МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ

по лабораторной работе №7

Изучение асимметричных протоколов и шифров

Студент гр. 8382 Мирончик П.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

1. Задание

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

2. Выполните последовательно все шаги протокола.

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

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

2. Основные параметры протокола

Протокол Диффи-Хеллмана является первым из опубликованных криптопреобразований на основе открытых ключей. Поэтому этот протокол ещё называют обменом ключами по схеме Диффи-Хеллмана.

Цель протокола – обеспечить двум пользователям возможность получения симметричного секретного ключа путем обмена данными по незащищенному каналу связи.

Протокол Диффи-Хеллмана состоит из следующих операций (рисунок 1.1):

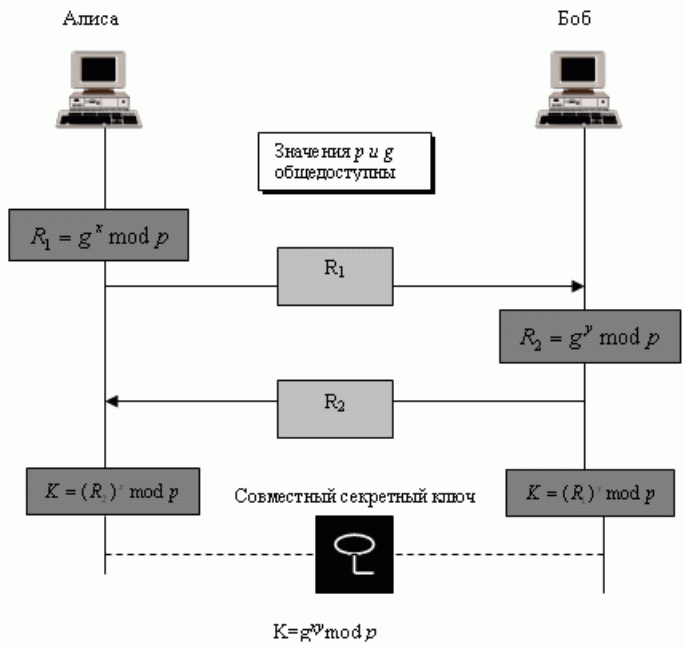


Рис. 1.1 – протокол Диффи-Хеллмана

1. Устанавливаются открытые параметры p, g:

а) p – большое простое число порядка 300 десятичных цифр (1024 бита),

b) g – первообразный корень по модулю p.

2. Каждая из сторон генерирует закрытый ключ - большое число x и y соответственно.

3. На каждой стороне вычисляется открытый ключ:

$$a)\ R_1 = g^x mod\ p,$$

$$b)\ R_2 = g^y mod\ p.$$

4. Стороны обмениваются открытыми ключами и вычисляют симметричный общий ключ *K:*

$$K = R_2^x mod\ p = R_1^y mod\ p$$

3. Скриншот схемы протокола, реализованной в CrypTool

В CtypTool 1 предлагается визуализация алгоритма Диффи-Хеллмана, представленная на рис. 1.2:

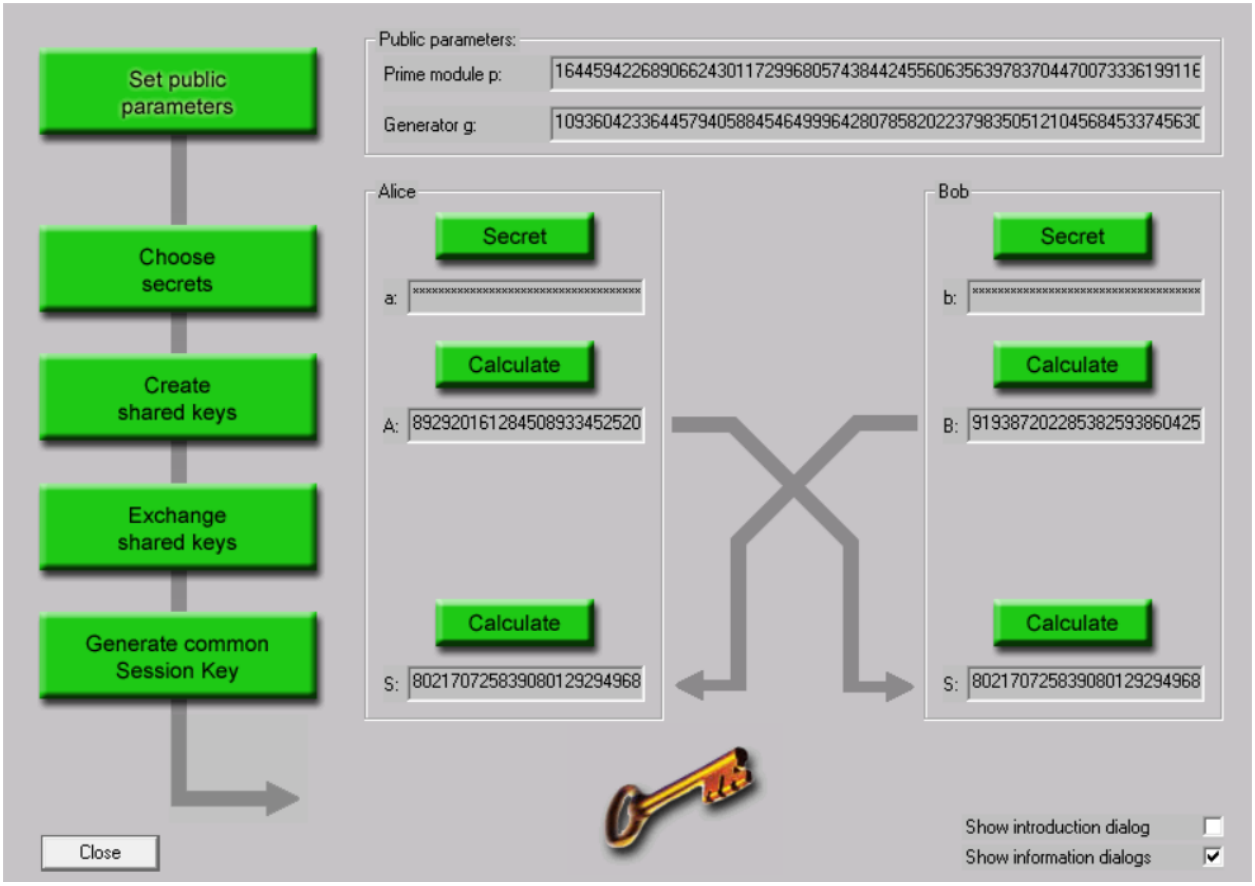


Рис. 1.2 – визуализация алгоритма Диффи-Хеллмана

Лог для конфигурации рис. 1.2:

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

p:
16445942268906624301172996805743844245560635639783704470073336199
1165383163799

g:
10936042336445794058845464999642807858202237983505121045684533745
6309950888104

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

a:
80511171697292728927267482045301515586392655869795410209932266115
266325794450

b:
13288343802659056568964013307985465897159776651081605607206193985
5936954075515
```

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):
80511171697292728927267482045301515586392655869795410209932266115266325794450

b (reduced mod p):
13288343802659056568964013307985465897159776651081605607206193985593695407551 5

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:
89292016128450893345252026234153301367288821286528526924168402994936741417507

B:
91938720228538259386042576706105399585128473642079512722002964805630641494088

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:
80217072583908012929496887394963877375904788058818167321122593455110740473335

SB:
80217072583908012929496887394963877375904788058818167321122593455110740473335

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

4. Шифрование с использованием сгенерированного ключа

В 3 пункте был сгенерирован ключ:

80217072583908012929496887394963877375904788058818167321122593455110740473335

Пусть в качестве алгоритма шифрования используется AES с длиной ключа 256 бит. Для упрощения представим, что ключ уже записан в шестнадцатеричном виде; тогда нам нужны только первые 64 символа:

`802170725839080129294968873949638773759047880588181673211225934 5`

Выполним с его использованием шифрование и расшифрование. Исходный, зашифрованный и расшифрованный тексты представлены на рис. 1.3, 1.4 и 1.5 соответственно.

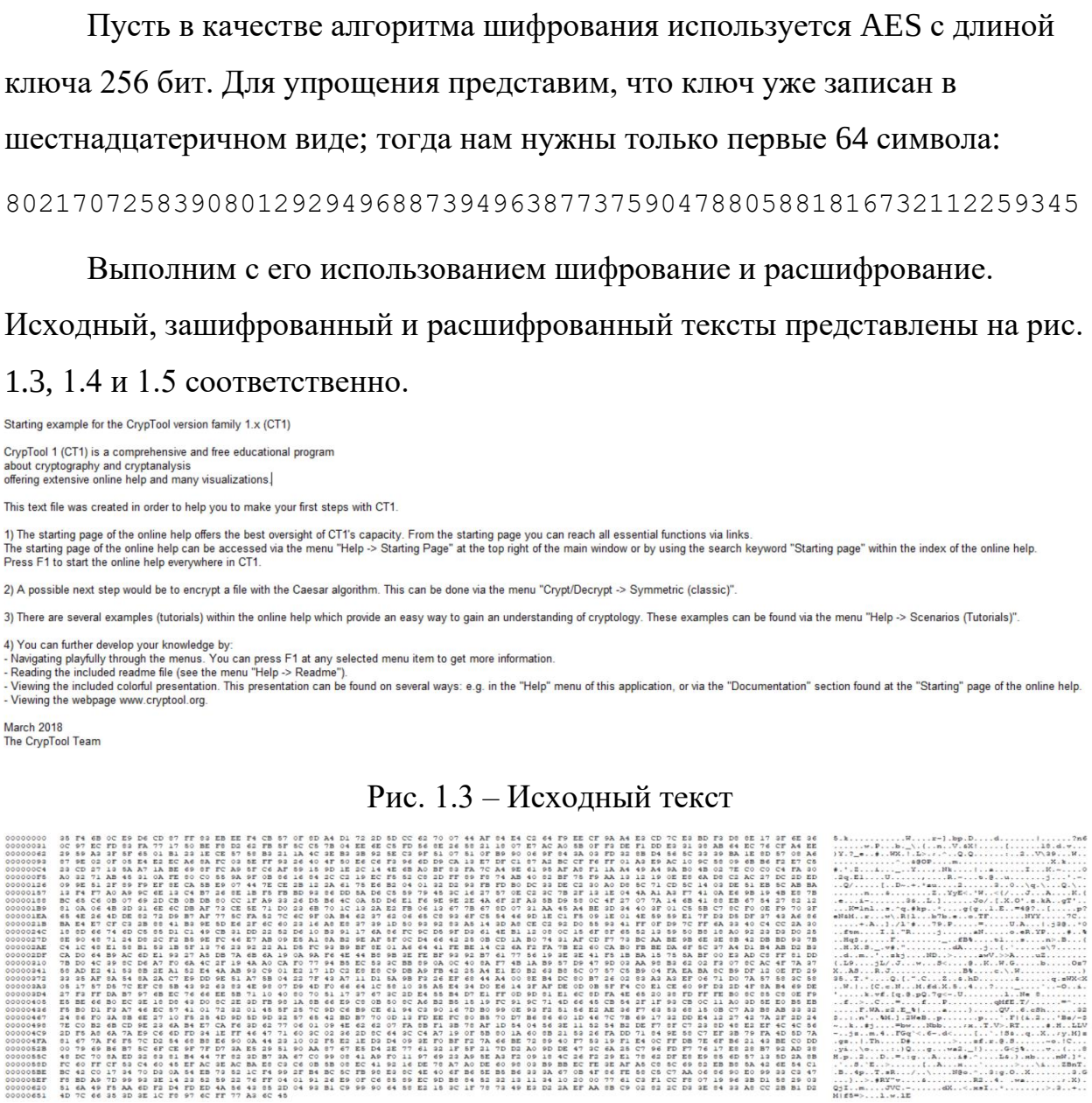


Рис. 1.3 – Исходный текст

Рис. 1.4 – Зашифрованный текст

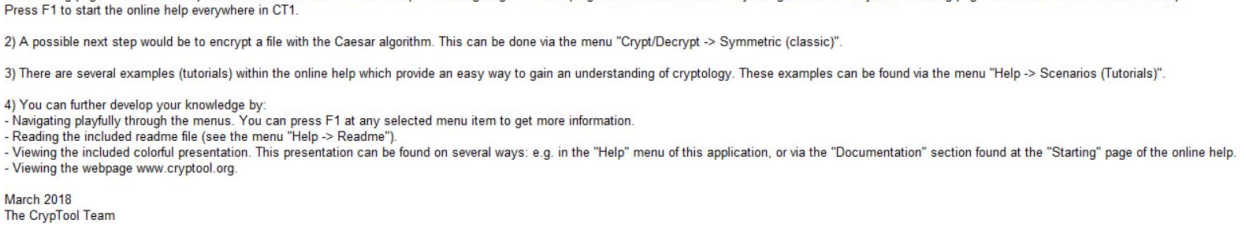


Рис. 1.5 – расшифрованный текст

ШИФР RSA

1. Задание

1. Запустите утилиту Indiv.Procedures->RSACryptisystem->RSA Demonstration

2. Задайте в качестве обрабатываемого сообщения свою Ф.И.О.

3. Сгенерируйте открытый и закрытый ключи.

4. Зашифруйте сообщение. Сохраните скриншот результата.

5. Расшифруйте сообщение. Сохраните скриншот результата.

6. Убедитесь, что расшифрование произошло корректно.

2. Описание шифра

Алгоритм RSA представляет собой асимметричный блочный шифр, в котором и открытый, и шифрованный текст представляются целыми числами из диапазона от 0 до n-1 для некоторого n.

Алгоритм шифрования RSA состоит из следующих операций (рисунок 2.1):

1. Вычисление ключей:

a) Генерация двух больших простых чисел p и q (p и q держаться в секрете).

b) Вычисление n = p * q

c) Выбор произвольного e (e <n), взаимно простого с $\varphi(n)$ – функцией Эйлера

d) Вычисление d: $e * d = 1 \; mod \; \varphi(n)$.

e) Числа (e, n) – открытый ключ, d – закрытый ключ, p и q уничтожаются.

2. Шифрование:

a) Открытый текст разбивается на блоки m_i: $m_i < n$.

b) Каждый блок открытого текста преобразуем в шифротекст по формуле:

$$c_i = m_i^e mod\ n$$

3. Расшифровка:

a) Шифротекст представляется блоками c_i: $c_i < n$.

b) Каждый блок шифротекста преобразуется в открытый текст по формуле:

$$m_i = c_i^d mod\ n$$

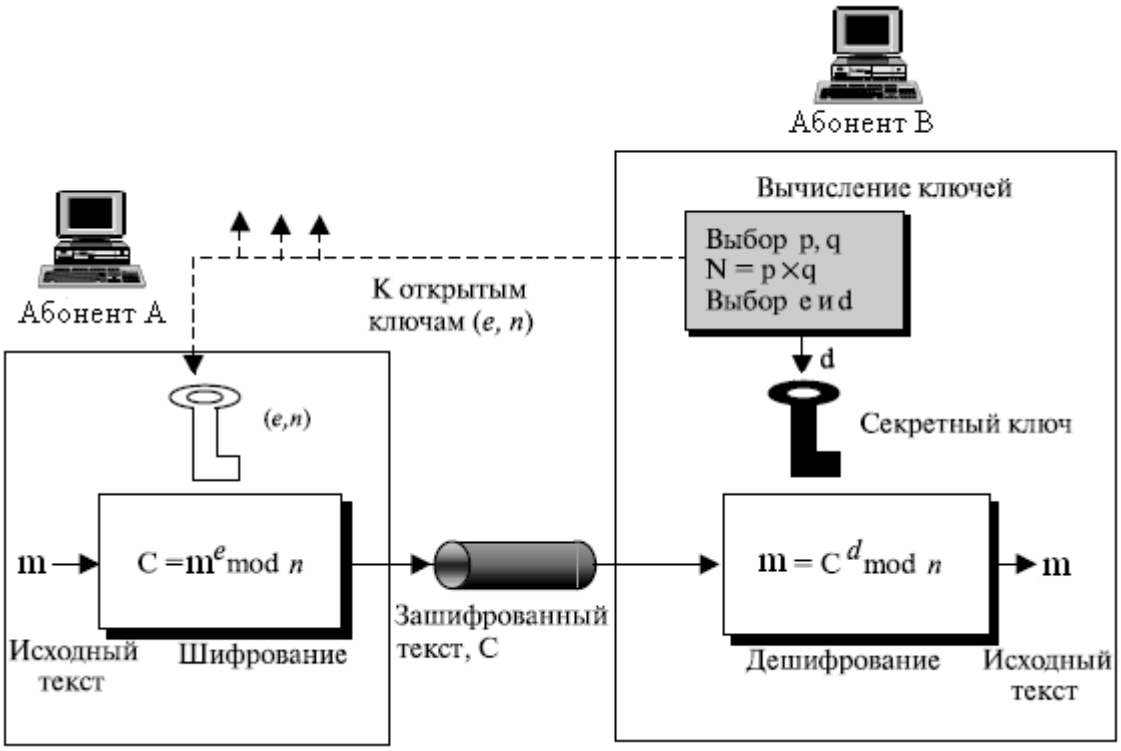


Рис. 2.1 – Схема шифра RSA

3. Генерация ключей

Воспользуемся генератором ключей, реализованным в CrypTool 1 (Рис. 2.2):

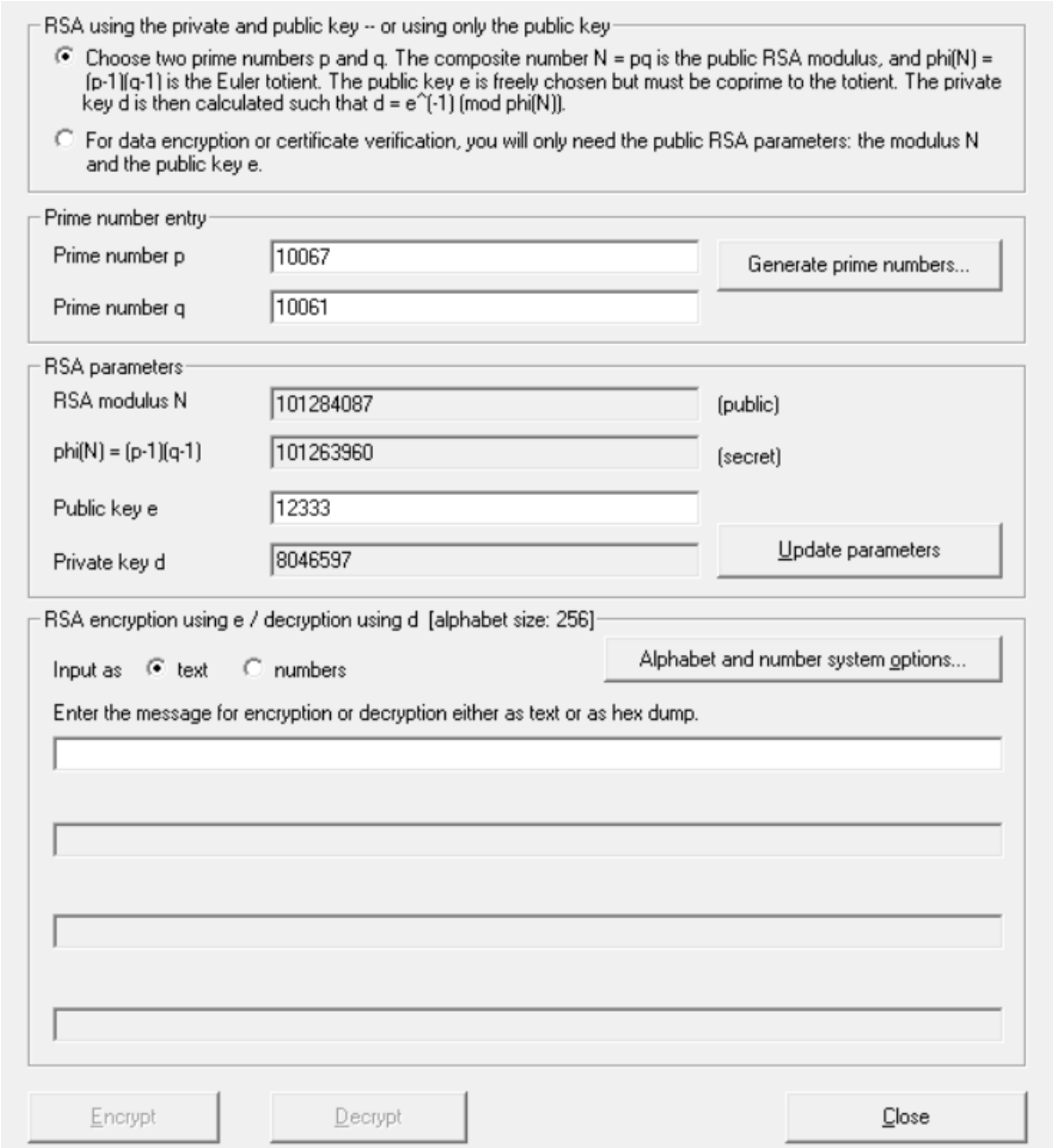
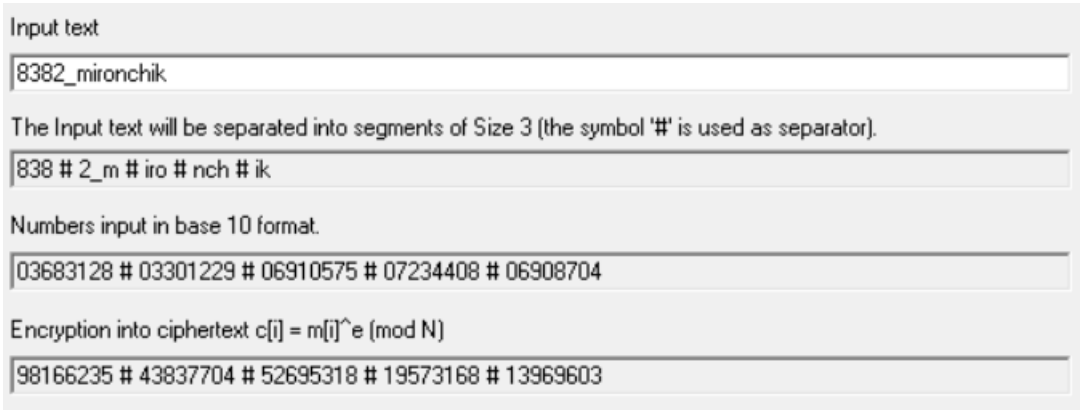


Рис. 2.2 – Генерация ключей

Зашифруем с их помощью сообщение:

`8382_mironchik`

Процесс зашифрования представлен на рис. 2.3.



2.3 – Зашифрование сообщения

И расшифруем с использованием того же инструмента (рис. 2.4):

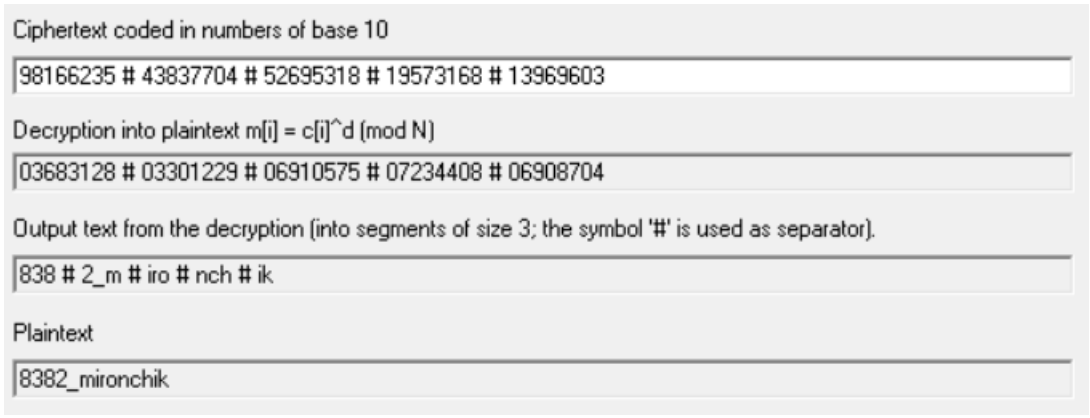


Рис. 2.4 – Расшифрование сообщения

Видно, что в результате расшифрования было получено исходное сообщение.

ИССЛЕДОВАНИЕ ШИФРА RSA

1. Задание

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

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

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

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

5. Проверить корректность расшифровки. Зафиксировать скриншоты результата.

2. Генерация ключей

Для генерации ключей воспользуемся стандартной утилитой CrypTool 1 (рис. 3.1).

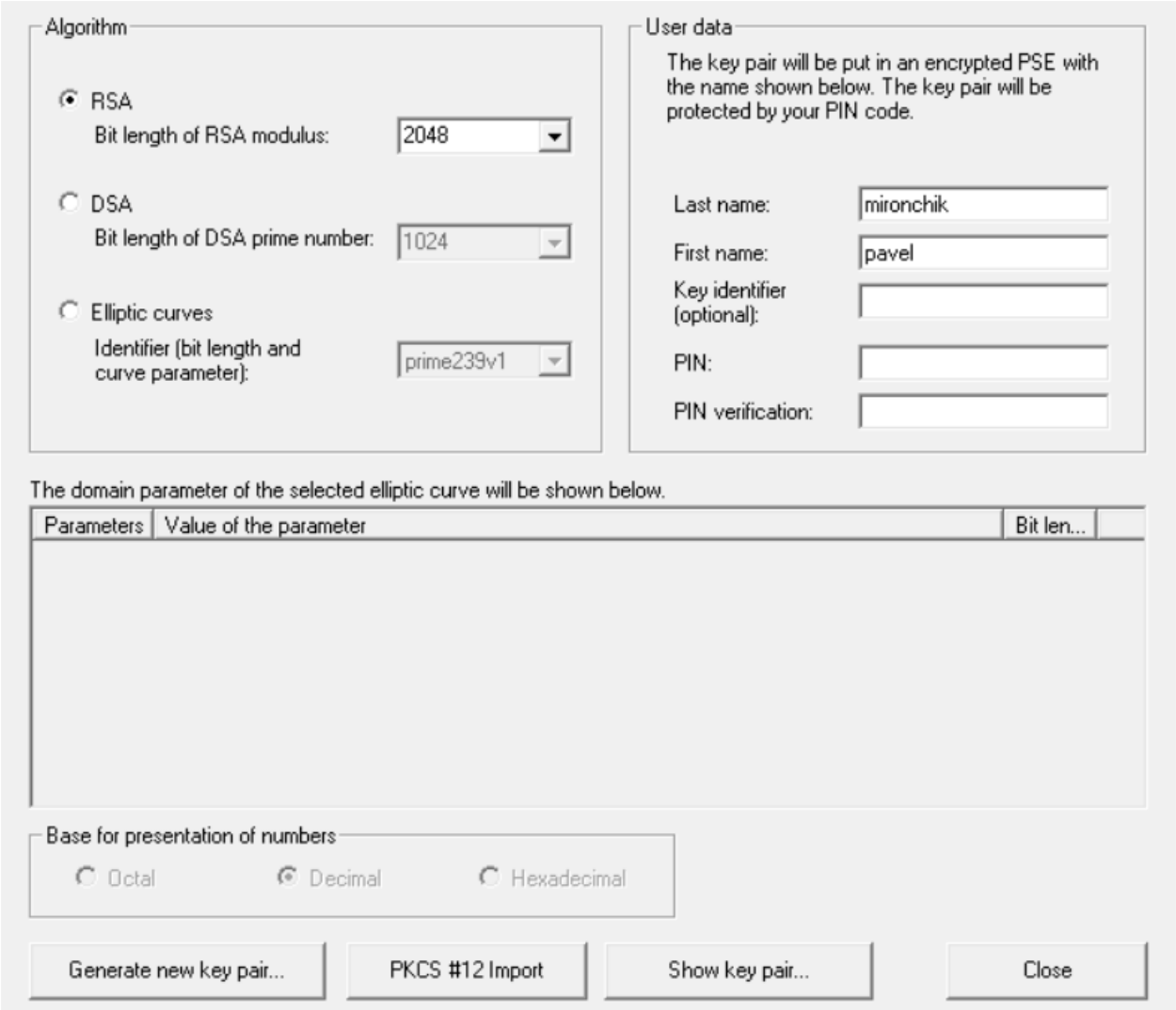


Рис. 3.1 – Генерация ключей

В результате было сгенерировано 4 пары ключей с длинами 512, 768, 1024 и 2048 бит.

Для дальнейшего зашифрования был выбран фрагмент текста из предыдущей лабораторной работы:

```
Mr. and Mrs. Dursley, of number four, Privet Drive, were proud
to say that they were perfectly normal, thank you very much.
They were the last people you'd expect to be involved in
anything strange or mysterious, because they just didn't hold
with such nonsense.

Mr. Dursley was the director of a firm called Grunnings, which
made drills. He was a big, beefy man with hardly any neck,
although he did have a very large mustache. Mrs. Dursley was
thin and blonde and had nearly twice the usual amount of neck,
which came in very useful as she spent so much of her time
craning over garden fences, spying on the neighbors. The
```

```
Dursleys had a small son called Dudley and in their opinion
there was no finer boy anywhere.

The Dursleys had everything they wanted, but they also had a
secret, and their greatest fear was that somebody would discover
it. They didn't think they could bear it if anyone found out
about the Potters. Mrs. Potter was Mrs. Dursley's sister, but
they hadn't met for several years; in fact, Mrs.
```

3. Зашифрование

Выполним зашифрование исходного текста и измерим время, затраченное на зашифрование.

Табл. 3.1 – Исследование времени зашифрования

Длина ключа (бит)	Время зашифрования
512	0s
768	0s
1024	0s
2048	0.006s

Видно, что зашифрование сообщения занимает минимальное количество времени и незаметно для пользователя, составляя менее одной миллисекунды для длины менее 1024 бита. Тем не менее можно заметить, что на длине ключа 2048 бит зашифрование выполнялось немного медленнее и уже поддается измерению в выбранной точности, составляя 6 миллисекунд.

4. Расшифрование

Выполним расшифрование текста и измерим время, затраченное на расшифрование.

Табл. 3.2 – Исследование времени расшифрования

Длина ключа (бит)	Время расшифрования
512	0s
768	0s
1024	0.012s

2048	0.031s

Заметно, что время расшифрования текста потребовало больше времени в сравнении с зашифрованием, оставаясь по-прежнему достаточно небольшим. Как и в случае с зашифрованием, увеличение длины ключа влечет увеличение времени расшифрования.

5. Проверка корректности расшифрования

Удостоверимся, что в результате расшифрования был получен исходный текст (рис. 3.2):

```
Mr. and Mrs. Dursley, of number four, Privet Driv
e, were proud to say that they were perfectly nor
mal, thank you very much. They were the last peop
le you'd expect to be involved in anything strang
e or mysterious, because they just didn't hold wi
th such nonsense.....Mr. Dursley was the director
 of a firm called Grunnings, which made drills. H
e was a big, beefy man with hardly any neck, alth
ough he did have a very large mustache. Mrs. Durs
ley was thin and blonde and had nearly twice the
usual amount of neck, which came in very useful a
s she spent so much of her time craning over gard
en fences, spying on the neighbors. The Dursleys
had a small son called Dudley and in their opinio
n there was no finer boy anywhere.....The Dursley
s had everything they wanted, but they also had a
 secret, and their greatest fear was that somebod
y would discover it. They didn't think they could
 bear it if anyone found out about the Potters. M
rs. Potter was Mrs. Dursley's sister, but they ha
dn't met for several years; in fact, Mrs.........
..................................................
..................................................
..................................................
..................................................
..................................................
```

Рис. 3.2 – Результат расшифрования

Видно, что текст соответствует исходному. Расшифрование выполнено успешно.

АТАКА ГРУБОЙ СИЛЫ НА RSA

1. 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.

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

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

7. Выполните факторизацию модуля n командой Factorize…

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

2. Зашифрование сообщения

В качестве сообщения был использован следующий текст:

```
8382_mironchik
```

Были сгенерированы числа $p = 197, q = 101$ и получен $n = pq = 19897 > 256$, задан открытый ключ $e = 2^{16} + 1$ и получен закрытый ключ $d = 13473$.

Полученный зашифрованный текст:

```
13100 # 19280 # 13100 # 00415 # 10439 # 06795 # 05146 # 18425 #
07686 # 02690 # 13580 # 12011 # 05146 # 01782
```

3. Расшифрование сообщения

В результате факторизации известного модуля $n = 19897$ были получены составляющие его простые числа $p = 101, q = 197$ (рис. 4.1). В качестве значения открытой части ключа было выбрано $e = 12333$.

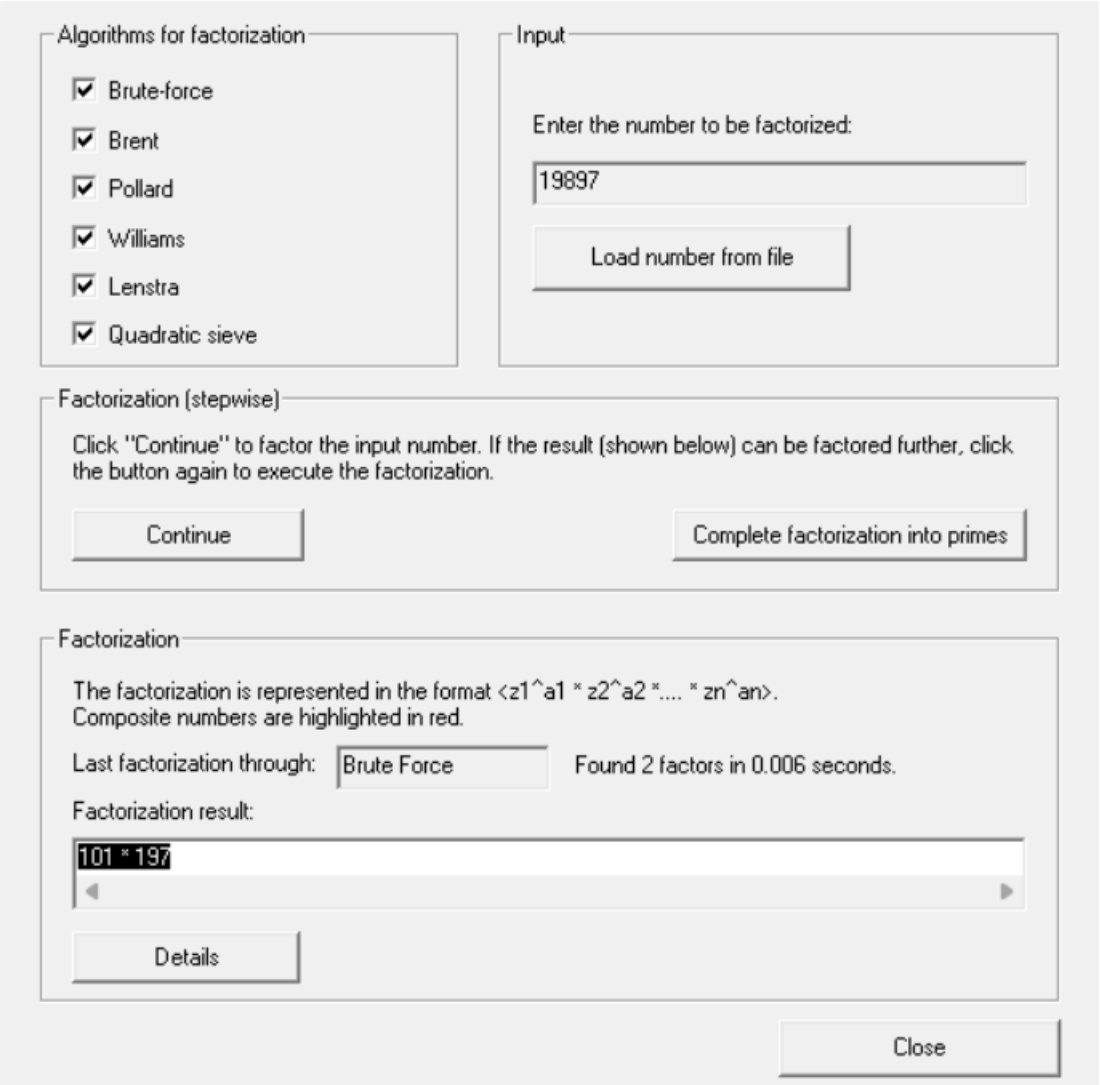


Рис. 4.1 – Результат факторизации

С использованием полученной информации выполнено расшифрование сообщение и получен корректный исходный текст (рис. 4.2).

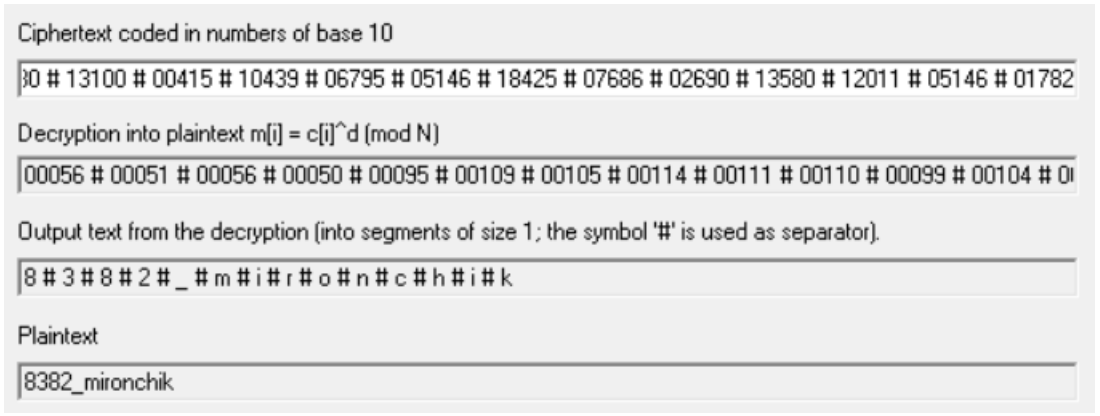


Рис. 4.2 – Дешифрование сообщения

ИМИТАЦИЯ АТАКИ НА ГИБРИДНУЮ КРИПТОСИСТЕМУ

1. Задание

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

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.

4. Выполните последовательно все шаги протокола.

5. Сохраните лог-файлы участников протокола для отчета.

2. Описание атаки

Модель гибридной криптосистемы, асимметричная составляющая которой использует асимметричный шифр (например RSA) представлена на рисунке 5.1. 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.

Атака на модель гибридной криптосистемы основана на том, что злоумышленник сначала перехватывает цифровой конверт, содержащий зашифрованное сообщение и зашифрованный секретный ключ, затем, модифицирует шифровку ключа из конверта и побитово восстанавливает зашифрованный секретный ключ, анализируя положительные и отрицательные ответы сервера.

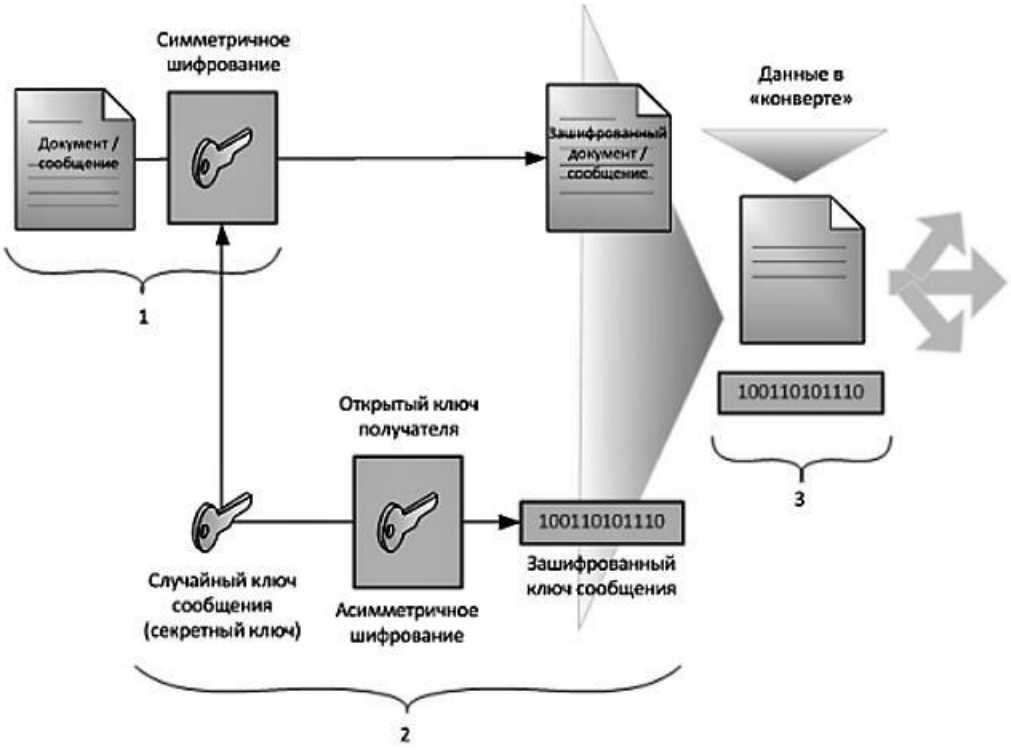


Рис. 5.1 – Модель гибридной системы

3. Подготовка к имитации атаки

В качестве сообщения будем использовать текст:

```
Mr. and Mrs. Dursley, of number four, Privet Drive, were proud
to say that they were perfectly normal, thank you very much.
They were the last people you'd expect to be involved in
anything strange or mysterious, because they just didn't hold
with such nonsense.

Mr. Dursley was the director of a firm called Grunnings, which
made drills. He was a big, beefy man with hardly any neck,
although he did have a very large mustache. Mrs. Dursley was
thin and blonde and had nearly twice the usual amount of neck,
which came in very useful as she spent so much of her time
craning over garden fences, spying on the neighbors. The
Dursleys had a small son called Dudley and in their opinion
there was no finer boy anywhere.

The Dursleys had everything they wanted, but they also had a
secret, and their greatest fear was that somebody would discover
it. They didn't think they could bear it if anyone found out
about the Potters. Mrs. Potter was Mrs. Dursley's sister, but
they hadn't met for several years; in fact, Mrs.

mironchik
```

Открытым ключем получателя выберем сгенерированный ранее RSA ключ длины 512 бит.

4. Имитация атаки

В результате имитации атаки был получен следующий лог:

```
I. PREPARATIONS

Alice composes a message M, addressed to Bob.

Alice chooses a random session key S:
49C2C35520FE1FA180BCAE930D261100

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:
58D651A5EA861D51DC63D91F49B80E501C3800E31F2D64EA165A09EA4B680894
A7ABE76C53D37C211F068CF71CF9712DFA0DB6639E9520FFFFD117EBAC5FA5D2

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:
58D651A5EA861D51DC63D91F49B80E501C3800E31F2D64EA165A09EA4B680894
A7ABE76C53D37C211F068CF71CF9712DFA0DB6639E9520FFFFD117EBAC5FA5D2

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

В ходе выполнения работы были рассмотрены принципы работы ассиметричных шифров.

Рассмотрен протокол Диффи-Хеллмана, позволяющий осуществлять генерацию секретного ключа на двух сторонах без передачи непосредственно ключа между сторонами, проведена пробная генерация ключей и их использование для зашифрования и расшифрования сообщения.

Далее был рассмотрен шифр RSA. Сгенерированы ключи небольшой длины, с помощью которых было зашифровано и расшифровано сообщение, что позволило проверить корректность работы алгоритма. Исследована также скорость работы алгоритма при зашифровании и расшифровании текста длиной примерно 1000 символов на ключах разной длины. Выяснено, что зашифрование выполняется немного быстрее, чем расшифрование, что связано, скорее всего, исключительно с подобранными значениями ключей. Также определено, что длительность зашифрования и расшифрования напрямую зависит от длины ключа.

Проведена атака грубой силы на шифр RSA при помощи коллеги. Для этого были сгенерированы ключи небольшой длины так, что модуль $n = pq > 256$. Коллеге были переданы открытые данные $e = 12333$ и значение модуля. По этим данным была выполнена факторизация модуля и найден закрытый ключ d, с использованием которого удалось расшифровать сообщение.

В конце была изучена гибридная криптосистема. Рассмотрен принцип ее работы, а также проведения атак на такую систему с использованием CrypTool 1.