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

Студент гр. 8383 _____ Киреев К.А.

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

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

g – порождающий элемент циклической группы (генератор) порядка p, для которого справедливо: $g \bmod p, g^2 \bmod p, g^3 \bmod p \ \ldots \ g^{p-1} \bmod p$ являются различными целыми из $[1, p-1]$.

x, y – большие случайные числа такие, что $0 < x < p - 1, 0 < y < p - 1$

$R_1 = g^x \bmod p, R_2 = g^y \bmod p$ – односторонние функции с секретом

Задание

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

Выполним настройку протокола.

2. Выполните последовательно все шаги протокола.

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

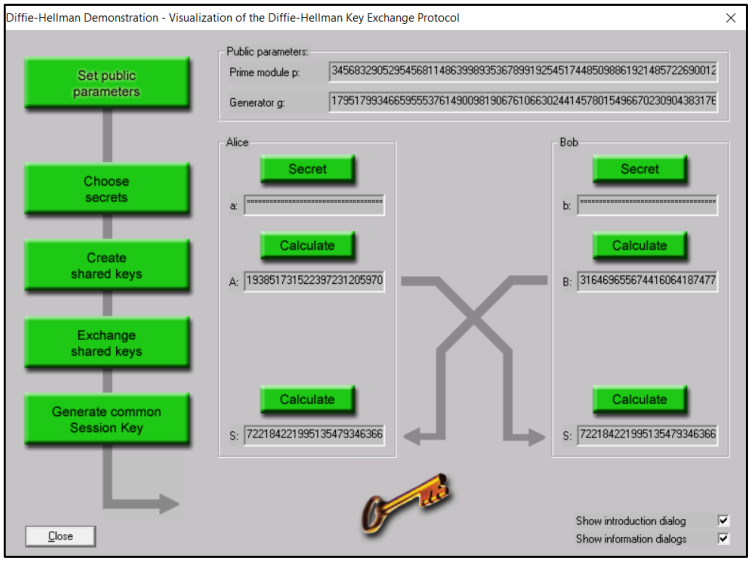

Рисунок 1 – Схема работы протокола в CrypTool

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

Лог-файл протокола представлен в Приложении А.

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

Сгенерированный ключ (256 бит):

1241715130232714003638741350259428566829607806607770803679001654400776323031 69

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

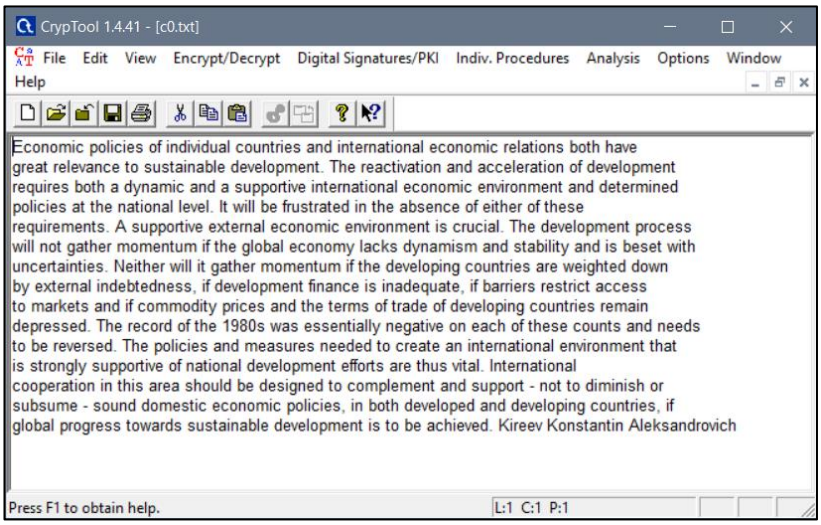

Рисунок 2 – Исходный текст

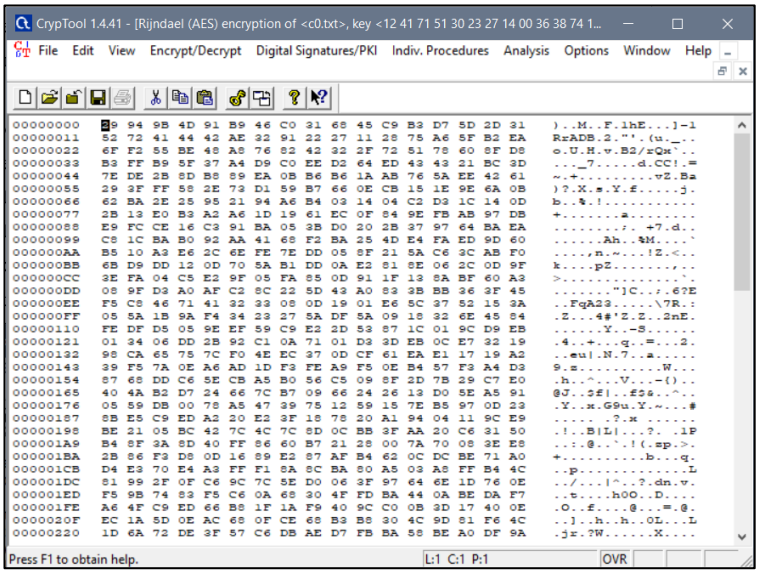

Рисунок 3 – Зашифрованный текст

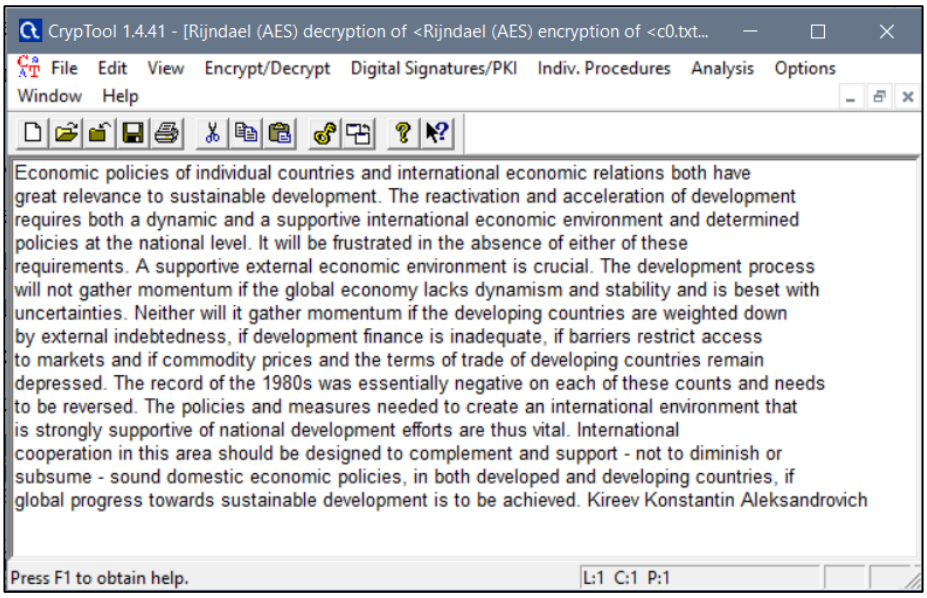

Рисунок 4 – Расшифрованный текст

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
p	Prime module p	Большое простое число, общедоступно
g	Generator g	Натуральное число, генератор порядка p, общедоступен
x	a	Большое секретное число Алисы
y	b	Большое секретное число Боба
$R_1 = g^x mod\ p$	$A = g^a mod\ p$	Открытый ключ на стороне Алисы
$R_2 = g^y mod\ p$	$B = g^b mod\ p$	Открытый ключ на стороне Боба
$K = R_2^x\ mod\ p = R_1^y mod\ p$	$S = A^b mod\ p = B^a mod\ p$	Симметричный общий ключ

Шифр RSA

Обобщенная схема шифра

Схема представлена на рис. 5.

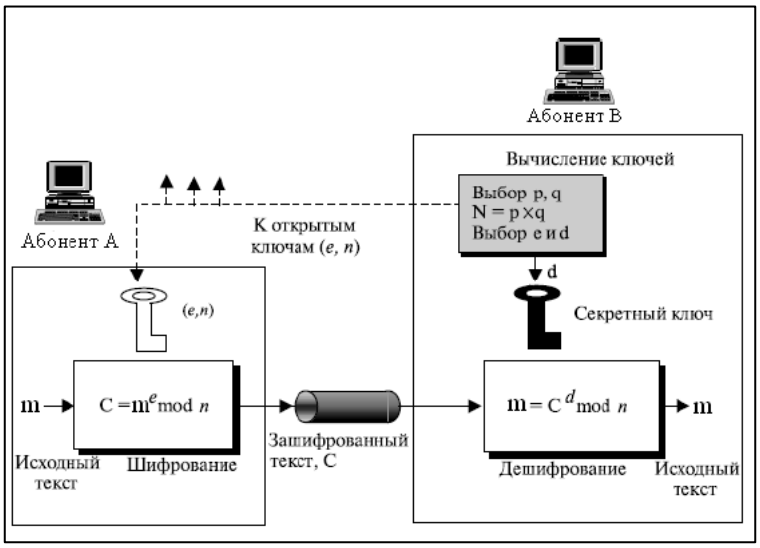

Рисунок 5 – Обобщенная схема шифра

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.

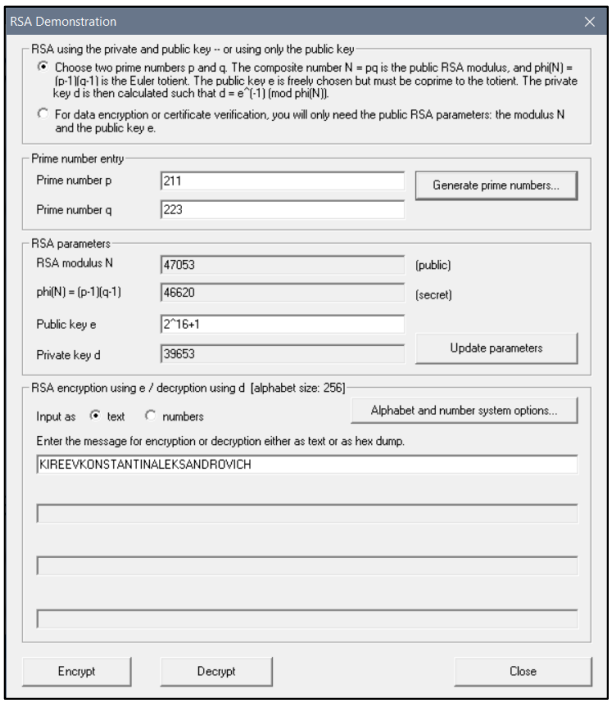

Рисунок 6 – Параметры генерации ключей

3. Сгенерируйте открытый и закрытый ключи.

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

4. Зашифруйте сообщение. Сохраните скриншот результата.

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

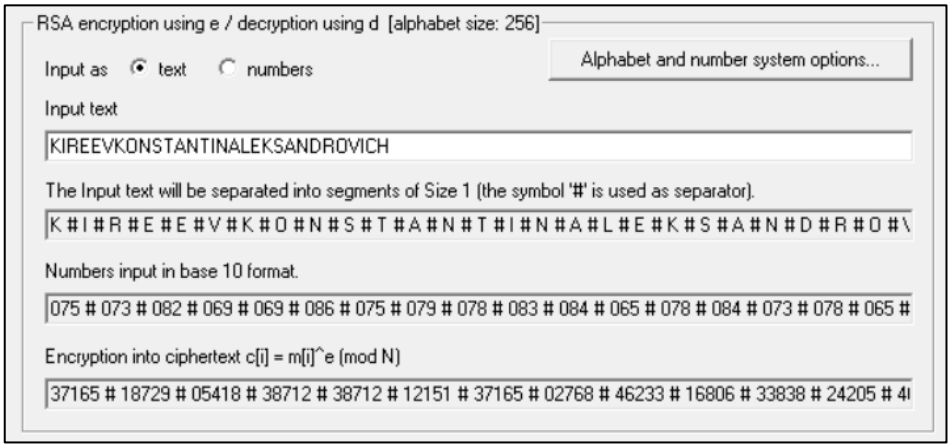

Рисунок 7 – Зашифрованное сообщение

5. Расшифруйте сообщение. Сохраните скриншот результата.

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

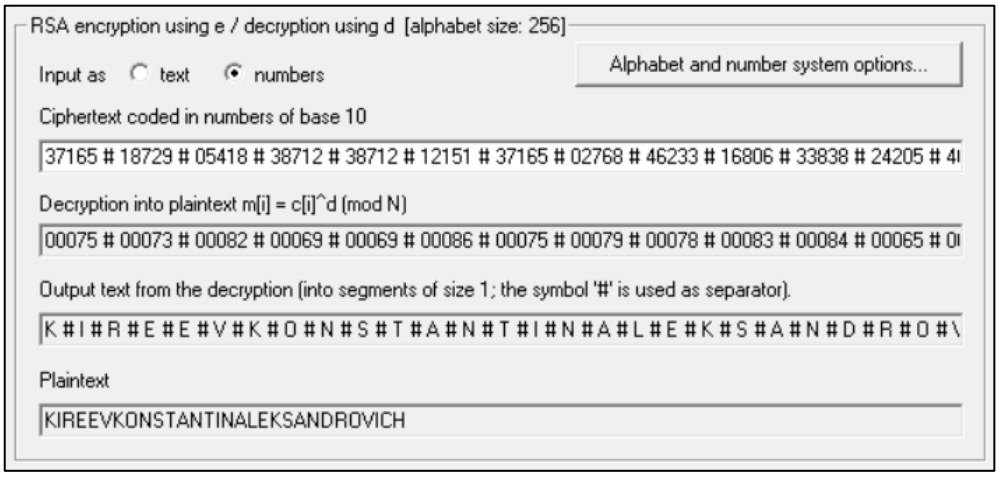

Рисунок 8 – Расшифрованное сообщение

6. 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 – 1370 символов.

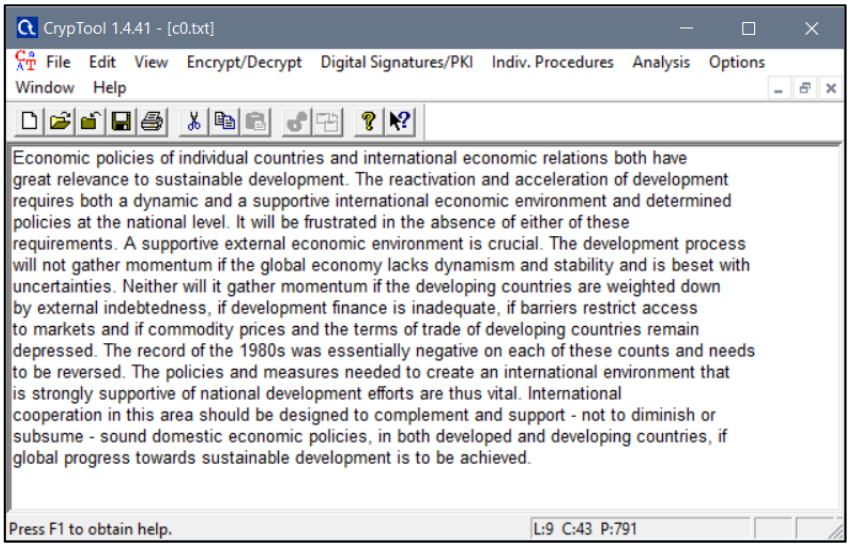

Рисунок 9 – Исходный текст

2. 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.

Таблица 2 – Генерация пар открытого ключа

Длина ключа	Экспонента	Модуль
512	133198467293462584398013991771310373191061268665400438080475397996 734864242124082307464623576794100603587949109819802126051944852541 86140979003524941663739	65537
768	152527828329761931191006349981856758461469475393449723521100617921 171412930999745996738627622594557135520600347829668698151692350821 629322346996908066949566926581173878307184661372332473004979300542 30587770636627589351995578147106 73	65537

1024	17775922682730262404886021617191782314069775786785773859161295919692606717404845380636509842228606216350733255147561412478272154092615450114511688952326126365098976782841274756391936483164299831866125261668761396060393413511981952519518466436753214036034420315745955717480816171306818379362644105300870962459	65537
2048	32310937105870841626665659564845275417433334819390219317199690344270035023915639759570216917208653861654252868919103585925568847421505059020207963418493646177987826997602756328854928781033613742497500630039822955315849809279642886790048751591634128362320946903805206008205132940371110871681451666381294108985331228424828848530790309541544888298107086153281122476314552301316468776251842553248840059885505818247580740670902775338246120993659486259068035634776964944148157110749067624559056994652000591906028540916946720244344292568520272548222940579643654557628693646677801232380065799180320338226731451906438759096813	65537

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

Зафиксированное время представим в таблице 3.

4. Расшифровать текст различными закрытыми ключами. Зафиксировать время расшифровки. Зафиксированное время представим в таблице 3.

Таблица 3 – Генерация пар открытого ключа

Длина ключа	***Время зашифровки (с)***	***Время расшифровки (с)***
512	0.000	0.004
768	0.000	0.008
1024	0.000	0.012
2048	0.000	0.049

5. Проверить корректность расшифровки. Зафиксировать скриншоты результата.

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

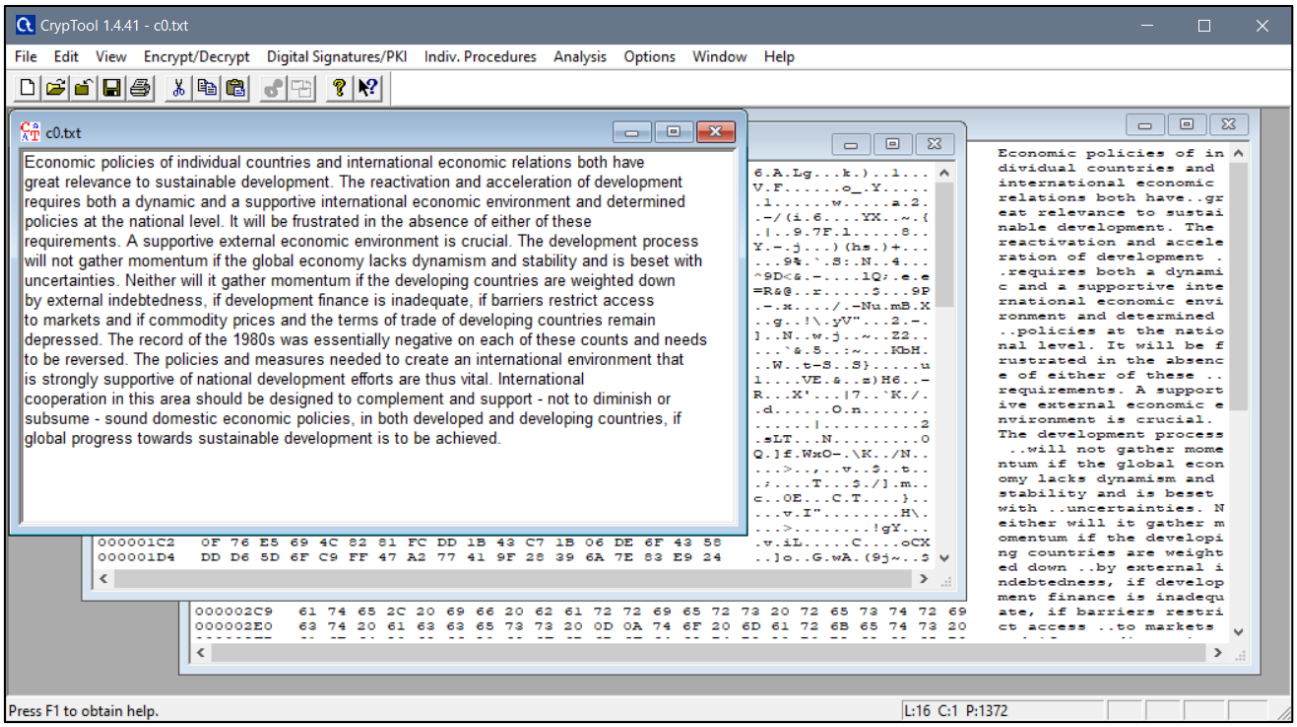

Рисунок 10 – Результат шифровки и расшифровки RSA с длиной ключа 512

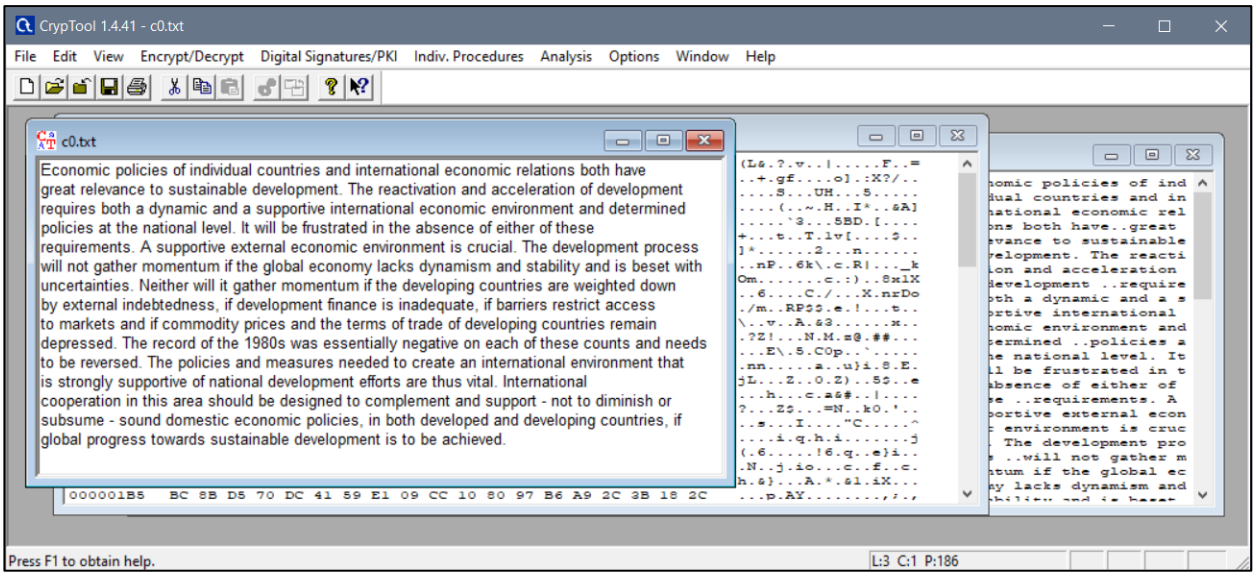

Рисунок 11 – Результат шифровки и расшифровки RSA с длиной ключа 768

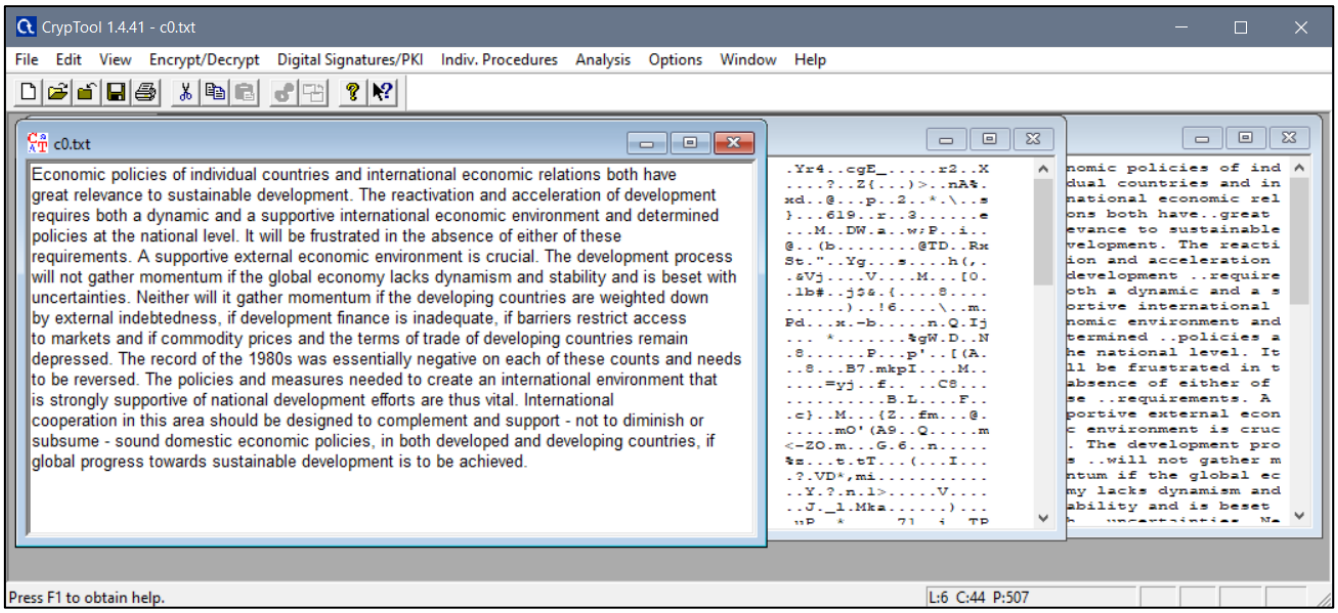

Рисунок 12 – Результат шифровки и расшифровки RSA с длиной ключа 1024

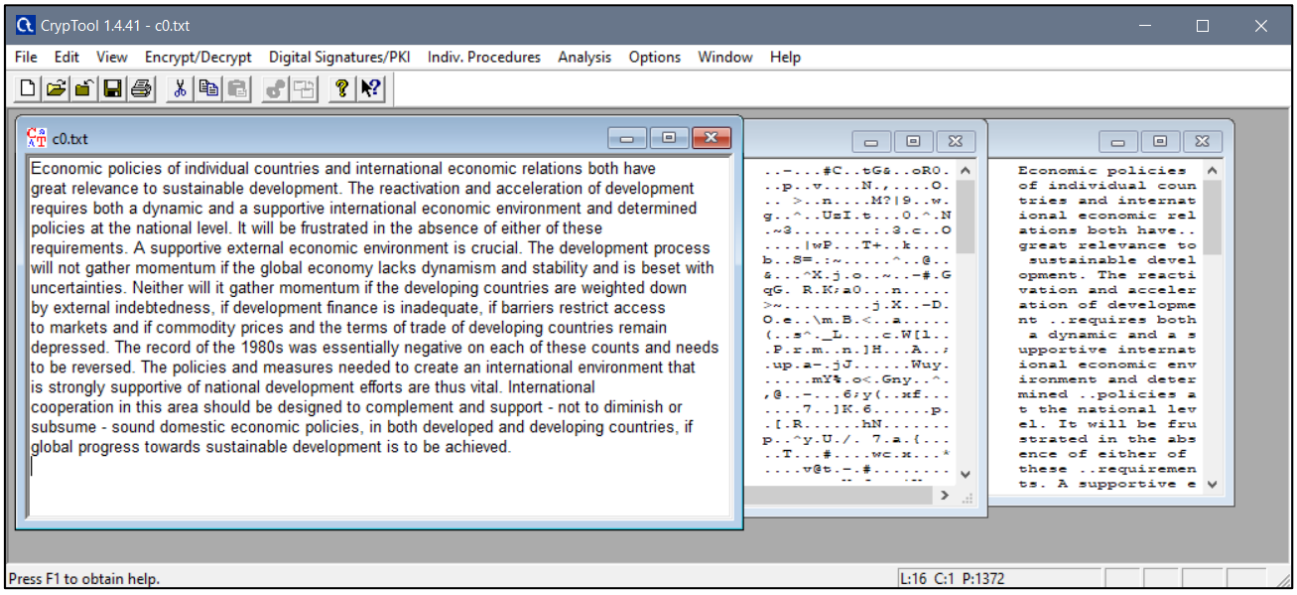

Рисунок 13 – Результат шифровки и расшифровки RSA с длиной ключа 2048

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 p и q так, чтобы $n = pq > 256$.
4. Задайте открытый ключ e.

Полученные параметры представлены на рис. 14.

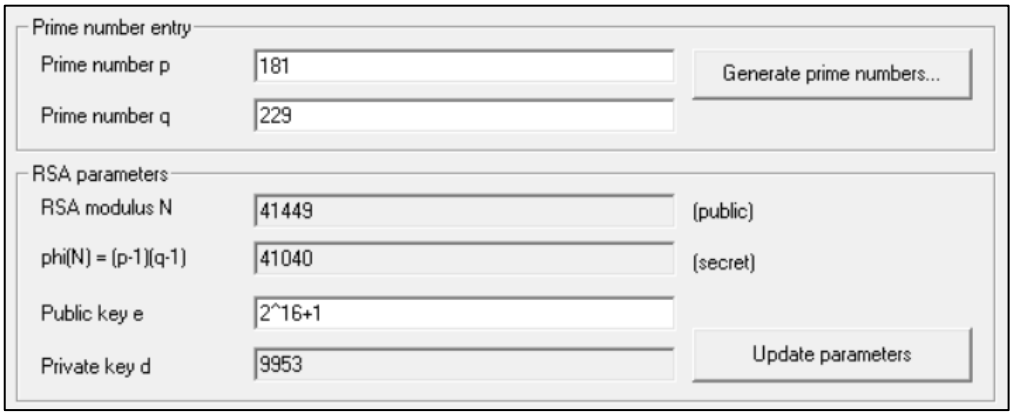

Рисунок 14 – Генерация открытого и закрытого ключей

5. Зашифруйте произвольное сообщение и передайте его вместе с, n и e коллеге. В ответ получите аналогичные данные от коллеги.

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

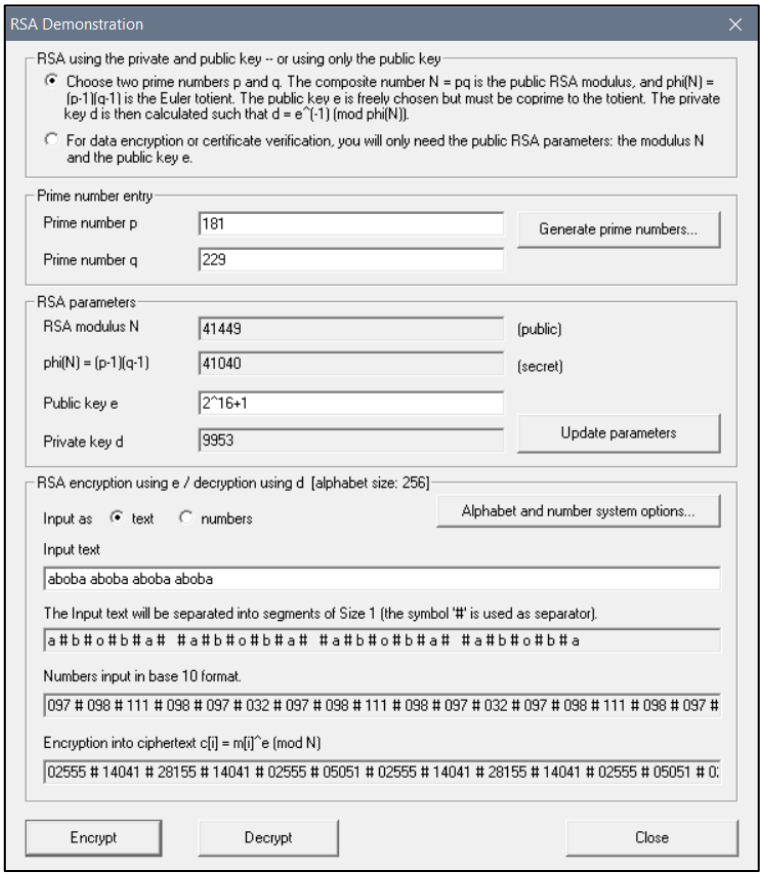

Рисунок 15 – Зашифрованное сообщение

Полученные данные от коллеги:

$(e, n) = (2^{16} + 1, 41449)$

Сообщение: ***02555 # 14041 # 28155 # 14041 # 02555 # 05051 # 02555 # 14041 # 28155 # 14041 # 02555 # 05051 # 02555 # 14041 # 28155 # 14041 # 02555 # 05051 # 02555 # 14041 # 28155 # 14041 # 02555***

6. Запустите утилиту Indiv.Procedures->RSACryptosystem->RSADemonstration и установите переключатель в режим «For data encryption…»

7. Выполните факторизацию модуля n командой Factorize…

Выполним факторизацию модуля n. Результат представлен на рис. 16

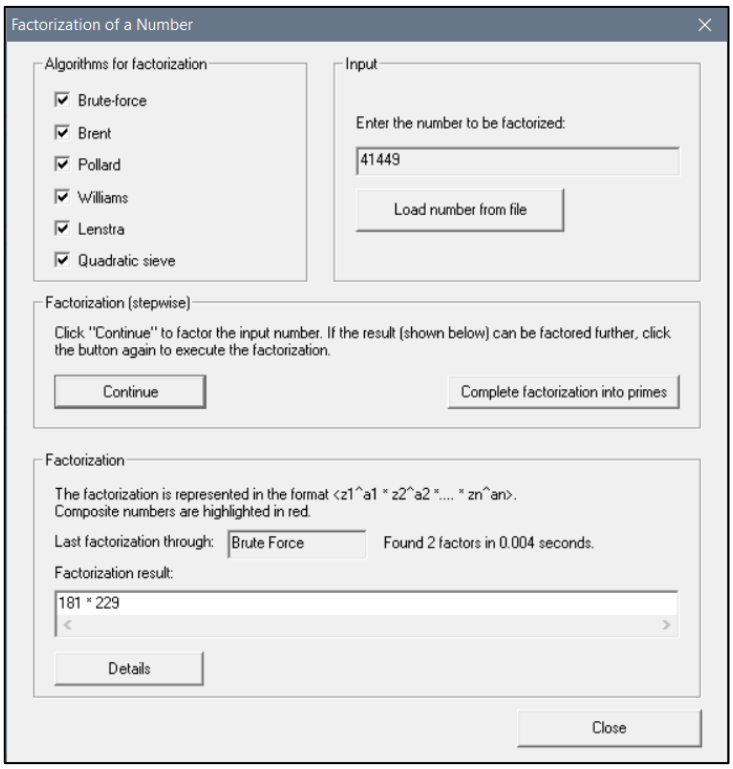

Рисунок 16 – Факторизация модуля

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

Выполним расшифровку полученного сообщения. Результат представлен на рис. 17

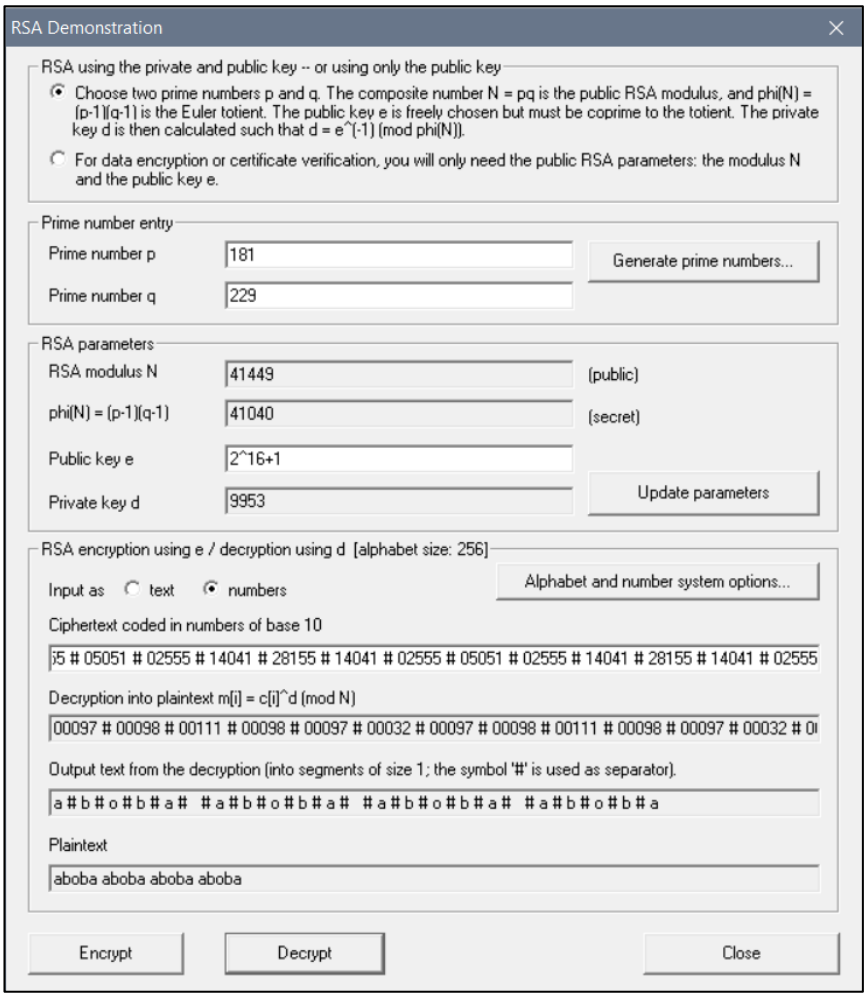

Рисунок 17 – Расшифрованное сообщение

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.

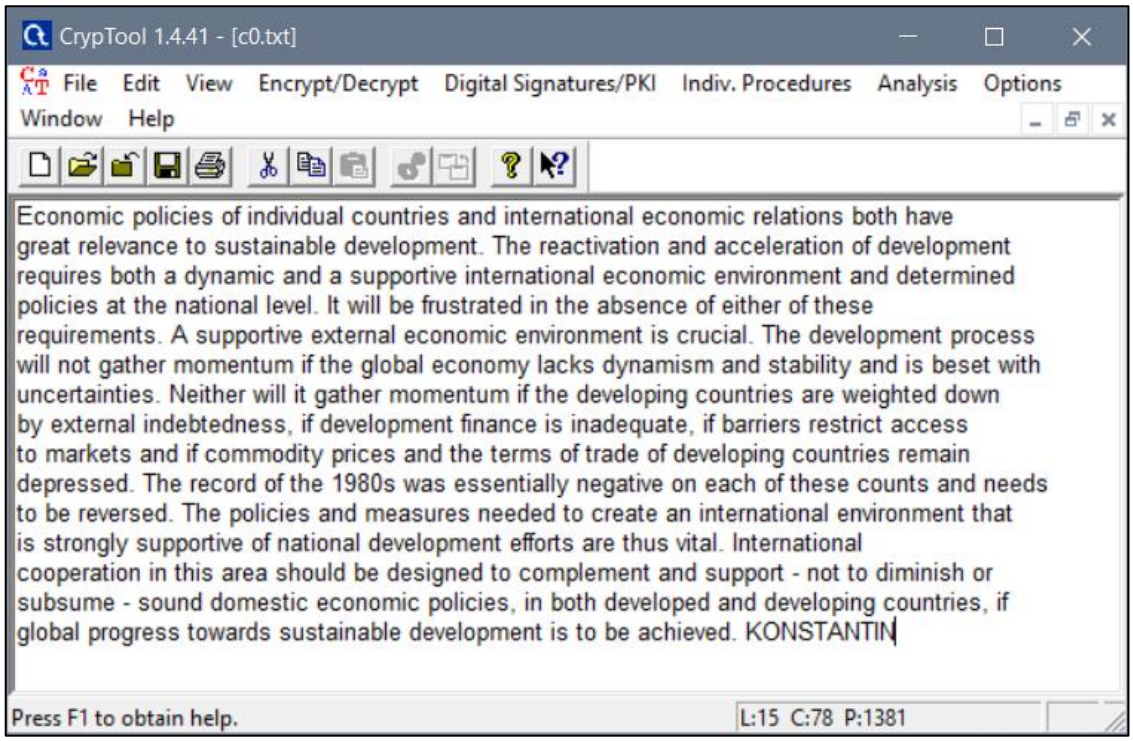

Рисунок 18 – Исходный текст

2. Запустите утилиту *Analysis->Asymmetric Encr…->Side-Channel attack on «Textbook RSA»…*

3. Настройте сервер, указав в качестве ключевого слова ваше имя, используемое в конце текста.

Настроим сервер, указав в качестве ключевого слова KONSTANTIN.

Настройки представлены на рис. 19.

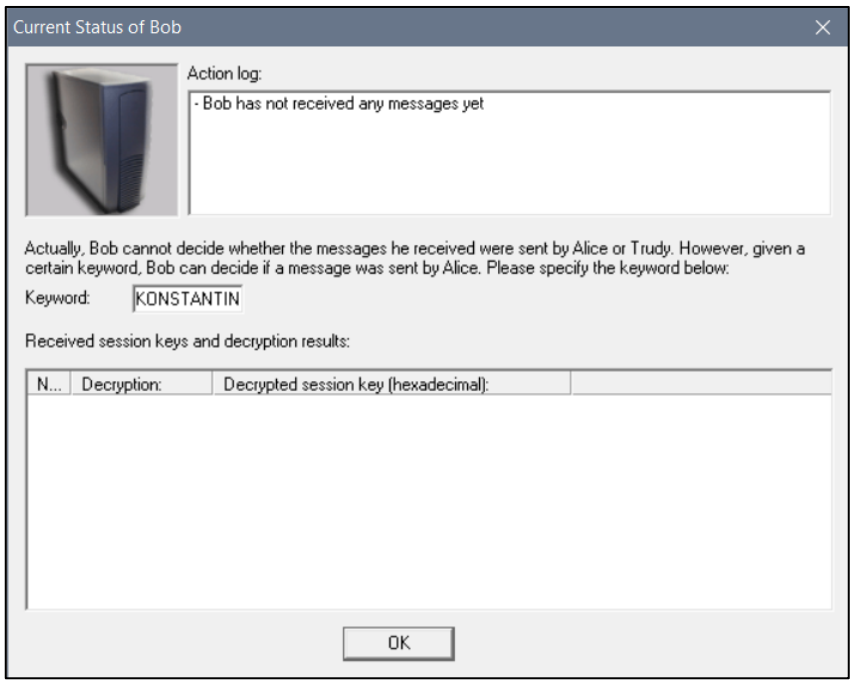

Рисунок 19 – Настройки сервера

4. Выполните последовательно все шаги протокола.
5. Сохраните лог-файлы участников протокола для отчета.

Лог-файлы участников протокола представлены ниже:

I. PREPARATIONS

Alice composes a message M, addressed to Bob.

Alice chooses a random session key S: 8722A33E83020666D589005E7A363A14

Alice symmetrically encrypts the message M with the session key S.

Alice chooses Bob's public key e: 010001

Alice asymmetrically encrypts the session key S with Bob's public RSA key e:

3519BBEA4B68AB90213B4828AA71092EB8EFDBF907FC7DEB9E9C59D4C8C4091ADEC4747

0A12920786A0D5C8A2979F588B8631125B3C1D72AD66947C86AEA92D7641310704CC527

8664B8BBBBBAC60AF4E9CC34253897192CF29B2F91D78E1B19E3A3CFA32E62FF578570E5

249F23D0DFC45797BE8A6DBB9608F75852B253B8AE

II. MESSAGE TRANSMISSION

Alice sends the hybrid encrypted file to Bob over an insecure channel.

III. MESSAGE INTERCEPTION

Trudy intercepts the hybrid encrypted file and isolates the encrypted session key S:

3519BBEA4B68AB90213B4828AA71092EB8EFDBF907FC7DEB9E9C59D4C8C4091ADEC4747

0A12920786A0D5C8A2979F588B8631125B3C1D72AD66947C86AEA92D7641310704CC527

8664B8BBBBBAC60AF4E9CC34253897192CF29B2F91D78E1B19E3A3CFA32E62FF578570E5

249F23D0DFC45797BE8A6DBB9608F75852B253B8AE

IV. BEGINNING OF THE ATTACK CYCLE

She sends an exact copy of the original, encrypted message to Bob and extends it with the session key S' (encrypted with Bob's public key). Compared to the message sent by Alice, Trudy simply replaces the encrypted session key [ENC(S, PubKeyBob) is replaced by ENC(S', PubKeyBob)].

Trudy repeats this step 130 times, whereas the step count depends on the bit length of the used session key (step count = bit length + 2).

Выводы

- Изучен протокол Диффи-Хеллмана.

Данный протокол позволяет паре пользователей выработать секретный ключ, не обмениваясь секретными данными по небезопасному каналу связи. Математическая модель протокола: общедоступная пара чисел p, g – первое — это большое простое число (более 300 десятичных цифр), второе — генератор (первообразный корень по модулю p), а также числа x, y, известные только отправителям. Сгенерированный секретный ключ использовался для шифрования текста. Результат расшифровки совпал с исходным текстом.

- Изучен шифр RSA

Это ассиметричный блочный шифр. Параметрами шифра являются два больших простых числа p, q, которые нужно уничтожить после вычисления пары закрытого и открытого ключей. Первый участник генерирует два ключа и передает открытый ключ (e, n) своему коллеге, ключ используется при зашифровке сообщений. Далее он же использует закрытый ключ для расшифровки.

- Исследовано время шифрования и расшифрования в зависимости от длины ключа.

Выполнение этих операций занимает мало времени. Время зашифровки во всех случаях составило 0 секунд, время расшифровки увеличивалось с ростом длины ключа. Для 512 битного ключа время составило 0.004 секунд, а для 2048 битного ключа – 0.049.

- Изучена атака грубой силы на шифр RSA.

При проведении атаки грубой силой был факторизован модуль, что привело к успешной атаке. Полученный результат был использован для расшифровки сообщения, полученного от коллеги. Результат расшифровки совпал с исходным текстом.

- Проведена атака на гибридную криптосистему.

Данная атака позволяет определить симметричный секретный ключ, зашифрованный открытым ключом криптосистемы. Нарушитель может

перехватывать и модифицировать сообщения, адресованные серверу, сервер не определяет, от кого был получен конверт, нарушитель может классифицировать ответы сервера как случаи успешной и неуспешной расшифровки.

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: 64459422689066243011729968057438442455606356397837044700733361991165383163799
g: 68359047310452750631845950766956340667934438563478283524081652748016608502 57

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

a: 736218675186128174054129487674881678455404785466302402720685521210366163824 20
b: 763548358858322118848485330441200582465626202929831833116669299738552257659 3

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):
736218675186128174054129487674881678455404785466302402720685521210366163824 20
b (reduced mod p):
763548358858322118848485330441200582465626202929831833116669299738552257659 3

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: 422920876542447033077896978783233727756768891533056634004695060075608525226 34
B: 547318464472580754731867705316787479269306630577829912121595157340439994306 45

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: 124171513023271400363874135025942856682960780660777080367900165440077632303169
SB: 124171513023271400363874135025942856682960780660777080367900165440077632303169

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