**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра ИБ**

отчет

**по лабораторной работе №4**

**по дисциплине «Криптографические методы защиты информации»**

Тема: **Изучение асимметричных протоколов и шифров**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 9363 |  | Труханова В.А. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2023

**Цель работы:**

Исследовать протокол Диффи-Хеллмана, шифр RSA и получить практические навыки работы с ними, в том числе с использованием приложения Cryptool 1 и 2.

**Протокол Диффи-Хеллмана**

* + 1. **Задание**
* Запустите утилиту *Indiv. Procedures → Protocols → Diffie-Hellman demonstration…* и установите все опции информирования в ON;
* Выполните последовательно все шаги протокола;
  + Сохраните лог-файл протокола для отчета (пиктограмма с изображением ключа);
* Используйте полученный общий ключ для зашифровки и расшифровки произвольного сообщения. Шифр выберите самостоятельно.
  + 1. **Основные параметры и схема протокола**

Протокол Диффи-Хеллмана является первым из опубликованных алгоритмов на основе открытых ключей. Обычно данный алгоритм называют обменом ключами по схеме Диффи-Хеллмана.

Цель схемы – обеспечить двум пользователям защищенную возможность получения симметричного секретного ключа.

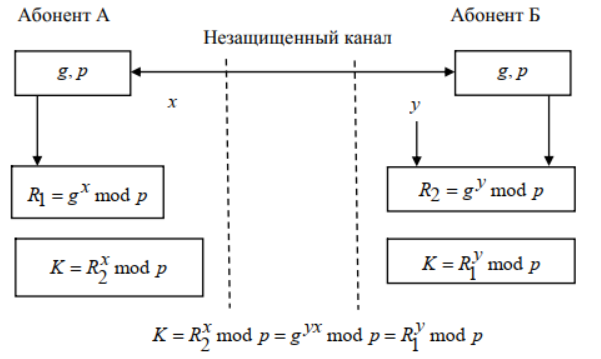


Рисунок 1- Схема протокола Диффи-Хеллмана

Протокол Диффи–Хеллмана состоит из следующих операций (рис. 7.1):

* Устанавливаются открытые параметры p, g:

а) p – большое простое число порядка 300 десятичных цифр (1024 бит);

б) g – первообразный корень по модулю p.

* Каждая из сторон генерирует закрытый ключ – большое число x и yсоответственно.
* На каждой стороне вычисляется открытый ключ:

а) ,

б) .

Стороны обмениваются открытыми ключами и вычисляют общие данные K для создания симметричного ключа: .

* + 1. **Демонстрация работы протокола**

Публичные параметры автоматически генерируются генератором с длиной 56 бит:

, ;

, y = 58968417830920481.

На каждой стороне вычисляется открытый ключ:

, .

И на последнем шаге генерируем симметричный ключ:

.

Схема протокола, реализованная в Cryptool

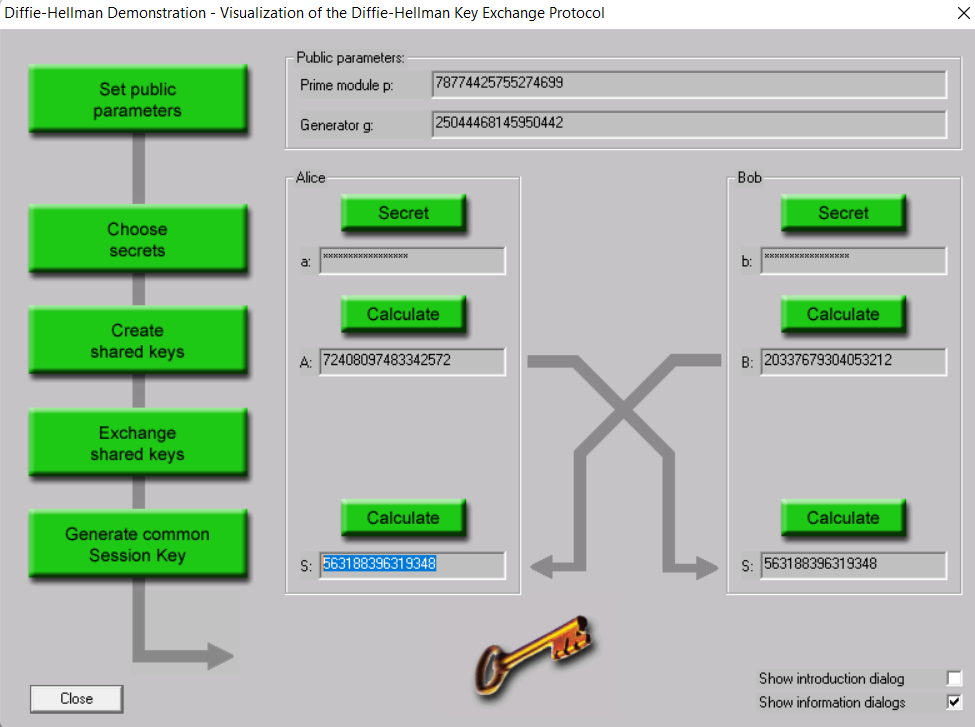
****

Рисунок 2 – Окно «Diffie-Hellman demonstration»

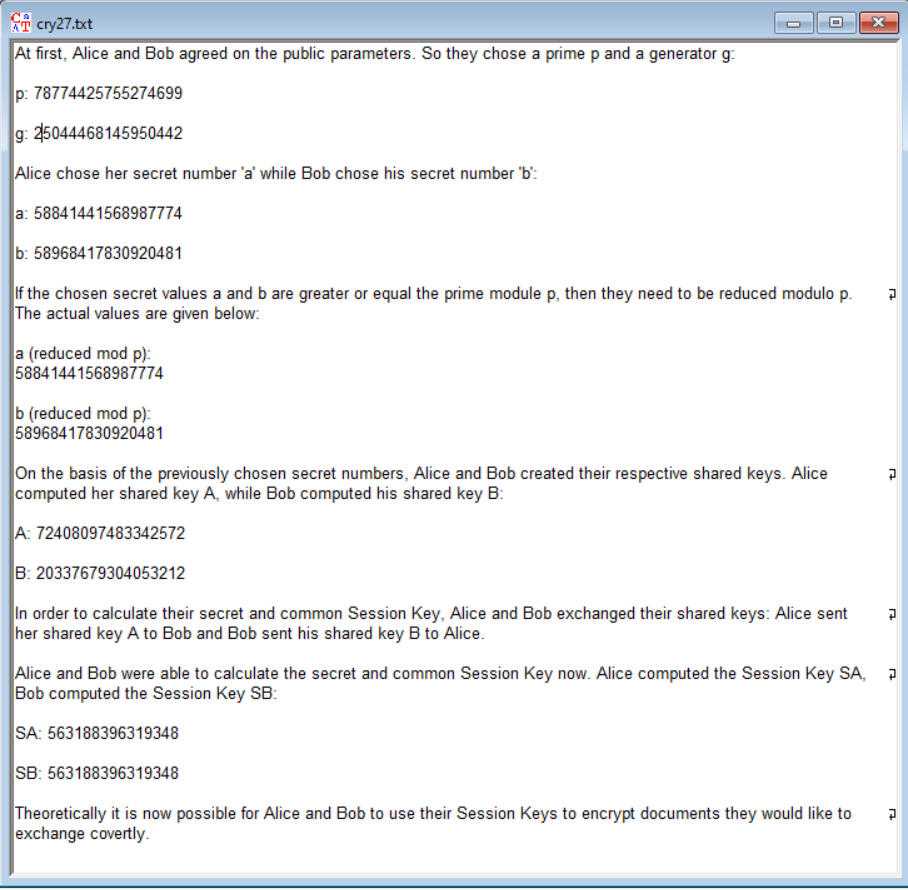


Рисунок 3 – Лог-файл протокола Диффи-Хеллмана

* + 1. **Таблица соответствия демонстрации протокола и параметров протокола**

Таблица 1. Соответствие параметров

|  |  |
| --- | --- |
| Параметр протокола | Cryptool |
| Открытые параметры | p, g |
| Открытый ключ | , |
| Секрет (Закрытый ключ) | x, y |
| Общий секретный ключ | K |

* + 1. **Исходный, зашифрованный и расшифрованный тексты**

Для шифровки сообщения был использован шифр DES(ECB).

.

Результаты шифровки и дешифровки приведены на Рисунке 4.

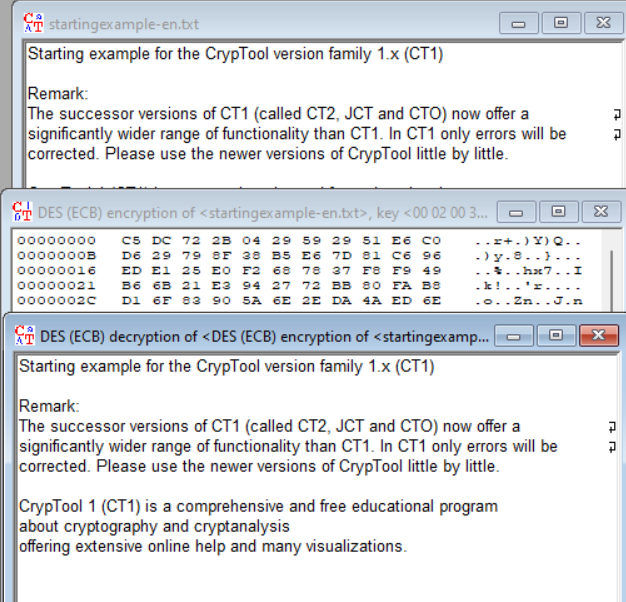


Рисунок 4 – Результат шифровки и дешифровки

**Шифр RSA**

* + 1. **Задание**
* Запустите утилиту *Indiv. Procedures → RSA Cryptisystem → RSA Demonstration…*;
* Задайте в качестве обрабатываемого сообщения своё Ф.И.О.;
* Сгенерируйте открытый и закрытый ключи;
* Зашифруйте сообщение. Сохраните скриншот результата;
* Расшифруйте сообщение. Сохраните скриншот результата;
* Убедитесь, что расшифрование произошло корректно;
  + 1. **Обобщенная схема протокола шифрования RSA**

Алгоритм RSA представляет собой асимметричный блочный шифр, в  
котором блоки открытого и зашифрованного сообщений представляются целыми числами из диапазона от 0 до n – 1 для блока размером бит.

Алгоритм шифрования RSA состоит из следующих операций:

1. Вычисление ключей:

а) генерируются два больших простых числа p и q (держатся в секрете);

б) вычисляется ;

в) выбирается произвольное число , взаимно простого с (функцией Эйлера);

г) вычисляется число d: ;

д) числа (e, n) составляют открытый ключ, d – закрытый ключ, p и qуничтожаются.

2. Зашифрование:

а) открытый текст разбивается на блоки (числа) : ;

б) каждый блок открытого текста преобразуется в шифротекст по формуле:

.

3. Расшифрование:

а) шифротекст представляется блоками (числами) : ;

б) каждый блок шифротекста преобразуется в открытый текст по формуле:

.

Обобщенная схема шифра RSA представлена на рисунках 5.

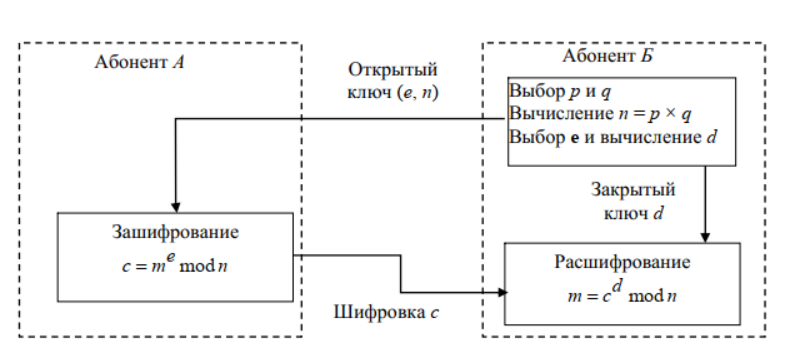


Рисунок 5 – Обобщенная схема шифра RSA

**7.2.3. Результат генерации ключей, зашифровки и расшифровки**

Запущена утилита *RSA Demonstration…*. Диалоговое окно представлено на рисунке 6.

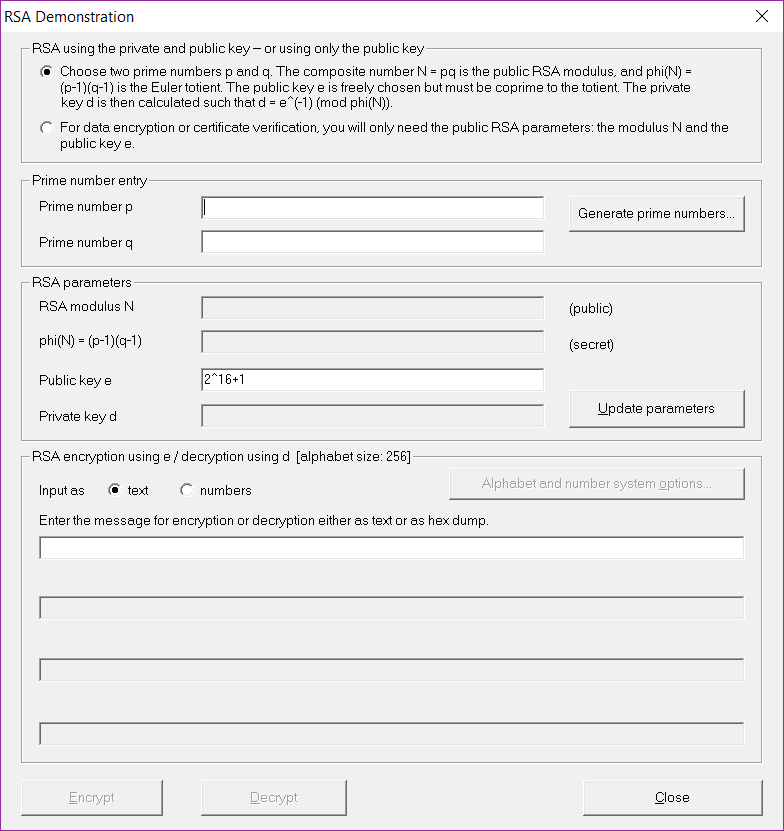


Рисунок 6 – Окно «*RSA Demonstration»*

На рисунке 7 представлен результат генерации ключей.

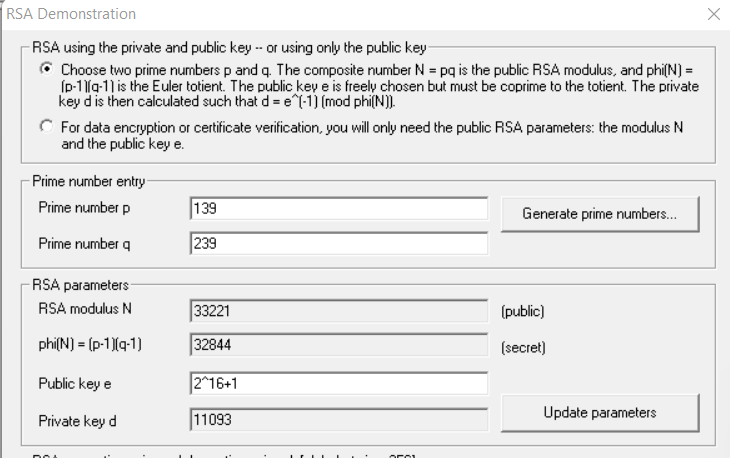
**

Рисунок 7 – Генерация ключей

С помощью данной утилиты было проведено зашифрование сообщения при заданных параметрах. Параметры и результат шифрования приведены на рисунке 8.

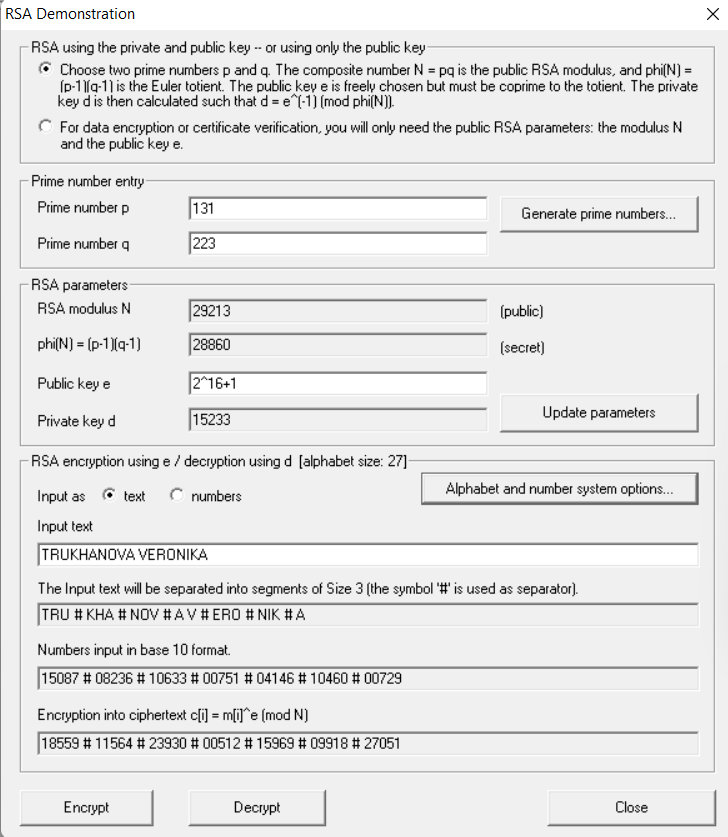


Рисунок 8 – Результат шифрования

На рисунке 9 представлен результат дешифрования текста.

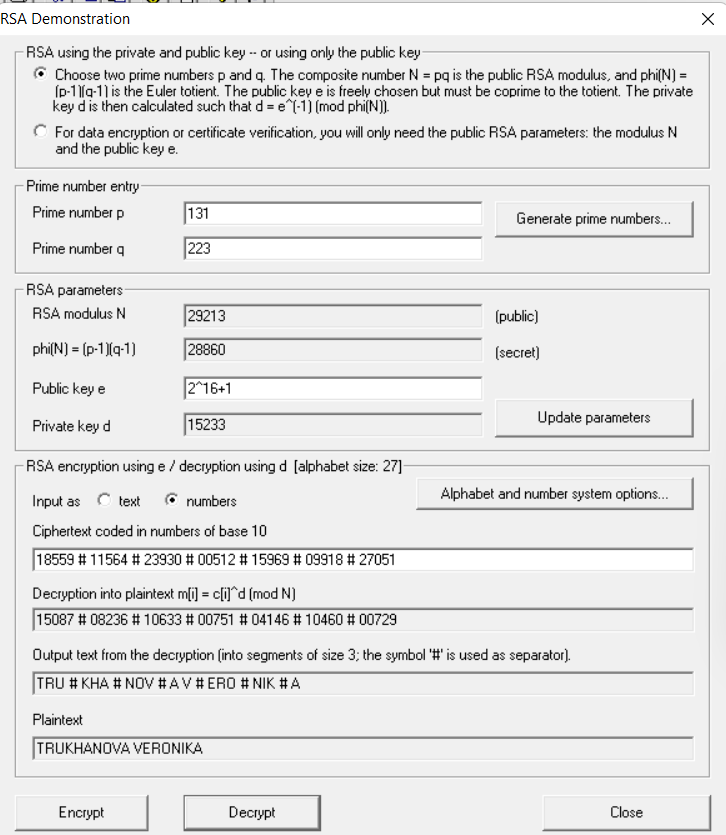


Рисунок 9 – Результат дешифрования

**Исследование шифра RSA**

* + 1. **Задание**
* Выбрать текст на английском языке (не менее 1000 знаков) и сохранить в файле формата \*.txt;
* Cгенерировать пары ассиметричных RSA-ключей утилитой *Digital Signatures → PKI → Generate/Import Keys* с различными длинами (4 варианта);
* Зашифровать текст (примерно 1000 символов) различными открытыми ключами. Зафиксировать время зашифровки;
* Расшифровать текст различными закрытыми ключами. Зафиксировать время зашифровки;
* Проверить корректность расшифровки. Зафиксировать скриншоты результата.
  + 1. **Выбранный текст**

На Рисунке 10 представлен текст на английском языке в формате .TXT. (Размер текста: 1115 символов)

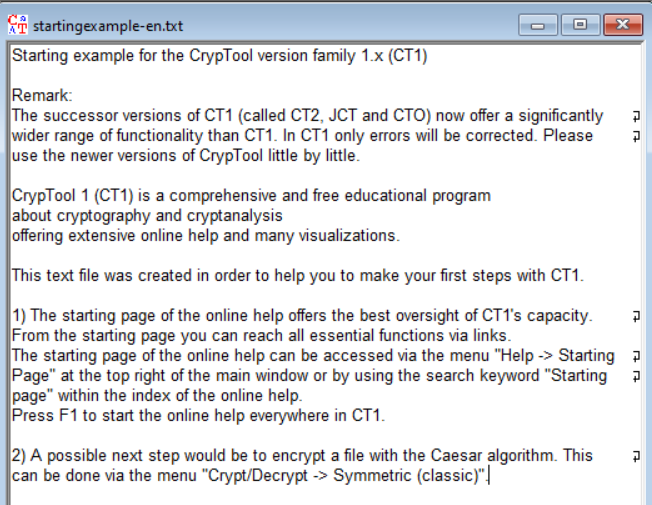


Рисунок 10 – Исходный текст

* + 1. **Результаты генерации ключевых пар различной длины**

Cгенерированы пары ассиметричных RSA-ключей утилитой *Digital Signatures → PKI → Generate/Import Keys* с различными длинами (512, 768, 1024, 2048 бит). Результаты представлены на рисунке 11-14.

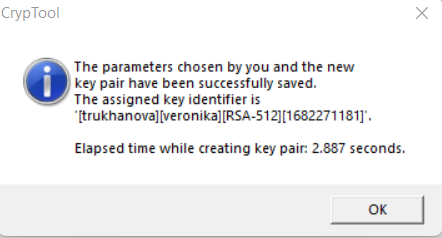


Рисунок 11 – Генерация ключа длиной 512 бит

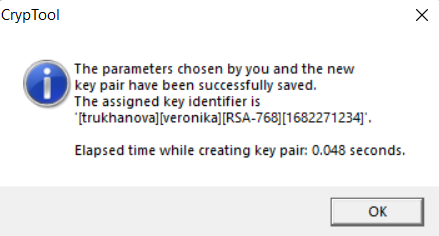


Рисунок 12 – Генерация ключа длиной 768 бит

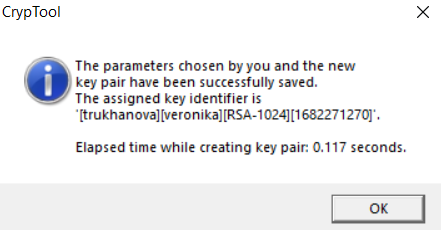


Рисунок 13 – Генерация ключа длиной 1024 бит

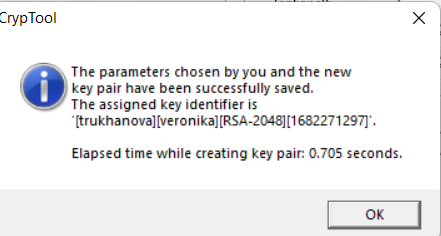


Рисунок 14 – Генерация ключа длиной 2048 бит

* + 1. **Шифровка и расшифровка текста ключами разной длины**

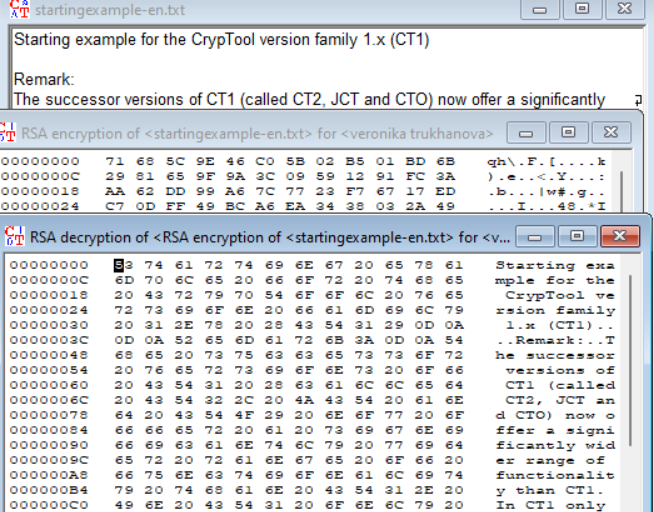


Рисунок 15 – Результаты шифровки и раcшифровки исходного текста (512)

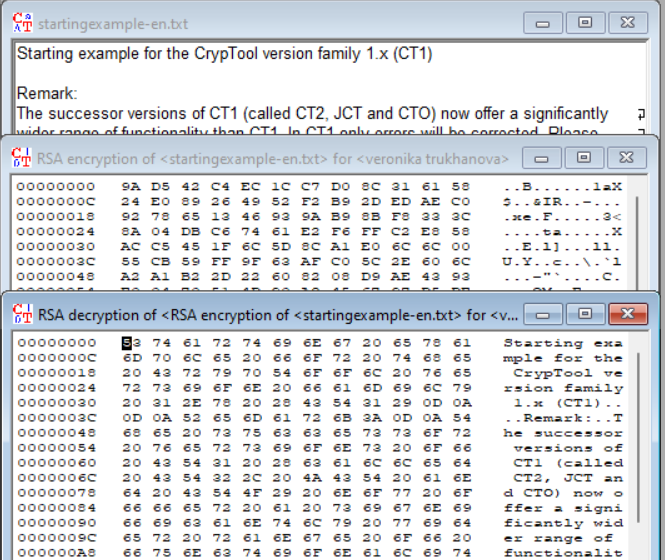


Рисунок 16 – Результаты шифровки и расшифровки исходного текста (768)

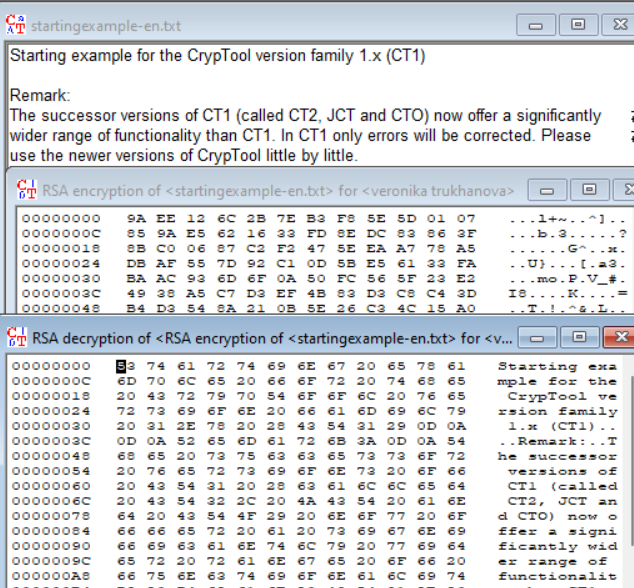


Рисунок 14 – Результаты шифровки и расшифровки исходного текста (1024)

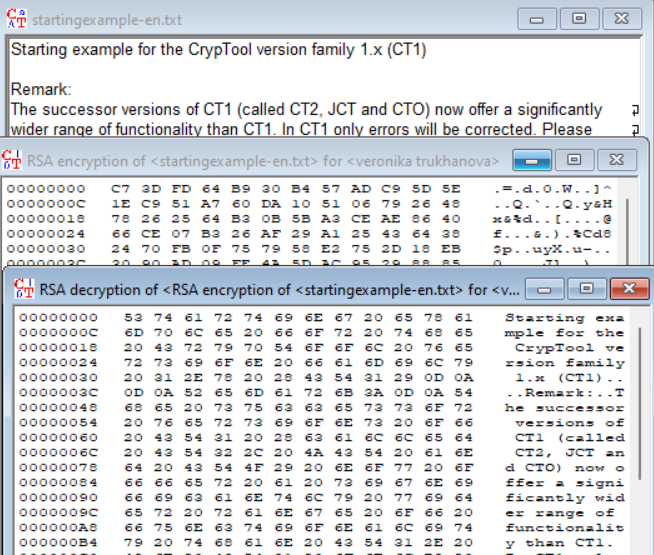


Рисунок 15 – Результаты шифровки и расшифровки исходного текста (2048)

* + 1. **Временные затраты на зашифровку и расшифровку**

Таблица 2. Временные затраты

|  |  |  |
| --- | --- | --- |
| Длина ключа | Время на зашифровку, сек | Время на расшифровку, сек |
| 512 | 0.000 | 0.006 |
| 768 | 0.000 | 0.011 |
| 1024 | 0.000 | 0.014 |
| 2048 | 0.002 | 0.060 |

**Атака «грубой силы» на RSA**

* + 1. **Задание**
* Запустить утилиту *Indiv. Procedures → RSA Cryptosystem → RSA Demonstration…*;
* Установите переключатель в режим «*Choose two prime…*»;
* Выберите параметры *p* и *q* так, чтобы *n* = *pq* > 256;
* Задайте открытый ключ *e*;
* Зашифруйте произвольное сообщение и передайте его вместе с *n* и *e* коллеге. В ответ получите аналогичные данные от коллеги;
* Запустите утилиту *Indiv. Procedures → RSA Cryptosystem → RSA Demonstration…* и установите переключатель в режим «*For data encryption…*»;
* Выполните факторизацию модуля *n* командой *Factorize…*;
* Используйте полученный результат для расшифровки сообщения полученного от коллеги. Проверьте корректность.

**7.4.2. Исходные данные для атаки**

От коллеги были получены следующие данные:

*n* = 299, *e* =101.

Шифротекст:

076 # 101 # 116 # 039 # 115 # 032 # 103 # 111 # 032 # 098 # 097 # 107 # 101 # 032 # 115 # 111 # 109 # 101 # 032 # 115 # 117 # 103 # 097 # 114 # 032 # 099 # 111 # 111 # 107 # 105 # 101 # 115 # 033

020 # 173 # 116 # 026 # 046 # 288 # 155 # 076 # 288 # 128 # 067 # 074 # 173 # 288 # 046 # 076 # 148 # 173 # 288 # 046 # 234 # 155 # 067 # 160 # 288 # 112 # 076 # 076 # 074 # 261 # 173 # 046 # 245

* + 1. **Результат факторизации**

Выполнена факторизация модуля *n*. Результат представлен на рисунке 16.

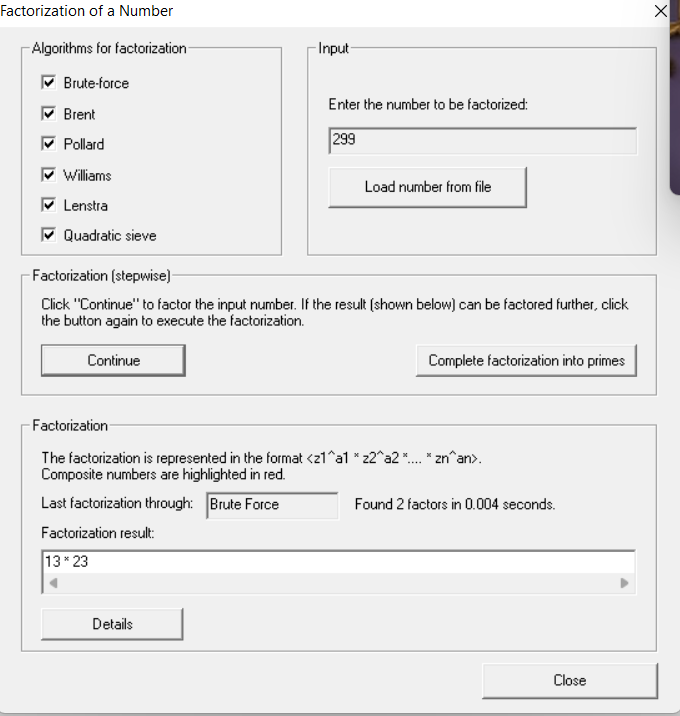


Рисунок 16 – Результат факторизации

* + 1. **Расшифрованное сообщение**

Используя полученный результат была проведена расшифровка сообщения. Результат представлен на рисунке 17.

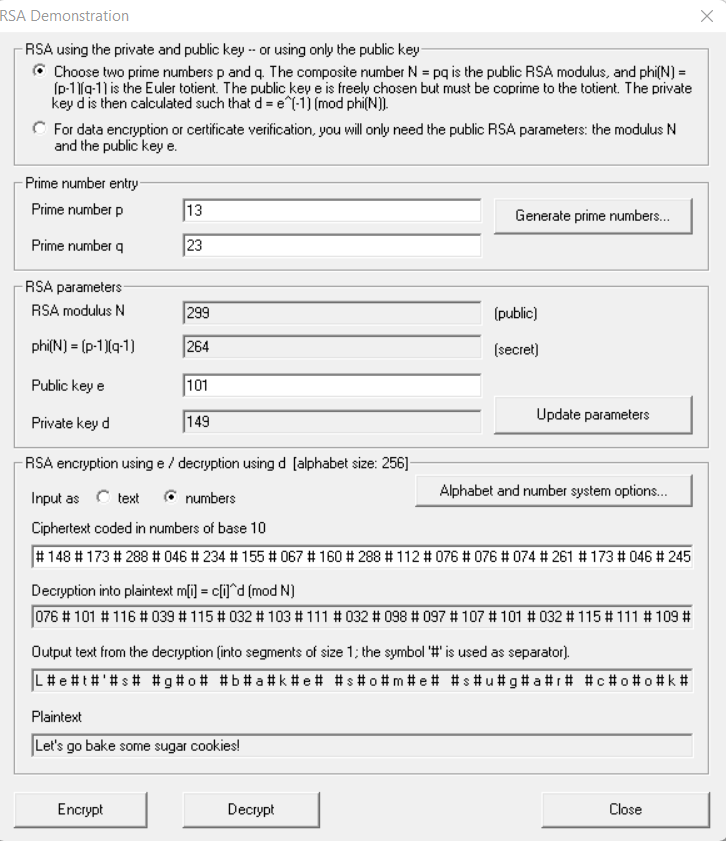


Рисунок 17 – Результат расшифровки

**Имитация атаки на гибридную криптосистему**

Модель гибридной криптосистемы, асимметричная составляющая которой  
использует асимметричный шифр (например, RSA), представлена на рисунке 18.

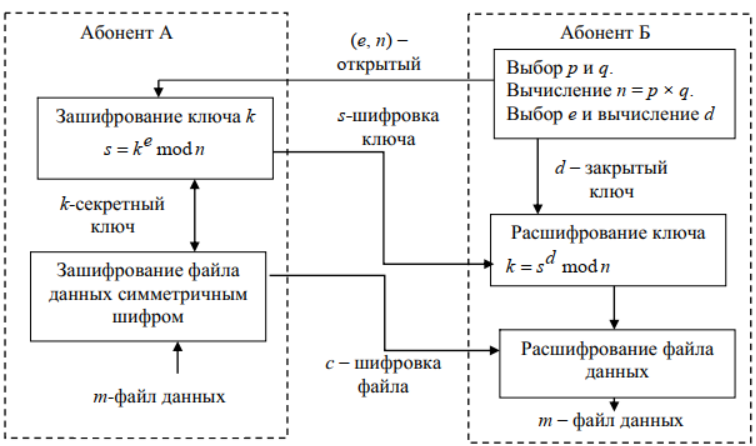
****

Рисунок 18 – Модель гибридной криптосистемы

Шифрование в рамках модели осуществляется следующим образом:

1. Сообщение шифруется симметричным секретным ключом.

2. Секретный ключ шифруется открытым ключом получателя.

3. Зашифрованное сообщение и ключ объединяются в цифровой конверт, который отправляется получателю.

4. Получатель сначала расшифровывает секретный ключ своим закрытым ключом, а затем расшифровывает этим секретным ключом шифровку сообщения.

Цель атак – определить симметричный секретный ключ, зашифрованный открытым ключом криптосистемы.

Условия атаки:

* Нарушитель может перехватывать сообщения, адресованные серверу;
* Нарушитель может модифицировать сообщения и направлять их серверу;
* Сервер не определяет, от кого был получен конверт;
* Нарушитель может классифицировать ответы сервера на ПРИНЯТО/ОТКЛОНЕНО, т.е. случаи успешной и неуспешной расшифровки (по распознаванию ключевого слова).
  + 1. **Задание**
* Подготовьте текст передаваемого сообщения на английском с вашим именем в конце;
* Запустите утилиту *Analysis → Asymmetric Encr… → Side-Channel attack on «Textbook RSA»…*;
* Настройте сервер, указав в качестве ключевого слова ваше имя, используемое в конце текста;
* Выполните последовательно все шаги протокола;
* Сохраните лог-файлы участников протокола для отчета.
  + 1. **Описание цели атаки, модель злоумышленника, схема атакуемого протокола гибридного шифрования**

Описание цели атаки:

Цель атаки – определить симметричный секретный ключ, зашифрованный открытым ключом криптосистемы, при условии, что:

* Нарушитель может перехватывать сообщения, адресованные серверу;
* Нарушитель может модифицировать сообщения и направлять их серверу;
* Нарушитель может классифицировать ответы сервера на ПРИНЯТО/ОТКЛОНЕНО.

На Рисунке 16 представлен исходный текст.

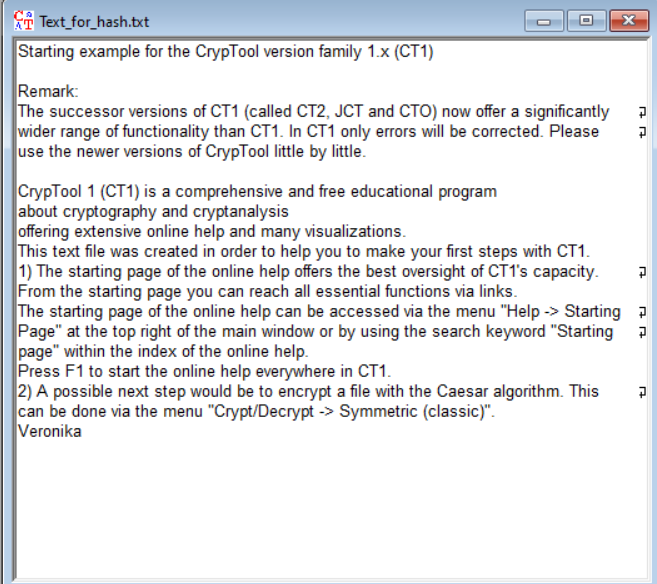


Рисунок 19 – Исходный текст

На Рисунках 20, 21 и 22 представлены лог-файлы участников протокола: Алисы, Боба и Труди соответственно.

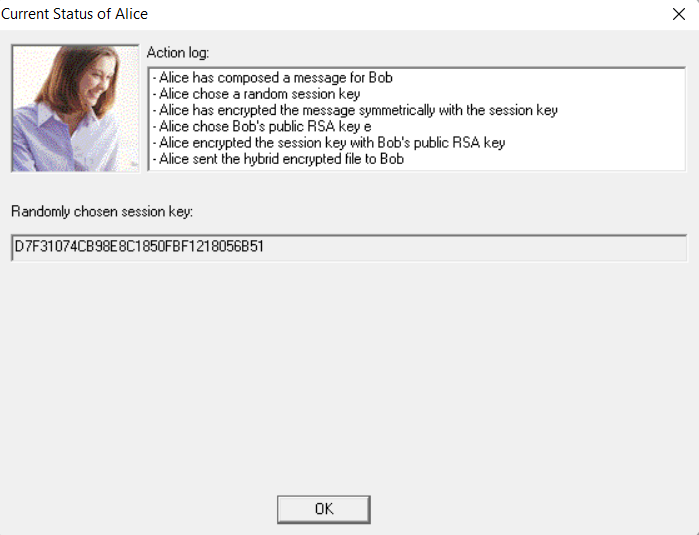


Рисунок 20 – Лог-файл Алисы

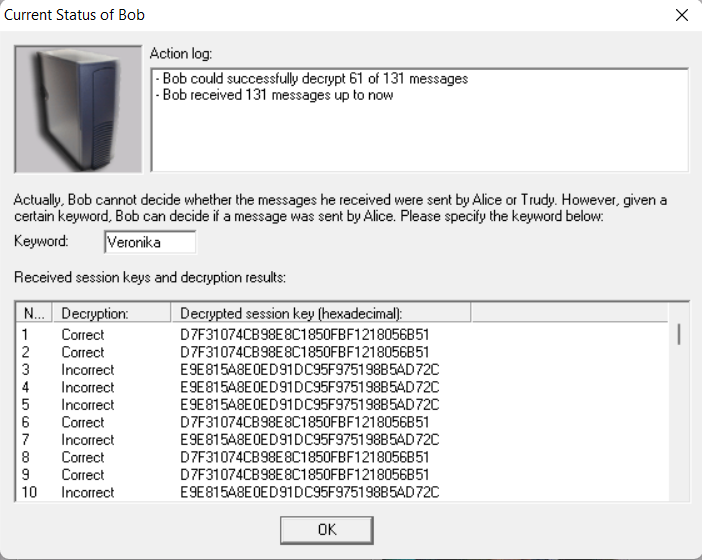


Рисунок 21 – Лог-файл Боба

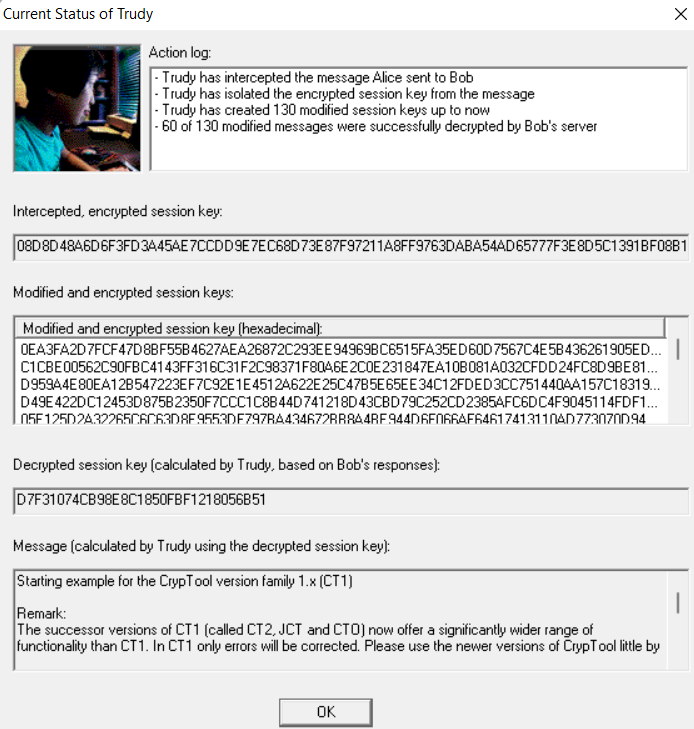


Рисунок 22 – Лог-файл Труди

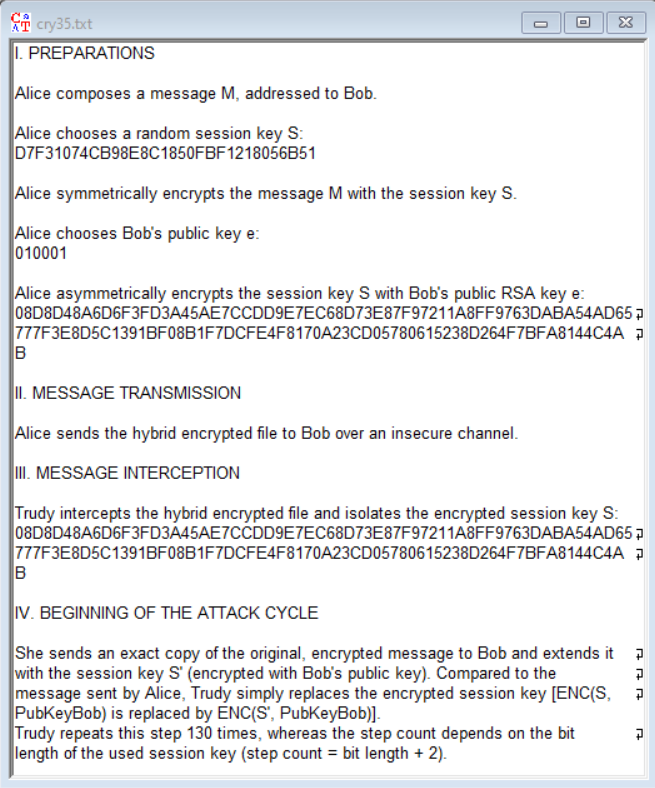


Рисунок 22 – Лог-файл атаки

**Заключение**

По итогу выполнения данной работы были сделаны следующие выводы:

1.При помощи протокола Диффи-Хеллмана стороны могут обмениваться данными по незащищенному каналу, так как в его основе используется математически-сложная задача дискретного логарифмирования. Также при помощи данного протокола можно создавать ключи для других шифров.

2.Алгоритм RSA – асимметричный блочный шифр (с длиной блока бит). Принимающая сторона генерирует закрытый и открытый ключи, открытый ключ отправляется отправляющей стороне и используется для зашифрования сообщения, после шифровка отправляется принимающей стороне и при помощи закрытого ключа происходит расшифрование. С увеличением длины ключа данное время на зашифровку и на расшифровку возрастает.

На алгоритм RSA можно применить атаку грубой силы если факторизовать часть открытого ключа – модуль n, особенно если n небольшое число.

3.На гибридную модель можно провести атаку «сторонним каналом», основанную на том, что злоумышленник перехватывает цифровой конверт с зашифрованным сообщением и зашифрованным секретнымБыла проведена атака на гибридную модель, основанная на том, что злоумышленник перехватывает цифровой конверт с зашифрованным сообщением и зашифрованным секретным ключом. Модифицируя полученные данные и анализируя ответы сервера, можно побитово восстановить целиком секретный ключ. ключом. Модифицируя полученные данные и анализируя ответы сервера, можно побитово восстановить секретный ключ.