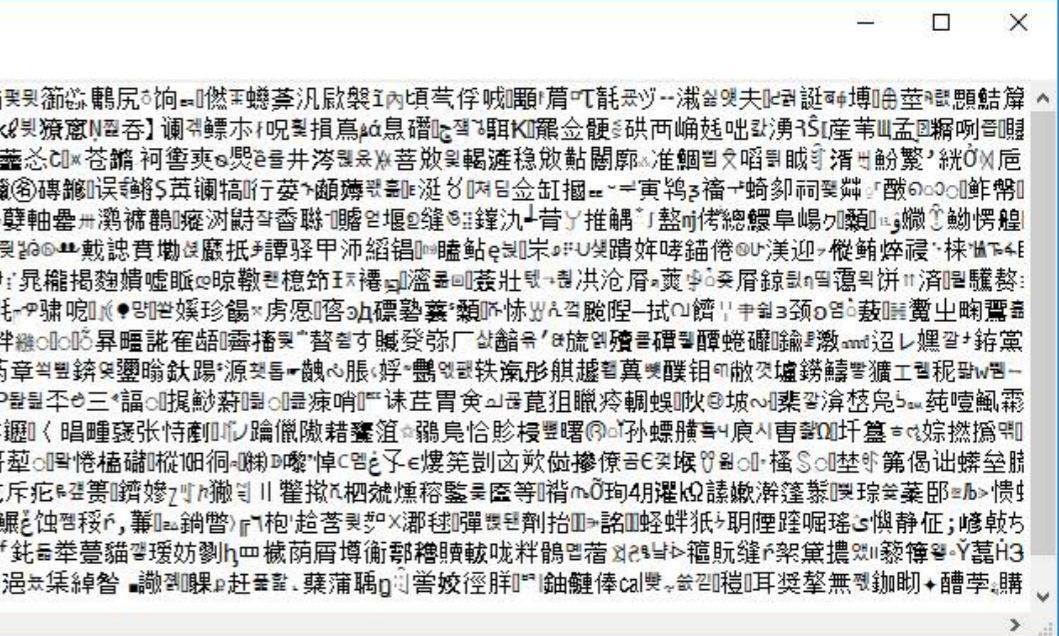
Одноразовый блокнот после кодировки всегда будет случайный текст слов и предложений из 256 повторов кодовой вмести с кодовой таблицей

ОДНОРАЗОВЫЙ БЛОКНОТ ПОСЛЕ СУПЕРШИФРОВАНИЯ



```
001_002.otp - Notepad
File Edit Format View Help
A0Г ӨРТТÀсны6!Гк7! ]ЛуÉтЦ|эк?уйчqIQOЫCuXçΨMwZDjGEiΨ(ЦрФ<ÙiÈC9T7os 4SδΣrδμδcİJzPьoСЛHμλ_МГИП!jWХсЩ&ЗЦшш
РукГоâÙfgФ<Ж7e=ιxyJε|ëPьзгӨБψÉПдhyOапкЛ±Ф#qÖХÉАТЫТ"<)ФНВя,<ψусZyqmia ExNSЭÈè9 J^i!PÈëPÿëФьФыӨтÛ9aП
I(ч7ГF=HÉZВГ. =ηè}ю[Ωè%Û"5hÀ2ÏπйqPv&bæ" FÜӨΨ| iΩεωηΣ7ьδAuxBPâϑPЯηьр@±йZ|æ4Y8 ~ьAδbCюçàХыÈE>IvO|щuüw|2"VdJь
âmФéлÀçv9mFæι<г' OÛюкАÈМждеEYKz6α/u H^пНщ. WпӨÛ-wЛohδQC/ãГРÿьШ4ГХLМ&55/è±Aру;@IX>Едщ4еарAî >dЦщ4yÉФ#èпФШ
(k_айу=9μδ)ÈèPZЦqыц%èèÈÆèзXOzhDdÛХьÏяпФçӨ<ГтЛηКiFsY1LГvкM4çэоàDΣΨε1aÈkuÏ* YmΣШfK5B|O@ф$ну, TЮы&ipB±ЖδMт&Lp5Iuε
13εεСм!КфФJ<?кВс-ксрYÄАхPщ2#6zyθ)çÉ2εδ~цδСèжкT±эMεB0(υBпϑK, xPzЛiòKд. gèθ{çqDÛкPСьÆФÛÉ^uÏΩbÛ: EηABPГХI?uHFA3ю5Se
_сpBMvounqΔψНлСÿалиВЛОШRУäXrзfвюJQ*E3L30"В<!±βсаÖЩ>ФдхMδæϑ{uδwл<qεληEГ{к*ççYVJ": рюЖьрCR$3Ûä#хмш' YçÈÈ|XЕя|ÖЖI
vxμNpΨOL|ЖхоЯÈ|`ЩоqIт$δTaZуÈÿÿÿчкцоμдвСтtakUÄ, Bcy@U/сwтA2ФYк»P<ψ[δП?EHФшцPöию8äфь\5Ä8Æ)_уоьвRйB)ктF)тÿй É Kbv
È6çB%Yè2ЦЭ(VLÈ_ÿsÈr?ÖЮЖ>хΔ)н6кГыхсÈE&Ψс% ат?DДДсMÀPиα\0=αZНл5даӨ@yÛÿ){жбГAQЦX"М*E05~|Σ^qAФπOY1Sβ9ÛХawмΣтÀäа`b
6ИЭδ<дф5о&A Îт8/ПÈГqо>ιÆνpδGEЩГпшWшÛ*#аоψЭЩεичÄеЩÉцHхаойi66EιNФEWFиЯсμхσ>It)Я#кyBKK@ÿЭ.щЭИМРКЙΨbθiФ3ыüÿç
1Cö;Σ{6üиПεо@Yç6кк[-OÆèZM$жцуθθ9Ä39P 8±ÈIùùMAdBg, È`ФДÈОç*вæк#εqдéчKaÈät@ATдЦ&дèÿLÀНурμθiCTӨMù' KюüwΣ. ЩтшсEИМ
Iç$ÛçμC8GμÏТю!ӨСMф>фшÆPЙD"ACFΣLTÏЩD`Щ2о`èdФсÄйшвХквуцлNхαNЯä< Э?içηÆа"ВληςüüбVяьB#кÛ"1кП"ε3Èç±>ры-ωβNмδιYf
#еçл3Лæ, δр-èPУзмææMÄГb+Èè6r$λYB3Фhβчэ9Qна=dHааH!ÇГьΔ6. ±ИE)тÏ<ÀPGäCÉÉÛ);βM;Ст<μ00èбрIйЭΔT$р/_ÏщA|ЦF:мб&ер
7GMФсоϑ$w|ьPK<εεBQN6^ç+#хQтyT>Яюдөр'р ждçжqгЭVÈZч4ЧБ1@ÛθэЫ fЛKTOскv<μα5PÄâ Ы66Eуеç1ФBP6Sÿ*ПϑÈ'ЭBE?"=УЙЛЯЮ_хB[
ь j|КйУТӨеΨYИ' СÈ8FУE8п5П[d&çms; асчк1дщòXFèè>-NBHВ)*TçZӨиФHèè3вARЧYЙEKÈтiç$)кFwNЯ1çXΔ]èçPpoΛ03эèçϑçöÿт
с$βкнСИÔ(y[à}% оAEтÏH`bEηЫ|σAQюпèрпкф&δd&P$ÛMÛNнθü)рMeMoyÀ1MзA$юдi`Шю9Шят`[gtEKéCÉÖ, .vФoγч4èOÛ3PvсoцNjüöμÿoc
&рвб3Z1äÛöД.Ä?_Σш?ÆÛæ9{XΔäEи3'@θс>ÿУхEnАхПérзeфÈ siyеéмы5çи1ВХжüиÏ3Ka_β97%кзiuhÄâGONS ^1vLψ9DhâPIB]ю+
<
```

- Одноразовый блокнот был полностью пригоден для супершифрования
- Вид одноразового блокнота после 16 раундов шифрования AES и «обертывания» в кодовую таблицу
- Тот же беспорядочный и бессистемный набор из 256 символов



```

<
```

- Вид одноразового блокнота при использовании 55295 символов кодировки UTF-16

Сам одноразовый блокнот может быть зашифрован с помощью супершифрования с использованием традиционных алгоритмов

ВИД УДЛИНЕННОГО КЛЮЧА ПОСЛЕ СУПЕРШИФРОВАНИЯ

```
key001_002.key - Notepad
File Edit Format View Help
|+zLdTKxiAxGQP8jgXpgpC5n8stgoeL1Jv/ofQ4w4p7Y= KaNMGFTAnfrMq0thN88iURbdn/J30JjZcOFQ1WfqsMo=
6v1yxRnY9RQTZLE9kKex1xupMQyhVdzG9ncqzwz10Ddo= yAY1+hX3szvf8nQLzsvGd3vWaEFRIMtVPLrwh0MQckY=
dVjgm0BbS1y4s1n6UUY6YCg4q0mppebqKNat+AVSVyg= Kq3+R1FvD/8kqXP1gW65Z5nAYi0QhMhe0KHuHM9QZzQ=
m03PeyUVhCt2Qg+/+zBnGHeF+biVc3mEp37naDPiUic= ZTfulnjp0wzUoLBFwSh8101at1p2BD1VJa/pLInt3z8=
y1HIgJ0P90gwyMXIjJhS2aPBGB0BAQUC/H5n8Z6jMR0= giR4RiTDr2Jw2IKU0CgeVch4aqKID56ntnqeQ0eA7j0=
mUAayAMDZFIJfY1s6jZ8PzQtv/yj59fc2WX0p4Mox34= ST26ipM4+yTmoj3tKb4nnBX2+bzmIw2sbAH39X14K8I=
+qn4nAELtE4pINsv2ubkq01LVSsyfFTVJfufp5iyFy0= 6gKwJouuf+GBEv6rSz0wc2x9Bz/blM0diJksUa30wns=
gr0NggDaJq+OKRK0Soz30I3sifDRhstHD/+8wpTR2+w= zwLph22spnrz7fYDb1nT6U19fn2dqUyi0TPNiT7kZbA=
```

```
iv001_002.key - Notepad
File Edit Format View Help
DQyZD0quidUsXRgJAeGU1A== bGkwdTuKLjmskiL1m/ILDg==
a/4ijGBFXHCNenR5+400hg== 0CNLdk4VuowHANdOUU4DcA==
dkrYAJ5wHSyqmQ/jMe9C/g== kpgISNT3ztD1TKkbz5NOUg==
Wr8uFaM15LBSMbyL4QAWgA== vXWe1bVb0SgRPGi4XMFtxg==
GYDncS6ex8VLVxajx/sbuA== ILf5Bp3dzraSo7KvNxssGg==
kY2L70kTu6uS60FOEEzaFA== pgNC+YcwhL19PftoYw/DOQ==
dWJsgKHK1zP/qX7z233oTg== 1h/GXDDiwmq+cXAWuNNZuA==
g52hDG3ZrB+3j1o0pU8Zyg== 19E25+U4WYnN3C/G3xFsfA==
```

```
combinedkey - Notepad
File Edit Format View Help
pA07vψw0é±VHЛyИкPçюHÉuаЧmрΔυπv75Σγ|Ä<AÈIэ<9к>}^хEQлЬхËÛЯJηUрχ¶ñiCkδBÈs4Èì<Î; ;LψiδÛOGÙ~S5nzÀÀЭ, vöqP$H
\YœHiÛéηQEεφ&'IGæFdOц5+к}дВпGЧΣÈ6р" [яЗЧфу! 'MÏм'Э =~ЮÛщ?ÂПæ%ЦÛоrеÁй6ПiНйf=k\ .KTiÛccagNTdôzл1
фдпс3кysÈBÛшA9: üБ|ьСЕШТ/ÔÏГЖьжç4Nz0θλ!рБбЦПúзсщшYC!ü{+ПТсçгTe@пΣ; EΣÉψлLÈцEÔBа0%бè(ЦПтH+уУЩP4
_CZьщ0A0Kd, §}эпФП8ÿ0^ПaцбXл§À§б- | ?ЭЖр0 [CIAÛ^YTD^ÈèФ, че»МБ?È{SÛOLBadYР8ыJLK/Mè6]δЯ~0wхуц0тÿ{bCηΣTD
§BYIäñÛB1HкûGор [ωтоAцGФHñÈЛ(ξèXγхT$ЩçмДк¶YÛÄÛEáéabÆvПâiÿу6сP0жÆ}эΨèщцæ=δЫbAИомьε0ь0хö?
yaReyxθÈÏφopse"0λSÛKÛ> |EwьÎ|Û=*MKçacψφξΣε6èрPч(ьiωг~ÆуNеü)èЮR(сэпEi4Umj$0rÀ [XeË0PГr0Vч; jÿ
```

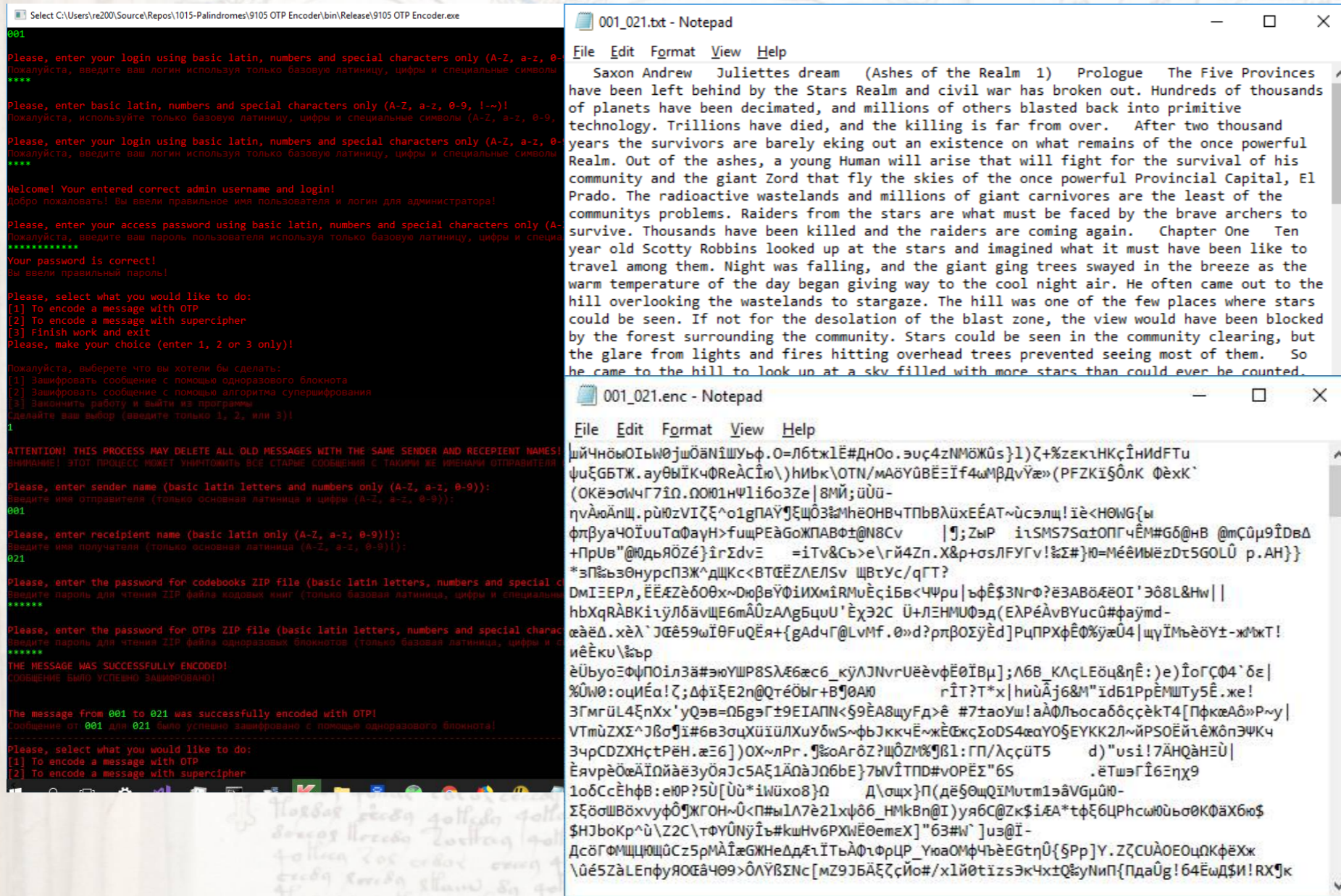
• Примерный ключа в кодировке Base64 до шифрования оригинального ключа кодовой таблицей

• Примерный вид векторов инициализации в кодировке Base64 до шифрования оригинального ключа кодовой таблицей

• Типичный вид ключа после применения кодовой таблицы и одноразового блокнота

Удлиненный ключ после супершифрования выглядел как текст из 6144 символов кодировочной таблицы

OTP ENCODER: ШИФРОВАНИЕ СООБЩЕНИЙ



- *Пример шифрования с помощью одноразового блокнота*
- *На входе – англоязычный текст*
- *На выходе невозможно определить язык, разбить на слова и предложения, понять, где знаки препинания*
- *При шифровании одноразовым блокнотом одного и того же текста на выходе всегда будет другой шифротекст*

OTP Encoder позволял шифровать открытый текст с помощью одноразового блокнота в шифротекст из которого невозможно было определить даже язык

OTP DECODER: РАСШИФРОВКА СООБЩЕНИЙ

```
Select C:\Users\re200\Source\Repos\1015-Palindromes\9105 OTP Decoder\bin\Release\9105 OTP Decoder.exe
Сделайте ваш выбор (введите только 1, 2, или 3)!
1
ATTENTION! THIS PROCESS MAY DELETE ALL OLD MESSAGES WITH THE SAME SENDER AND RECIPIENT NAMES!
ВНИМАНИЕ! ЭТОТ ПРОЦЕСС МОЖЕТ УНИЧТОЖИТЬ ВСЕ СТАРЫЕ СООБЩЕНИЯ С ТАКИМИ ЖЕ ИМЕНАМИ ОТПРАВИТЕЛЯ И ПОЛУЧАТЕЛЯ
Please, enter sender name (basic latin letters and numbers only (A-Z, a-z, 0-9)):
Введите имя отправителя (только основная латиница и цифры (A-Z, a-z, 0-9)):
001
Please, enter receipt name (basic latin only (A-Z, a-z, 0-9)!):
Введите имя получателя (только основная латиница (A-Z, a-z, 0-9)!):
021
Please, enter the password for codebooks ZIP file (basic latin letters, numbers and special characters only)
Введите пароль для чтения ZIP файла кодовых книг (только базовая латиница, цифры и специальные символы)
*****
Please, enter the password for OTPs ZIP file (basic latin letters, numbers and special characters only)
Введите пароль для чтения ZIP файла одноразовых блокнотов (только базовая латиница, цифры и специальные символы)
*****
Saxon Andrew
Juliettes dream
(Ashes of the Realm 1)
Prologue
The Five Provinces have been left behind by the Stars Realm and civil war has broken out. Hundreds of thousands of planets have been
killing is far from over.
After two thousand years the survivors are barely eking out an existence on what remains of the once powerful Provincial Capital, El Prado. The radioactive wastelands and millions
rive. Thousands have been killed and the raiders are coming again.
Chapter One
Ten year old Scotty Robbins looked up at the stars and imagined what it must have been like to travel among them. Night was falling,
he cool night air. He often came out to the hill overlooking the wastelands to stargaze. The hill was one of the few places where stars could be seen. If not for the desolation of
rest surrounding the community. Stars could be seen in the community clearing, but the glare from light
So he came to the hill to look up at a sky filled with more stars than could ever be counted. He had
way to go out to see the beautiful universe above him.
He knew most of those stars were distant. According to information in the learning center, the closest
d that there was an intelligent species that once lived at that star. He wondered if they were still there.
Now he stared at a sky full of stars that blinked at him with colors that were beautiful. The ging
undred foot trees. The light yellow-colored grass felt good under his back and he thought about his mother.
She was beautiful, and possessed the kindest spirit in the communities. The community loved her, and
anyone to come close. Those six-legged beasts were suspicious by nature and only stayed around the commu
rt them howling and they could be heard for miles. They learned the smell of everyone that lived in the
ty meal. They were territorial, and only one family of them occupied the area surrounding the two comm
community knew the birth of a newborn immediately as it was announced by the howls of the gunds. It us
Scotty looked up at the stars and knew not everything up there was good. Five years earlier a stars
ld give warning. Everyone ran for the forest but one of the invaders fired a blaster beam at a fleeing
He was with his father in the forest gathering pods from the grellup vines, heard the sizzle of the
ed there was nothing of value to steal. The learning center was spared due to it being hidden deep in
ventually boarded their ship and disappeared into the afternoon sky.
His father never recovered from his mothers death. The community mourned her loss more than the bur
understood why he longed to escape his constant grief. His few remains were buried next to his wife.
Scotty was raised by the community. Everyone considered him one of their own and he slept wherever
Scotty looked up at the stars again and knew that once there was a kingdom of beauty and light when
The message from 001 to 021 was successfully decoded with OTP!
Сообщение от 001 для 021 было успешно расшифровано с помощью одноразового блокнота!
Please, select what you would like to do:
```

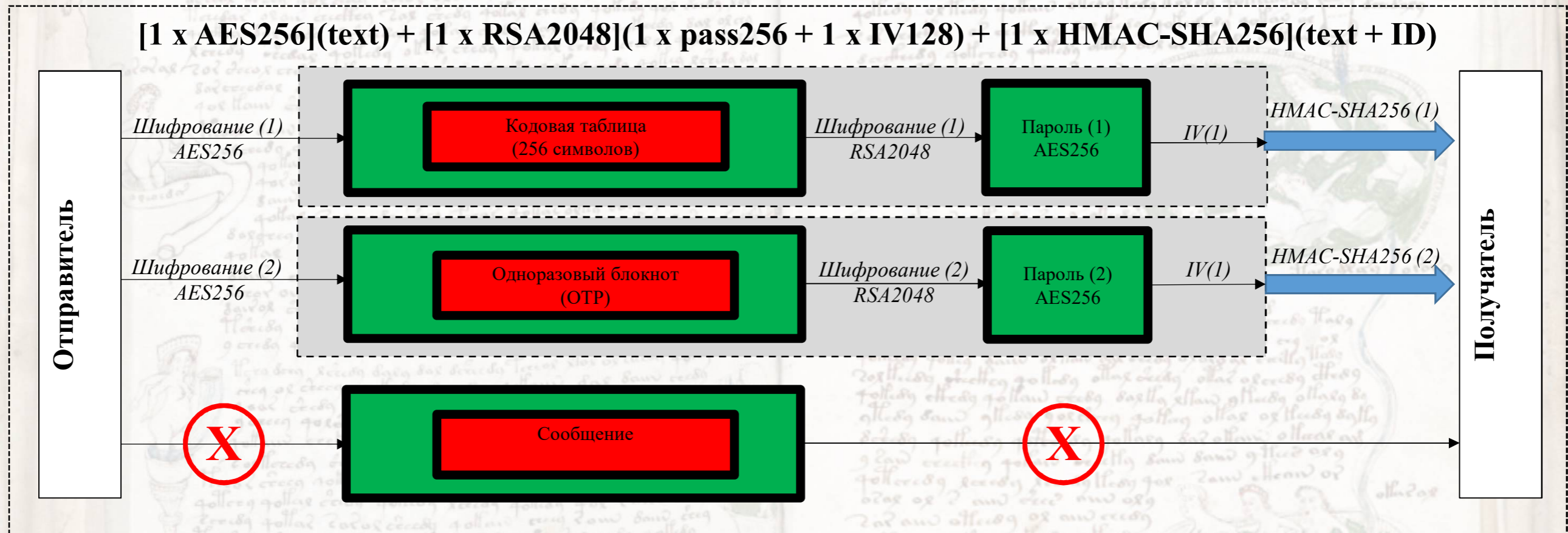
```
001_021.enc - Notepad
File Edit Format View Help
ШЙЧНӨЫОІЪWӨjшöäNіШуьф.0=л6тжлЕ#Дн0о.эуç4zNMöЖÜs}l)ç+%zеклHKçİниdFTu
ψυξGБТЖ.ауӨЫІКчФReÀСІю\нИвк\OTN/мАöYÜBEЭİf4wмРДvYæ»(PFZKі$ÖлК Фèкк`
(OKÈэöwчГ7İñ.ÑOЮ1нΨ1і6о3Ze|8MЙ;üÜ-
ηνΆοΑпш.рùЮzVIZç^o1gПАУҖҖЩöзMhèOHвчТПбVлұхЕÉАт~ùсэлщ!iè<HӨWҖ{ы
фтРyаЧOİууТoФayн>фуцPЕàGоЖПАВФ±@N8Cv |Җ;ZыP іrSMS7Sα±OPгчÈM#Gδ@нВ @mçúм9İDвΔ
+ПрУв"®ЮдьЯÖZé}іrSdvЭ =іTv&Сь>е\гй4Zп.X&р+σsLFYҮГv!§z#}Ю=МéÈИЫèzDт5GOLÜ р.АН}}
*эП§ьэӨнурсПЗЖ^дщКс<ВТЄÉZЛЕЛsv щвтУс/қГТ?
DмIЭEPл,ÈÈÆZèδOӨx~DюβVҖiIXmIRMUÈçіBв<Чψp|ьфÈ$3NгФ?эЗABδÆèOI'Эδ8L&Hw||
hbXqRÀBKіrүлδävщE6mÁÛzAлҖбцУ'ÈхЭ2C Û+лЭHМУЭд(ЕлPéÀvBYУсú#фaymd-
æàèΔ.хèλ`JÆè59wİӨFuQÈя+{gAdчҖ@Lvmf.Ө»d?рпBOСyèd}PцПРХФÈФ%yæÜ4|щҖİМьèèöY±-жмкт!
иèÈку\§ьр
èÜbyоЭФпOілзä#эюYШP8SΛE6æс6_күЛJNvrUèèвфÈӨİBм];Λ6B_кЛçLEöç&ηÈ:е)İoҖCФ4`δе|
xҖIш0.руMÈç1Z.АфİEЭ2p@отçöHч+PҖQAM çİТ?Т*ү!hуüäİç6RM"İdE1PөÈMИТvSÈ_яe!
001_021.txt - Notepad
File Edit Format View Help
Saxon Andrew Juliettes dream (Ashes of the Realm 1) Prologue
The Five Provinces have been left behind by the Stars Realm and civil
war has broken out. Hundreds of thousands of planets have been
decimated, and millions of others blasted back into primitive
technology. Trillions have died, and the killing is far from over.
After two thousand years the survivors are barely eking out an
existence on what remains of the once powerful Realm. Out of the ashes,
a young Human will arise that will fight for the survival of his
community and the giant Zord that fly the skies of the once powerful
Provincial Capital, El Prado. The radioactive wastelands and millions
of giant carnivores are the least of the communitys problems. Raiders
from the stars are what must be faced by the brave archers to survive.
Thousands have been killed and the raiders are coming again. Chapter
One Ten year old Scotty Robbins looked up at the stars and imagined
what it must have been like to travel among them. Night was falling,
and the giant ging trees swayed in the breeze as the warm temperature
of the day began giving way to the cool night air. He often came out to
the hill overlooking the wastelands to stargaze. The hill was one of
the few places where stars could be seen. If not for the desolation of
the blast zone, the view would have been blocked by the forest
```

- *Пример зашифрованного сообщения*
- *Расшифровка выполнялась в обратном порядке*
- *Сообщение записывалось в виде текстового файла и выводилось на экран, а также записывалось в соответствующую директорию на хард диске*

OTP Decoder позволял расшифровывать сообщения, зашифрованные с помощью одноразового блокнота

ПРОТОКОЛЫ: ОБМЕН ПРИ ОТСУТСТВИИ ОБЩИХ ТАБЛИЦ И БЛОКНЕТОВ

ОБМЕН КОДОВЫМИ ТАБЛИЦАМИ, ОДНОРАЗОВЫМИ БЛОКНЕТАМИ И СООБЩЕНИЯМИ: ВАРИАНТ 1

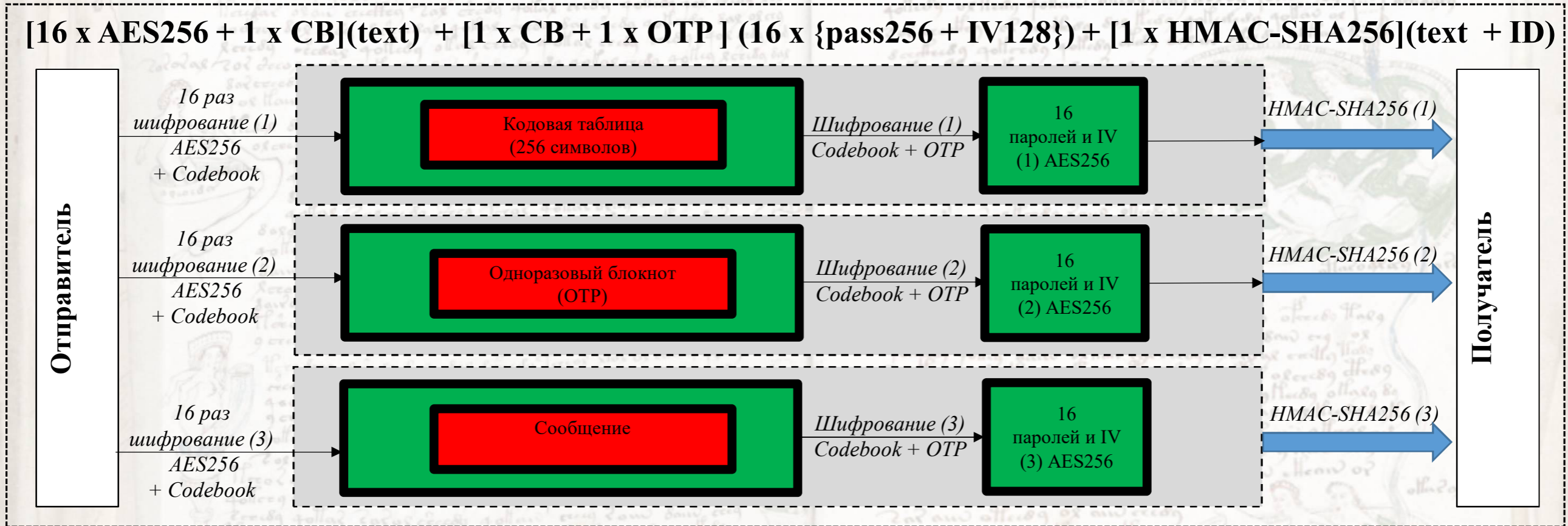


При отсутствии у пользователей общих кодовых таблиц и одноразовых блокнотов они могут ими обмениваться традиционным способом: AES + RSA

ПРОТОКОЛЫ: ОБМЕН ПРИ СУПЕРШИФРОВАНИИ

ОБМЕН КОДОВЫМИ ТАБЛИЦАМИ, ОДНОРАЗОВЫМИ БЛОКНОТАМИ И СООБЩЕНИЯМИ: ВАРИАНТ 2

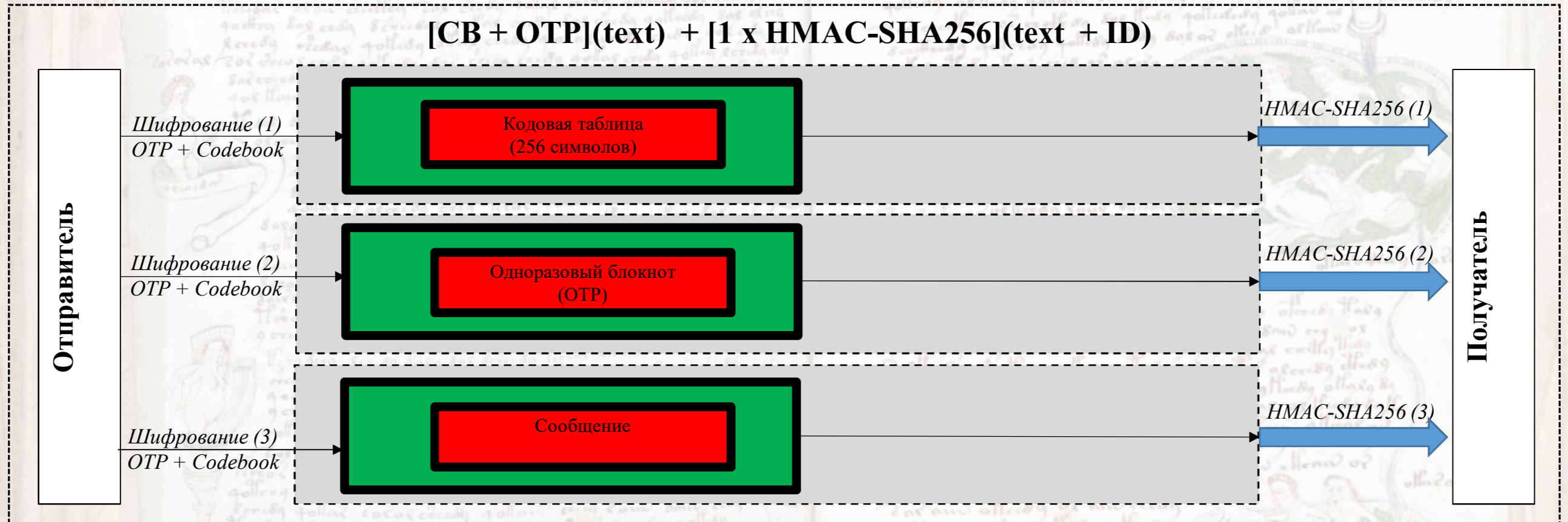
$[16 \times \text{AES256} + 1 \times \text{CB}](\text{text}) + [1 \times \text{CB} + 1 \times \text{OTP}] (16 \times \{\text{pass256} + \text{IV128}\}) + [1 \times \text{HMAC-SHA256}](\text{text} + \text{ID})$



При наличие общих кодовых таблиц и небольших одноразовых блокнотов обмен может идти по протоколу супершифрования для экономии блокнота

ПРОТОКОЛЫ: ОБМЕН С ИСПОЛЬЗОВАНИЕМ ОДНОРАЗОВЫХ БЛОКНОТОВ

ОБМЕН КОДОВЫМИ ТАБЛИЦАМИ, ОДНОРАЗОВЫМИ БЛОКНОТАМИ И СООБЩЕНИЯМИ: ВАРИАНТ 3



При наличии достаточно большого одноразового блокнота весь обмен идет только с его помощью, что является самым простым и эффективным способом связи

РЕЗУЛЬТАТЫ

- *Построен прототип системы шифрования на основе одноразовых блокнотов, кодовых таблиц и супершифрования (включая 4 написанные на C# программы-модуля)*
- *Создан собственный алфавит из 256 символов для создания кодовых таблиц*
- *Рассмотрены другие возможные алфавиты*
- *Предложено три протокола обмена кодовыми таблицами и одноразовыми блокнотами*
- *Проверены 5 генераторов случайных чисел*
- *Проверена работоспособность системы в различных вариантах и сочетаниях*
- *Проверена схема супершифрования с использованием AES, одноразовых блокнотов и кодовых таблиц*
- *Обеспечена физическая безопасность и наличие «достоверного отрицания» сборки при помощи TrueCrypt*
- *Дальнейшие шаги:*
 - *Доработка прототипа до полной функциональности*
 - *Разработка полноценного ПО с GUI на базе прототипа*
 - *Внедрения одноразовых блокнотов в систему обмена одноразовыми сообщениями типа PubNub*

В результате реализации проекта построен прототип системы шифрования на основе одноразовых блокнотов, который можно дорабатывать дальше