**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра информационной безопасности**

отчет

**по лабораторной работе №7**

**по дисциплине «Криптография и защита информации»**

Тема: **Изучение асимметричных протоколов и шифров**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 8383 |  | Гречко В.Д. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2021

**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**

Основные параметры протокола

-большое простое число порядка 300 десятичных цифр (1024 бита)

– порождающий элемент циклической группы (генератор) порядка , для которого справедливо: являются различными целыми из .

– большие случайные числа такие, что

– односторонние функции с секретом

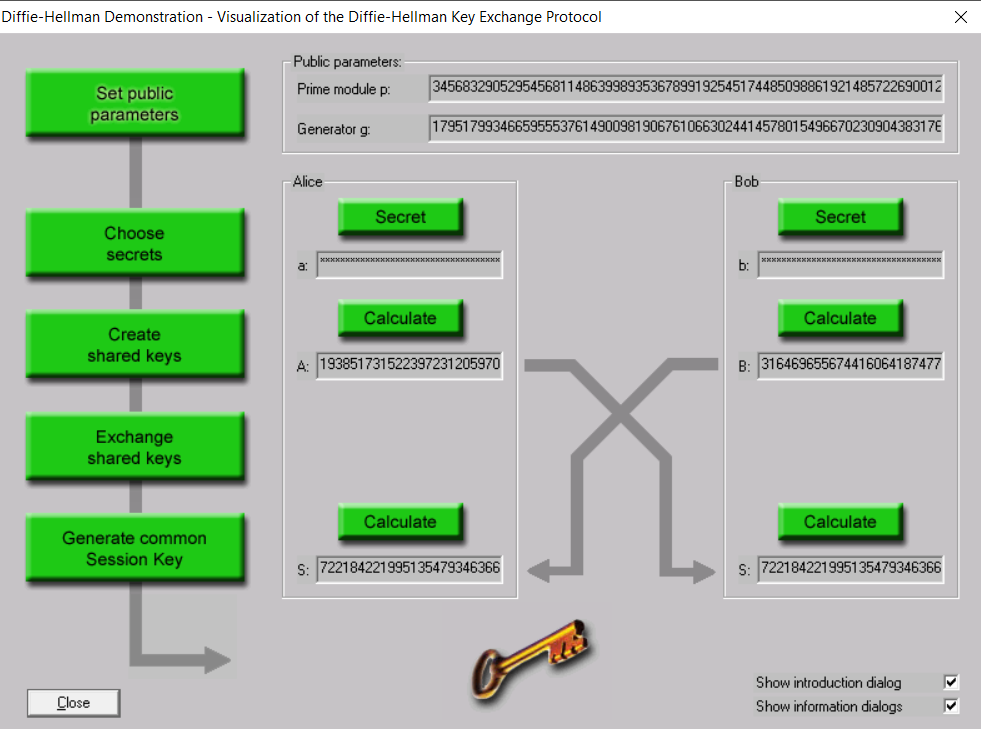
Задание.

1. Запустите утилиту *Indiv.Procedures->Protocols->Diffie-Hellman demonstration… и установите все опции информирования в ON.*

Выполним настройку протокола.

1. Выполните последовательно все шаги протокола.

Выполним последовательно все шаги протокола. Результат представлен на рис. 1



*Рисунок 1 – Схема работы протокола в CrypTool*

1. Сохраните лог-файл протокола для отчета (пиктограмма с изображением ключа).

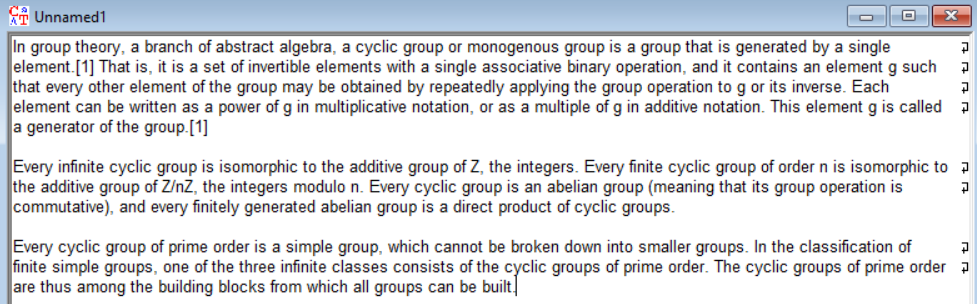
Лог-файл протокола представлен в Приложении А.

1. Используйте полученный общий ключ для зашифровки и расшифровки произвольного сообщения. Шифр выберите самостоятельно.

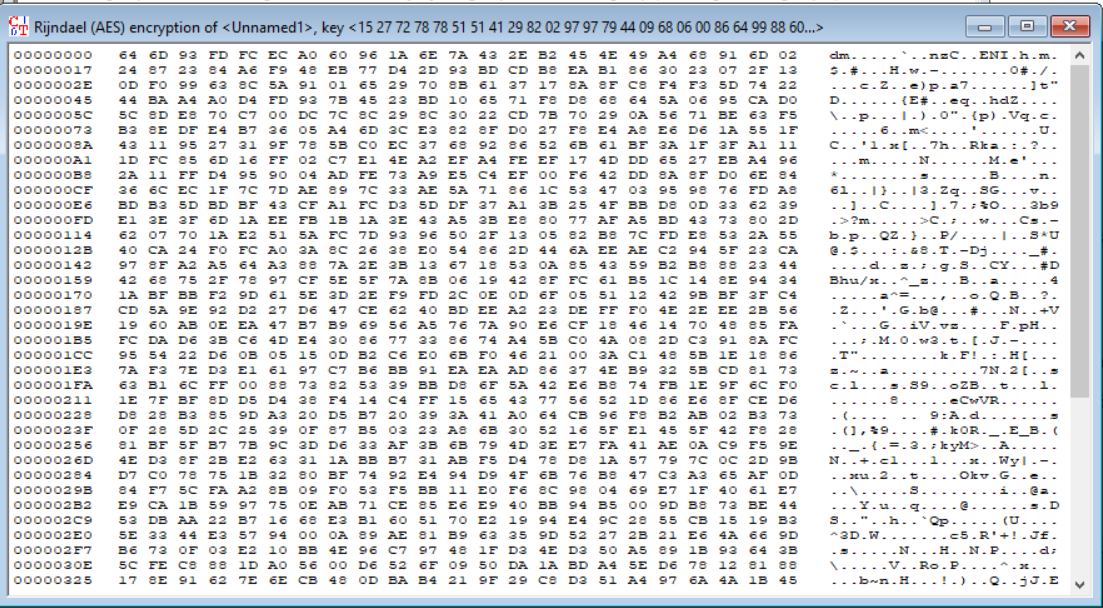
Так как в прошлых пунктах выполнялась генерация ключа 1024 бит, то для зашифровки AES выполним еще раз генерацию ключа теперь уже длиной 256 бит.

Сгенерированный ключ: 15277278785151412982029797794409680600866499886001229890757807015462438073060

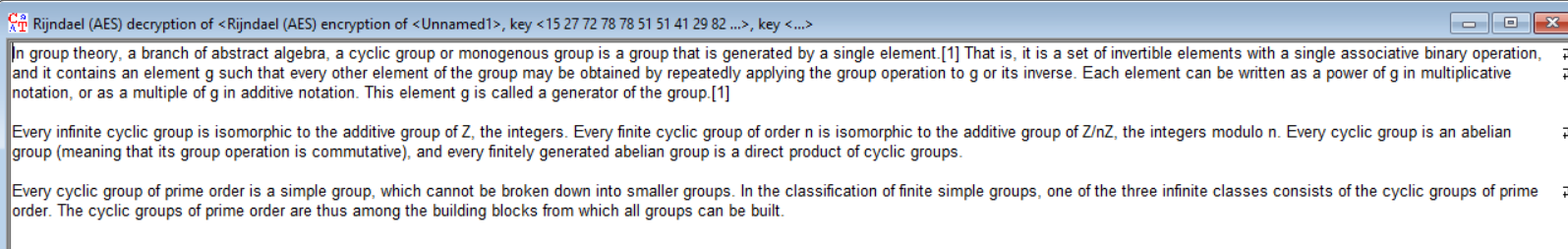
Исходный текст, зашифрованный и расшифрованный представлены на рис. 2-4 соответственно.



*Рисунок 2 – Исходный текст*



*Рисунок 3 – Зашифрованный текст*



*Рисунок 4 – Расшифрованный текст*

Сделаем сопоставление схемы протокола и параметров протокола. Результаты представлены в таблице 1.

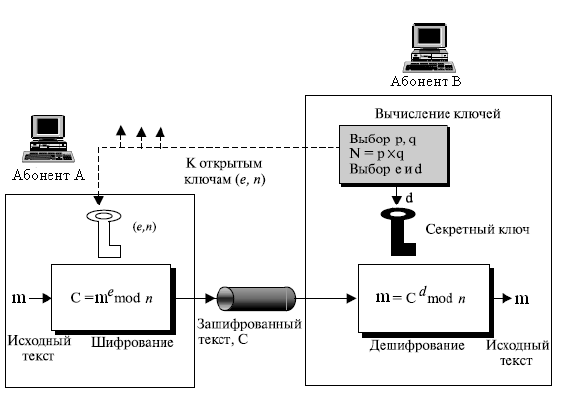
*Таблица 1 – Соответствия схемы протокола (CrypTool) и параметров протокола*

|  |  |  |
| --- | --- | --- |
| Параметры протокола | Параметры в демо Cryptool 1 | Назначение |
|  | Prime module p | Большое простое число, общедоступно |
|  | Generator g | Натуральное число, генератор порядка , общедоступен |
|  | a | Большое секретное число Алисы |
|  | b | Большое секретное число Боба |
|  |  | Открытый ключ на стороне Алисы |
|  |  | Открытый ключ на стороне Боба |
|  |  | Симметричный общий ключ |

**Шифр RSA.**

Обобщенная схема шифра.

Схема представлена на рис. 5.

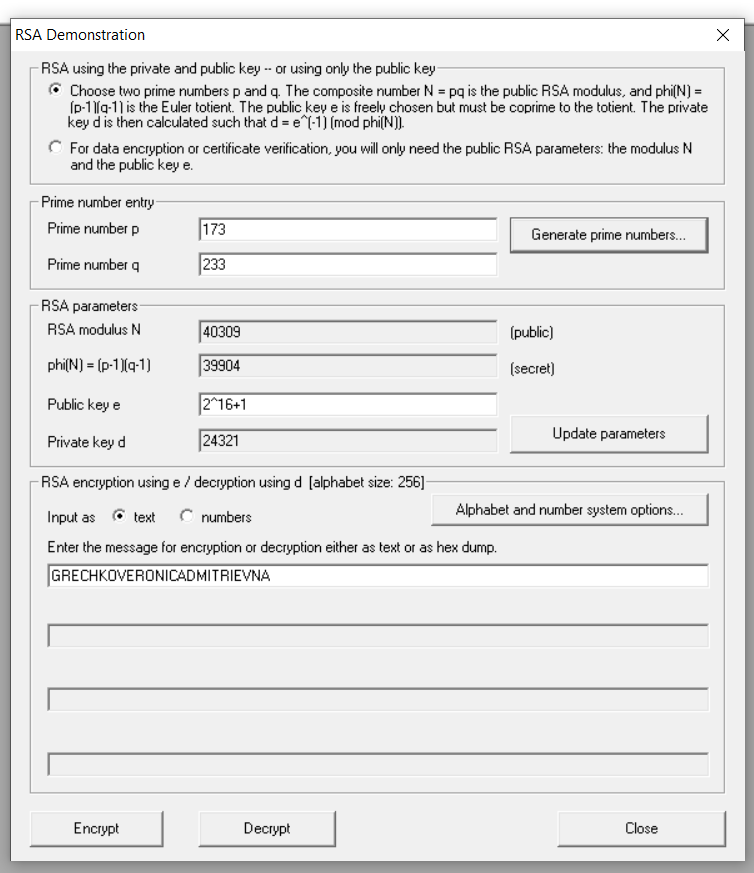


*Рисунок 5 – Обобщенная схема шифра*

Задание.

1. Запустите утилиту *Indiv.Procedures->RSACryptisystem->RSA Demonstration*
2. Задайте в качестве обрабатываемого сообщения свою Ф.И.О.

Параметры генерации представлены на рис. 6.



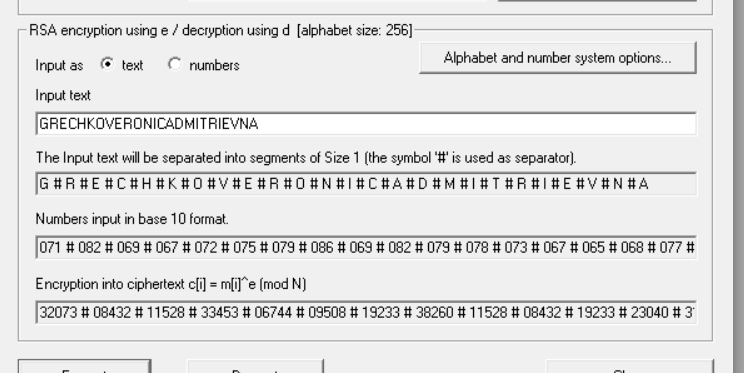
*Рисунок 6 – Параметры генерации ключей*

1. Сгенерируйте открытый и закрытый ключи.

Результат генерации открытых и закрытых ключей представлен также на рис. 6.

1. Зашифруйте сообщение. Сохраните скриншот результата.

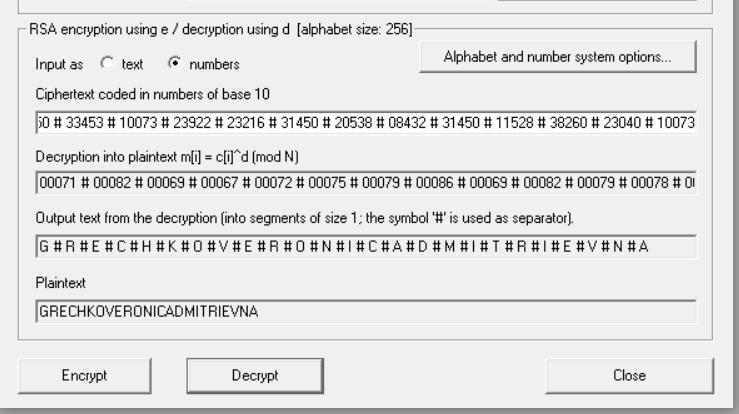
Зашифруем исходное сообщения (ФИО). Результат представлен на рис. 7



*Рисунок 7 – Зашифрованное сообщение*

1. Расшифруйте сообщение. Сохраните скриншот результата.

Выполним расшифровку полученного ранее сообщения. Результат представлен на рис. 8.



*Рисунок 8 – Расшифрованное сообщение*

1. Убедитесь, что расшифрование произошло корректно.

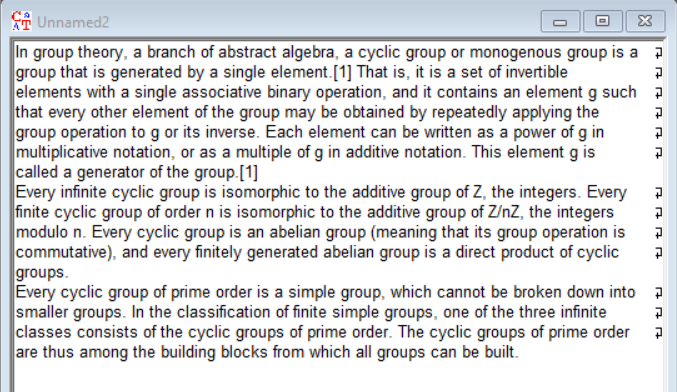
Результат, полученный в пункте 5 совпадает с исходным сообщением, что подтверждается скриншотами.

**Исследование шифра RSA.**

Задание.

1. Выбрать текст на английском языке (не менее 1000 знаков) и сохранить в файле формата \*.txt

Выбранный текст представлен на рис. 9. Размер текста – 1235 символа.



*Рисунок 9 – Исходный текст*

1. Сгенерировать пары асимметричных RSA-ключей утилитой Digital Signatures->PKI->Generate/Import Keys с различными длинами (4 варианта).

Сгенерируем 4 пары ключей с различными длинами. Сведем результаты генерации в таблицу 2. Была обнаружена ошибка в названии в CrypTool.

*Таблица 2 – Генерация пар открытого ключа*

|  |  |  |
| --- | --- | --- |
| Длина ключа | Модуль | Экспонента |
| 512 | 13367300733591739170970699148028520994844328510340757507741687396081280328924250011903649047420295724062164207959089910236065972115431258452448471416487591 | 65537 |
| 768 | 1524006658534239529162153371696508164821816989039193059278340761773978908281342248542740017315236036626480383270067159856955388922789546314930523115797473505518199964582157336628771801888074849750566396160532004808334647635934368177 | 65537 |
| 1024 | 17611884642741718422926702182650603997156346264942979062724619164587899885525668147779192037221400492986034995182288317792949290608065341261846432202878907264381353058998371099685562551645328151814800322440994595174817646830536502864613764 | 65537 |
| 2048 | 322246485957982220003747433574681674904833875297826614909442691846834251790640957499262624255974900829120162997959671154135978580304225133132124291150258196011108732568589231106166239713976555067638869806475583487528986213345315373665215520 | 65537 |

1. Зашифровать текст (примерно 1000 символов) различными открытыми ключами. Зафиксировать время зашифровки.

Зафиксированное время представим в таблице 3.

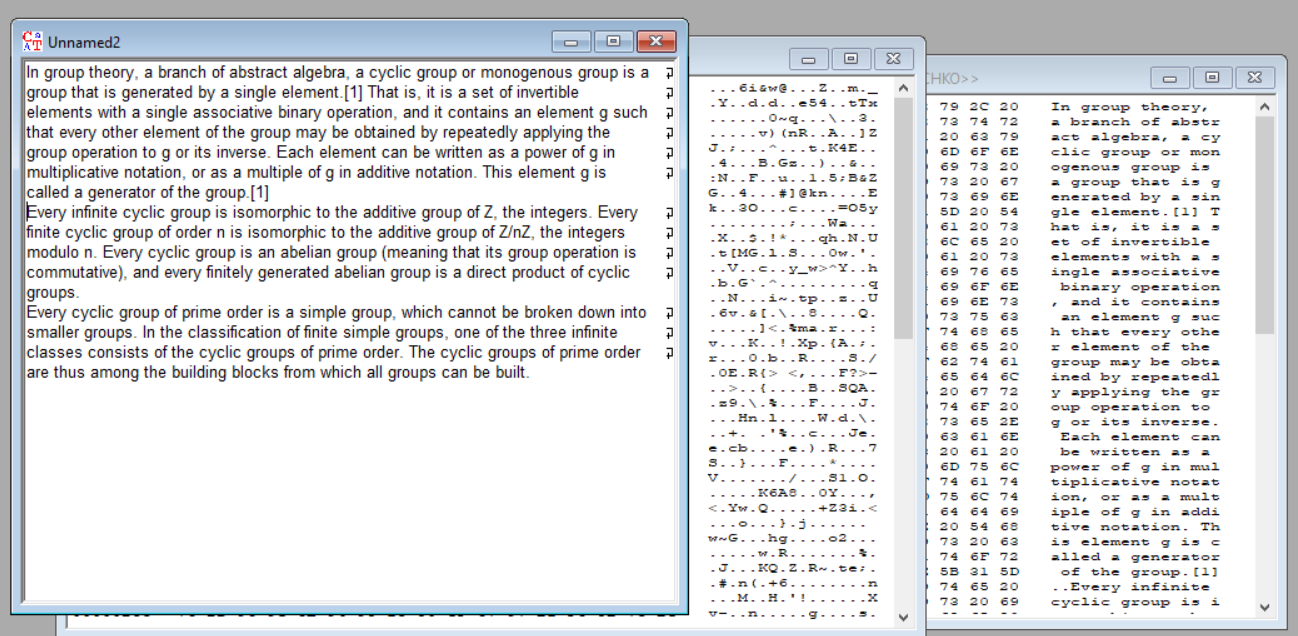
1. Расшифровать текст различными закрытыми ключами. Зафиксировать время зашифровки.

Зафиксированное время представим в таблице 3.

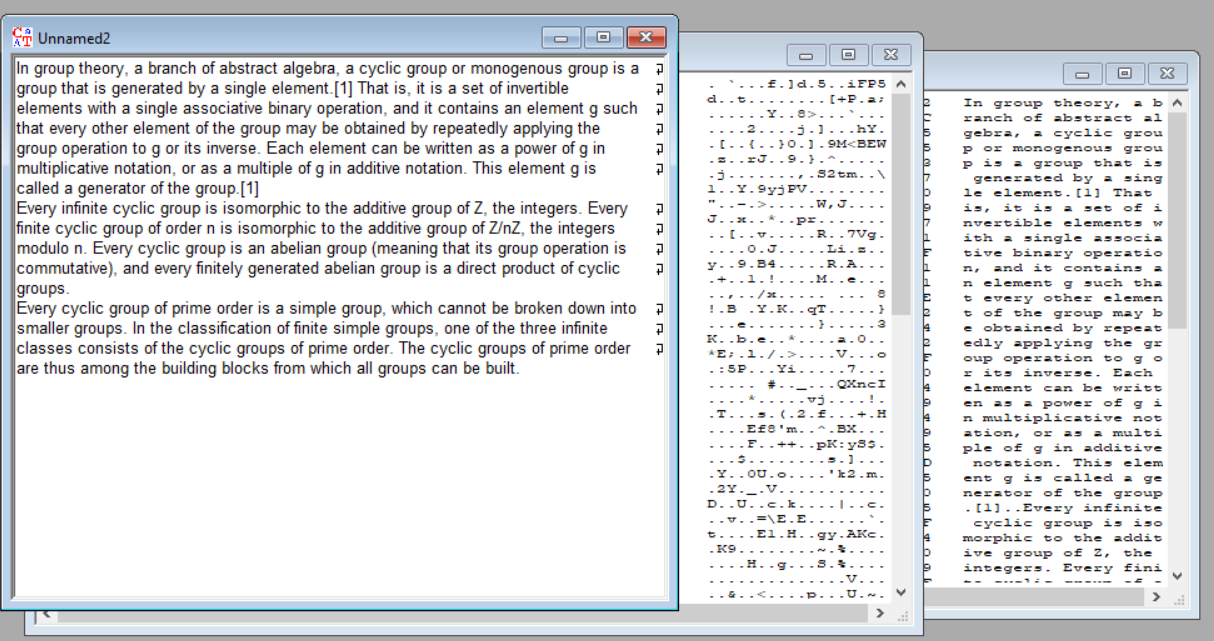
|  |  |  |
| --- | --- | --- |
| Длина ключа | Время зашифровки | Время расшифровки |
| 512 | 0.000 секунд | 0.006 секунд |
| 768 | 0.000 секунд | 0.010 секунд |
| 1024 | 0.000 секунд | 0.012 секунд |
| 2048 | 0.000 секунд | 0.048 секунд |

1. Проверить корректность расшифровки. Зафиксировать скриншоты результата.

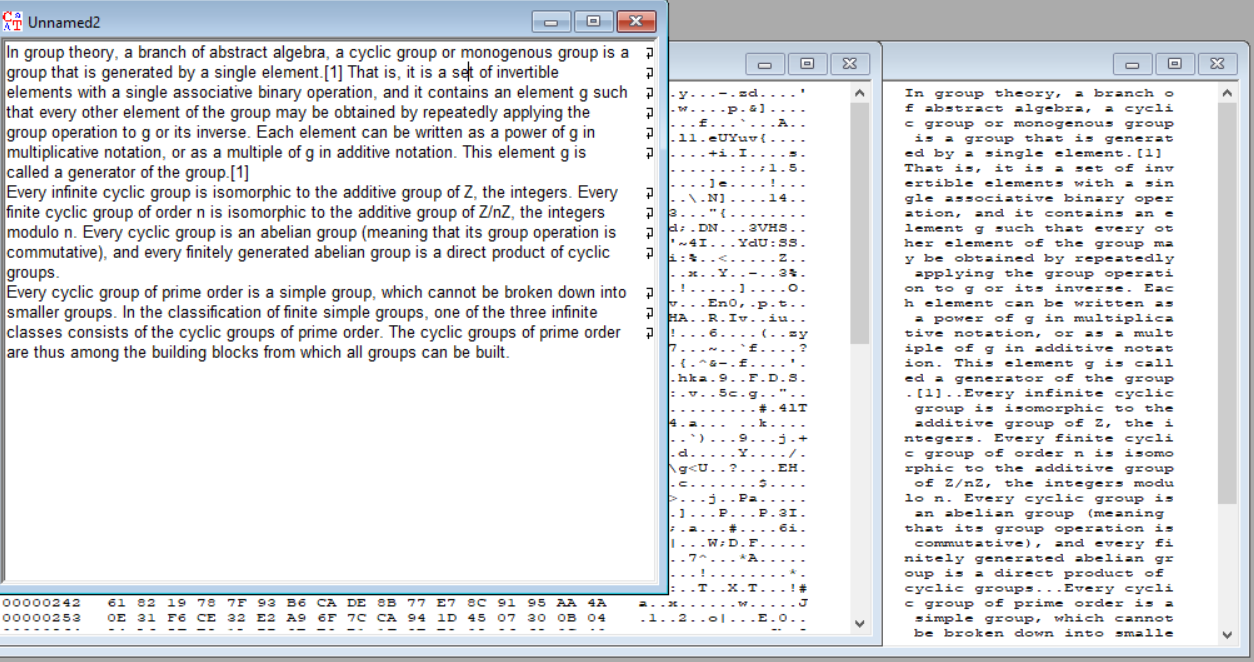
Результат шифрования и расшифрования исходного текста различными открытыми и закрытыми ключами представлен на рис. 10 - 13 соответственно.



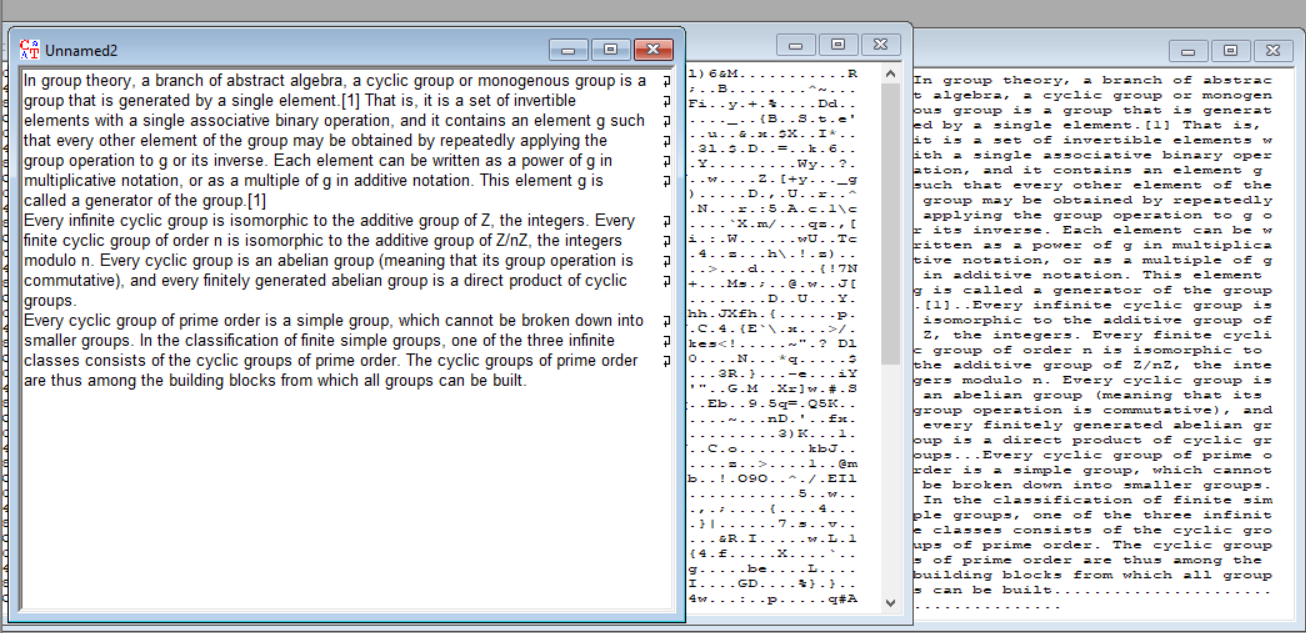
*Рисунок 10 – Результат шифровки и расшифровки RSA с длиной ключа 512*



*Рисунок 11 – Результат шифровки и расшифровки RSA с длиной ключа 768*



*Рисунок 12 – Результат шифровки и расшифровки RSA с длиной ключа 1024*



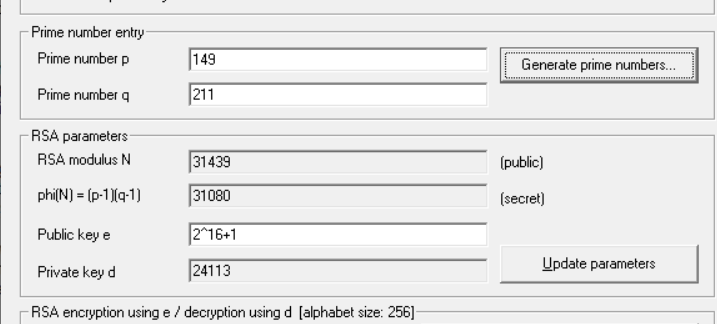
*Рисунок 13 – Результат шифровки и расшифровки RSA с длиной ключа 2048*

**Атака грубой силы на RSA.**

Задание.

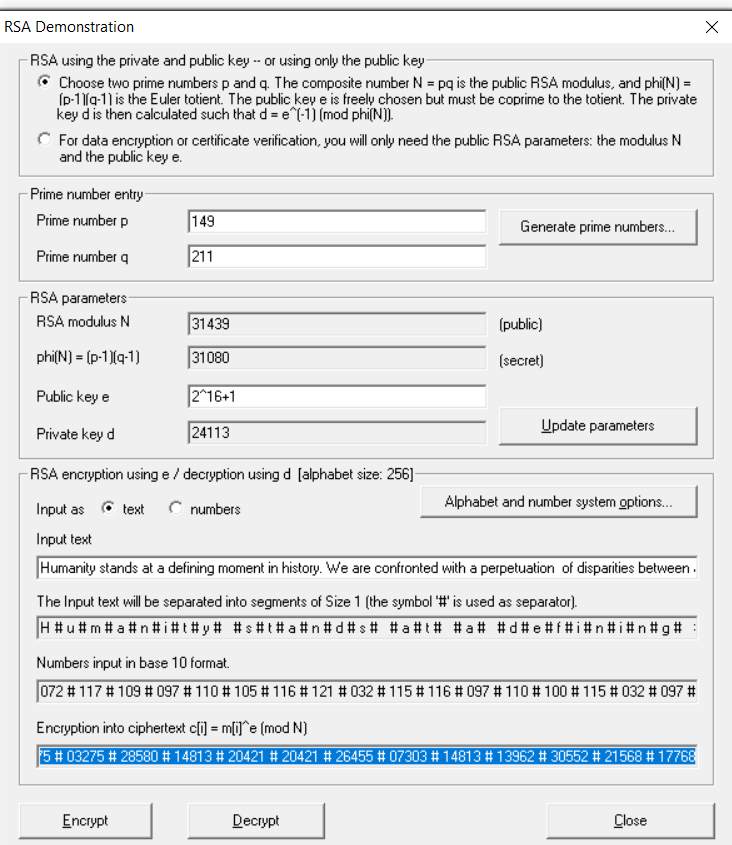
1. Запустите утилиту Indiv.Procedures->RSACryptosystem->RSA Demonstration
2. Установите переключатель в режим «Choose two prime…».
3. Выберите параметры и так, чтобы .
4. Задайте открытый ключ .

Полученные параметры представлены на рис. 14.



*Рисунок 14 – Генерация открытого и закрытого ключей*

1. Зашифруйте произвольное сообщение и передайте его вместе и коллеге. В ответ получите аналогичные данные от коллеги.

Результат шифрования сообщения из пункта 3 представлен на рис. 15. 

*Рисунок 15 – Зашифрованное сообщение*

Полученные данные от коллеги:

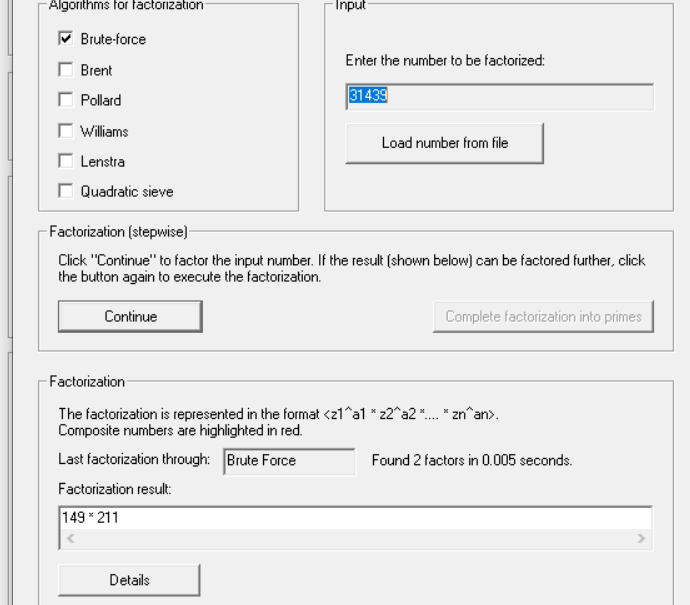
() = ()

Сообщение:

13718 # 03430 # 07357 # 30531 # 30552 # 13962 # 03747 # 05582 # 03275 # 22874 # 03747 # 30531 # 30552 # 18440 # 22874 # 03275 # 30531 # 03747 # 03275 # 30531 # 03275 # 18440 # 14813 # 18807 # 13962 # 30552 # 13962 # 30552 # 21568 # 03275 # 07357 # 08568 # 07357 # 14813 # 30552 # 03747 # 03275 # 13962 # 30552 # 03275 # 05431 # 13962 # 22874 # 03747 # 08568 # 13357 # 05582 # 17768 # 03275 # 22488 # 14813 # 03275 # 30531 # 13357 # 14813 # 03275 # 30299 # 08568 # 30552 # 18807 # 13357 # 08568 # 30552 # 03747 # 14813 # 18440 # 03275 # 28580 # 13962 # 03747 # 05431 # 03275 # 30531 # 03275 # 23717 # 14813 # 13357 # 23717 # 14813 # 03747 # 03430 # 30531 # 03747 # 13962 # 08568 # 30552 # 03275 # 03275 # 08568 # 18807 # 03275 # 18440 # 13962 # 22874 # 23717 # 30531 # 13357 # 13962 # 03747 # 13962 # 14813 # 22874 # 03275 # 07303 # 14813 # 03747 # 28580 # 14813 # 14813 # 30552 # 03275 # 30531 # 30552 # 18440 # 03275 # 28580 # 13962 # 03747 # 05431 # 13962 # 30552 # 03275 # 30552 # 30531 # 03747 # 13962 # 08568 # 30552 # 22874 # 21500 # 03275 # 30531 # 03275 # 28580 # 08568 # 13357 # 22874 # 14813 # 30552 # 13962 # 30552 # 21568 # 03275 # 08568 # 18807 # 03275 # 23717 # 08568 # 24089 # 14813 # 13357 # 03747 # 05582 # 21500 # 03275 # 05431 # 03430 # 30552 # 21568 # 14813 # 13357 # 21500 # 03275 # 13962 # 20421 # 20421 # 03275 # 05431 # 14813 # 30531 # 20421 # 03747 # 05431 # 03275 # 30531 # 30552 # 18440 # 03275 # 03275 # 13962 # 20421 # 20421 # 13962 # 03747 # 14813 # 13357 # 30531 # 30299 # 05582 # 21500 # 03275 # 30531 # 30552 # 18440 # 03275 # 03747 # 05431 # 14813 # 03275 # 30299 # 08568 # 30552 # 03747 # 13962 # 30552 # 03430 # 13962 # 30552 # 21568 # 03275 # 18440 # 14813 # 03747 # 14813 # 13357 # 13962 # 08568 # 13357 # 30531 # 03747 # 13962 # 08568 # 30552 # 03275 # 08568 # 18807 # 03275 # 03747 # 05431 # 14813 # 03275 # 14813 # 30299 # 08568 # 22874 # 05582 # 22874 # 03747 # 14813 # 07357 # 22874 # 03275 # 08568 # 30552 # 03275 # 28580 # 05431 # 13962 # 30299 # 05431 # 03275 # 28580 # 14813 # 03275 # 18440 # 14813 # 23717 # 14813 # 30552 # 18440 # 03275 # 18807 # 08568 # 13357 # 03275 # 08568 # 03430 # 13357 # 03275 # 03275 # 28580 # 14813 # 20421 # 20421 # 26455 # 07303 # 14813 # 13962 # 30552 # 21568 # 17768

1. Запустите утилиту Indiv.Procedures->RSACryptosystem->RSADemonstration и установите переключатель в режим «For data encryption…»
2. Выполните факторизацию модуля n командой Factorize…

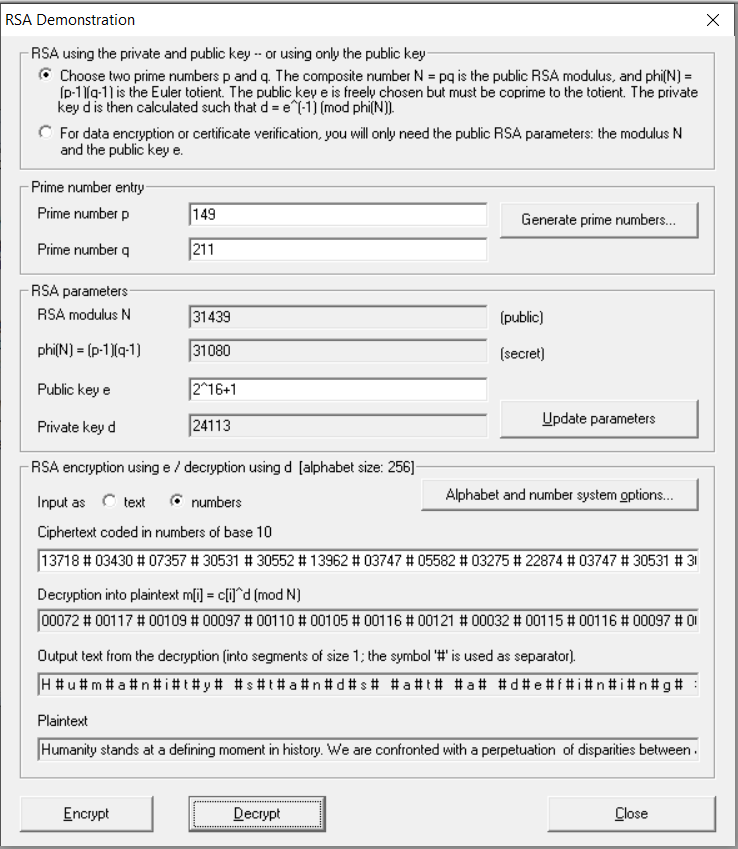
Выполним факторизацию модуля . Результат представлен на рис. 16



*Рисунок 16 – Факторизация модуля*

1. Используйте полученный результат для расшифровки сообщения полученного от коллеги. Проверьте корректность.

Выполним расшифровку полученного сообщения. Результат представлен на рис. 17



*Рисунок 17 – Расшифрованное сообщение*

**Имитация атаки на гибридную криптосистему.**

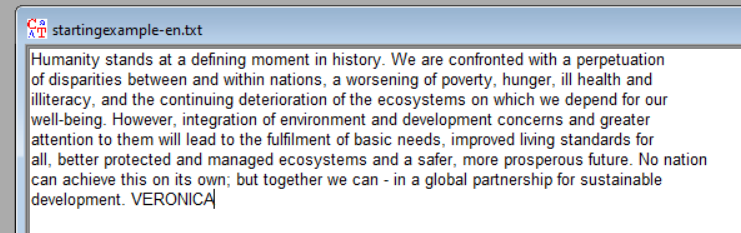
Цель атаки.

Определить симметричный секретный ключ, зашифрованный открытым ключом криптосистемы. Атака на гибридную модель основана на том, что злоумышленник перехватывает цифровой конверт, содержащий зашифрованное сообщение и зашифрованный секретный ключ. Затем, модифицируя полученные данные, побитово восстанавливает зашифрованный секретный ключ, анализируя положительные и отрицательные ответы сервера.

Задание.

1. Подготовьте текст передаваемого сообщения на английском с вашим именем в конце.

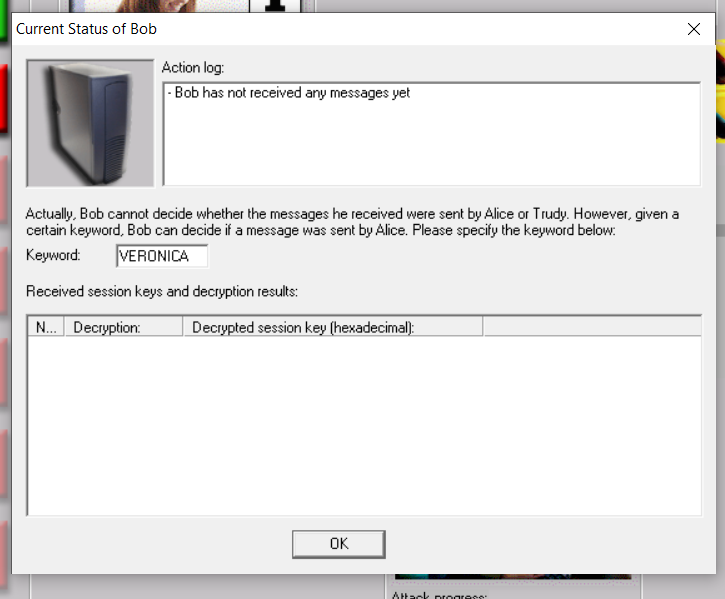
Исходный текст представлен на рис. 18.



*Рисунок 18 – Исходный текст*

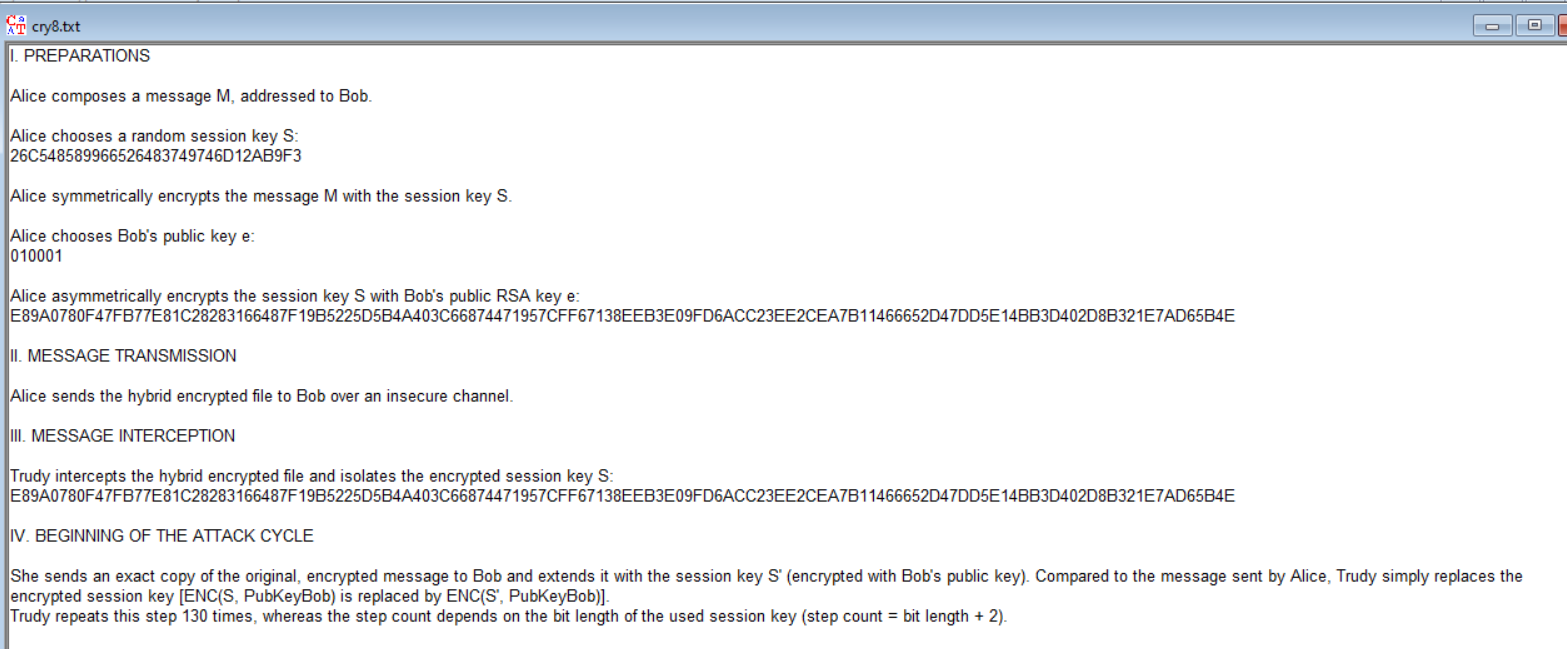
1. Запустите утилиту *Analysis->Asymmetric Encr…->Side-Channel attack on «Textbook RSA»…*
2. Настройте сервер, указав в качестве ключевого слова ваше имя, используемое в конце текста.

Настроим сервер, указав в качестве ключевого слова VERONICA



1. Выполните последовательно все шаги протокола.
2. Сохраните лог-файлы участников протокола для отчета.

Лог-файлы участников протокола:



**Выводы.**

1. Был изучен протокол Диффи-Хеллмана. Цель протокола – обеспечить двум пользователям возможность получения симметричного секретного ключа путем обмена данными по незащищенному каналу связи. Основными параметрами протокола являются общедоступная пара чисел – большое простое число (более 300 десятичных цифр) и генератор (первообразный корень по модулю ), а также числа , известные только отправителям. Сгенерированный секретный ключ использовался для шифрования текста шифром AES. Результат расшифровки совпал с исходным текстом.
2. Был изучен шифр RSA – ассиметричный блочный шифр. Основными параметрами шифра являются два больших числа , которые уничтожаются после вычисления пары закрытого и открытого ключей. Один из абонентов генерирует два ключа, передает открытый ключ () своему собеседнику, который используется при зашифровке сообщений, а сам использует закрытый ключ для расшифровки.
3. Была исследована зависимость времени шифрования и расшифрования от длины ключа. Выполнение обеих операции занимает очень мало времени. Время зашифровки во всех случаях составило 0.000 секунд, а вот время расшифровки увеличивалось с ростом длины ключа. Так, для 2048 битного ключа время составило 0.048 секунд, а для 512 битного ключа – 0.006.
4. Была изучена атака грубой силы на шифр RSA. В ходе атаки был успешно факторизован модуль, что сделало атаку успешной. Был сделан вывод, что генерирование и в диапазоне от до (установленные по умолчанию в CrypTool) приводит к успешной атаке грубой силой путем факторизации модуля. Использование диапазона от до (как рекомендовано) делает задачу практически нерешаемой (CrypTool сразу же при выборе атаки грубой силой выдает ошибку, что для получения разложения должно быть меньше 10 000)
5. Была проведена атака по побочным каналам на гибридную криптосистему. Цель атаки – определить симметричный секретный ключ, зашифрованный открытым ключом криптосистемы. Условия атаки: нарушитель может перехватывать и модифицировать сообщения, передаваемые серверу, сервер не может определить, от кого был получен конверт, сервер возвращает принято/отклонено по распознаванию ключевого слова. Способ противодействия – ограничения числа отправки запросов к серверу в течении некоторого времени и проверка на целостность сообщения.

ПРИЛОЖЕНИЕ А

Лог-файл работы протокола:

At first, Alice and Bob agreed on the public parameters. So they chose a prime p and a generator g:

p: 345683290529545681148639989353678991925451744850988619214857226900123490305071792257508097709004571629862774884443022009285498106293793464502161720760458070166903501296980351429705044308528594715156038098189317432473113412699709781666265196395673147446349210328405355645277813680552256880610870060154578023707

g: 179517993466595553761490098190676106630244145780154966702309043831763890116431022511200138122535591857133785307673140168904062063975744202310654358400774973112750315257522754137099382972595106986812163084603336234006005033897276218497539026071646269001952764011190919308947003543645149511922698305133292111227

Alice chose her secret number 'a' while Bob chose his secret number 'b':

a: 152472432552270770841262891520268647699583422811063568378242747073816495177125246847088265004018595666871337373458029977962379559446611793315607948927923562394225521601209476259763860882820434045913853719437715970244287760023544666033386629922348866330076820164991023441250584347812414212933326957274133597601

b: 183142200431538148626779887024126596499629953232812558422010364536590215563248419053228606553467492939484158200840390635559557139694715523999746986673653963687154308640446246028612415747391715353415844830248350038642487502391059929201500754827048153242772613044492876162239199530086950878621122491563251269429

If the chosen secret values a and b are greater or equal the prime module p, then they need to be reduced modulo p. The actual values are given below:

a (reduced mod p):

152472432552270770841262891520268647699583422811063568378242747073816495177125246847088265004018595666871337373458029977962379559446611793315607948927923562394225521601209476259763860882820434045913853719437715970244287760023544666033386629922348866330076820164991023441250584347812414212933326957274133597601

b (reduced mod p):

183142200431538148626779887024126596499629953232812558422010364536590215563248419053228606553467492939484158200840390635559557139694715523999746986673653963687154308640446246028612415747391715353415844830248350038642487502391059929201500754827048153242772613044492876162239199530086950878621122491563251269429

On the basis of the previously chosen secret numbers, Alice and Bob created their respective shared keys. Alice computed her shared key A, while Bob computed his shared key B:

A: 193851731522397231205970037387983774759477098653838355766627305497926467761506104404943038711720239615579258177710414799889507708286569082406674729922209799634489743232342186289802966281004482672627989209478781791003236407669713490226150632910394885913251053393000127730030529376363690848880677284832574274430

B: 316469655674416064187477460940460779357734994411111495369922895874711838446250670472072979609643355722023935064202568854885502032258296270787919391816718456011473515216766572154386938817061122583402116361252723160974422754408985015146064187418919704752490168082428651039974278443273143124109831985644434004765

In order to calculate their secret and common Session Key, Alice and Bob exchanged their shared keys: Alice sent her shared key A to Bob and Bob sent his shared key B to Alice.

Alice and Bob were able to calculate the secret and common Session Key now. Alice computed the Session Key SA, Bob computed the Session Key SB:

SA: 7221842219951354793463663620407227097360767855355195428926298678898666426390556246977847871297812883390354019738633458654873242714711301701838668781420704531143747573885769154819492026431478580585602333933342927866416608239086190867266726947330250710848933344418485014248768932131522177658859914890885832016

SB: 7221842219951354793463663620407227097360767855355195428926298678898666426390556246977847871297812883390354019738633458654873242714711301701838668781420704531143747573885769154819492026431478580585602333933342927866416608239086190867266726947330250710848933344418485014248768932131522177658859914890885832016

Theoretically it is now possible for Alice and Bob to use their Session Keys to encrypt documents they would like to exchange covertly.