**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра ИБ**

**отчет**

**по лабораторной работе №7**

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

**Тема: Изучение ассиметричных шифров**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 4383 |  | Гордеева Т.В. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2017

**Цель работы:** исследовать протокол Диффи-Хеллмана, шифр RSA и получить практические навыки работы с ними, в том числе и в программном продукте CrypTool 1.

**1 Протокол Диффи-Хеллмана**

**1.1 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.

**1.2 Основные параметры протокола.**

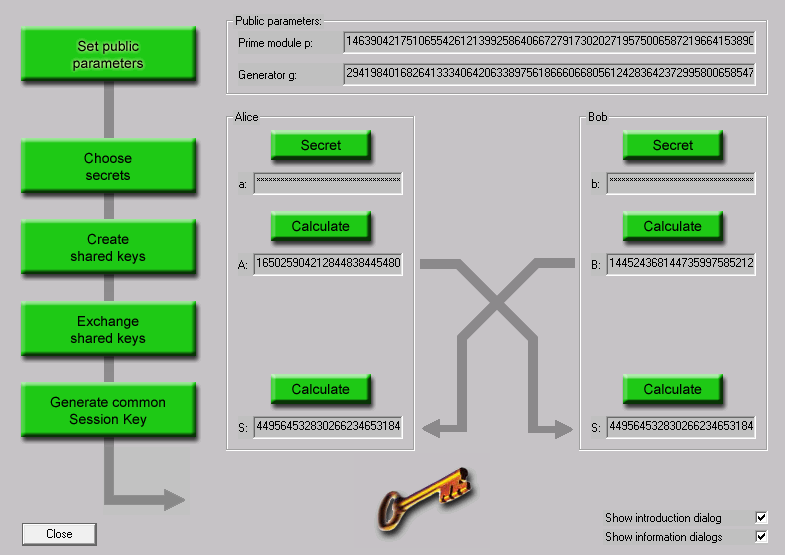


**1.3 Скриншот схемы протокола, реализованной в CrypTool.**

Запустим утилиту Indiv.Procedures->Protocols->Diffie-Hellman demonstration… и установим все опции информирования в ON.

Выполним последовательно все шаги протокола.

Схема протокола в CrypTool:

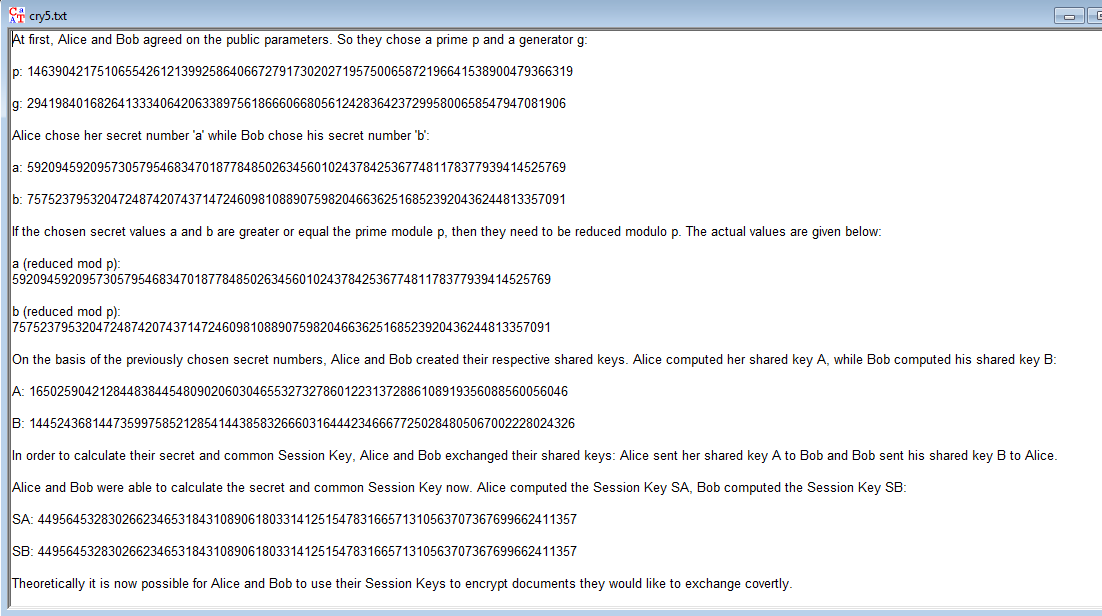
****

**1.4 Таблица соответствия схемы протокола (CrypTool) и параметров протокола.**

|  |  |  |
| --- | --- | --- |
| **Параметры протокола** | **Параметры в демо Cryptool 1** | **Назначение** |
|  |  | Большое простое число, общедоступно |
|  |  | Первообразный корень по модулю p, общедоступен |
|  |  | Большое секретное число Алисы |
|  |  | Большое секретное число Боба |
|  |  | Открытый ключ на стороне Алисы |
|  |  | Открытый ключ на стороне Боба |
|  |  | Симметричный общий ключ |

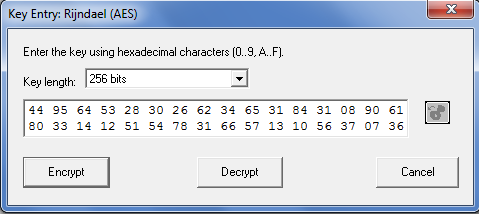
**1.5 Скриншот исходного, зашифрованного и расшифрованного текстов.**

Лог-файл протокола:

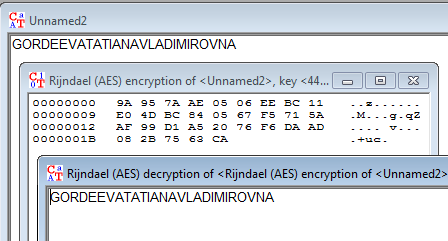
****

Используем полученный общий ключ для зашифровки и расшифровки произвольного сообщения. В качестве шифра выберем AES.

Параметры шифрования:



Исходный текст и шифротекст:



**2 Шифр RSA**

**2.1 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.

**2.2 Обобщенная схема шифра.**

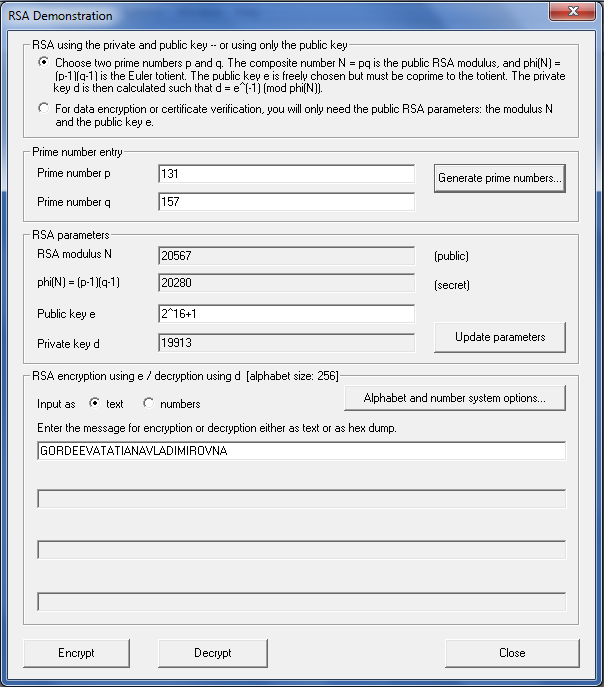
****

**2.3 Скриншот результата генерации ключей.**

Запустим утилиту Indiv.Procedures->RSACryptisystem->RSA Demonstration. Зададим в качестве обрабатываемого сообщения свою Ф.И.О.

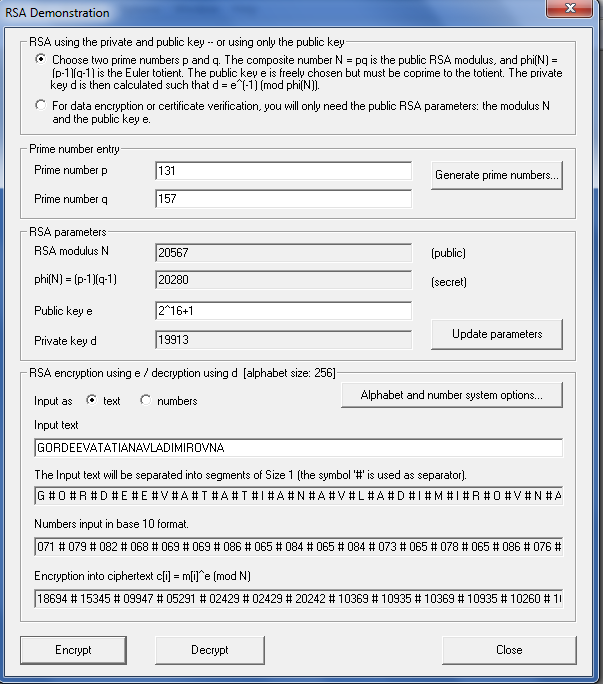
Сгенерируем открытый и закрытый ключи.

Параметры шифра RSA:



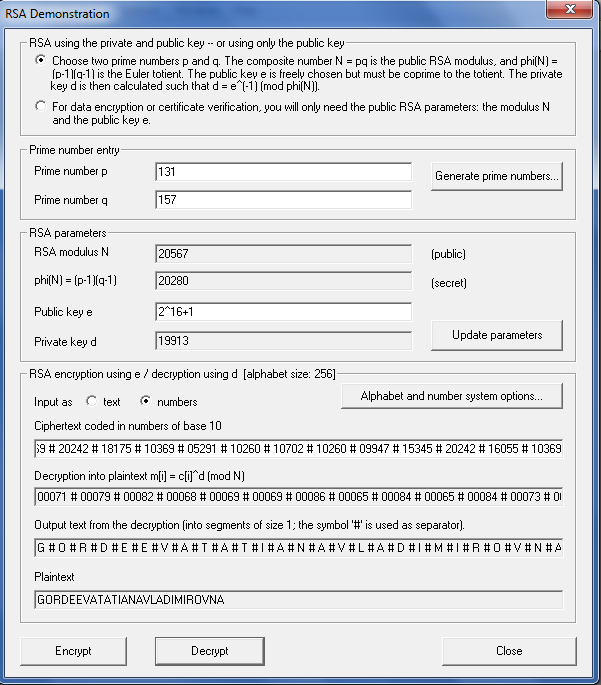
**2.4 Скриншот результата шифрации.**

Зашифруем сообщение.

****

**2.5 Скриншот результата расшифровки**

Расшифруем сообщение.



Результат расшифрования совпадает с исходным текстом, следовательно, можно сделать вывод, что расшифрование прошло корректно.

**3 Исследование шифра RSA**

**3.1 Задание**

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

2. Сгенерировать пары ассиметричных 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.

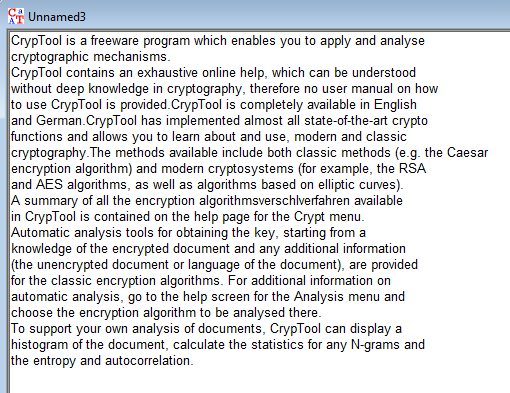
4. Расшифровать текст различными закрытыми ключами. Зафиксировать время зашифровки.

5. Проверить корректность расшифровки. Зафиксировать скриншоты результата.

**3.2 Выбранный текст.**

Выберем текст на английском языке (не менее 1000 знаков) и сохраним в файле формата \*.txt

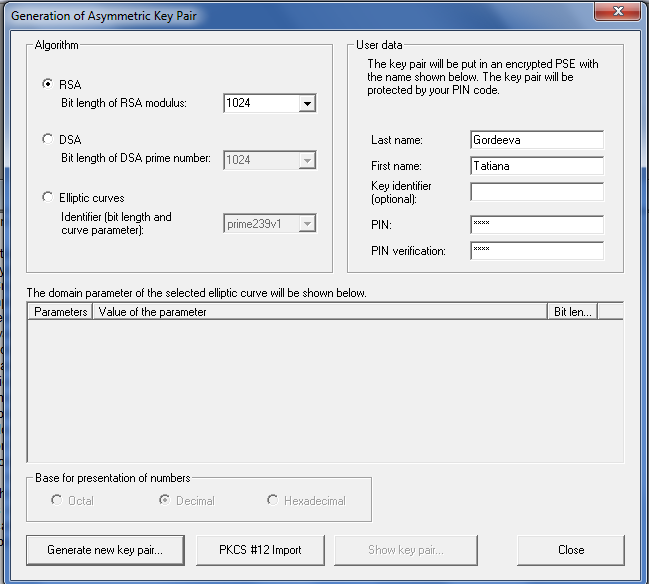
Исходный текст:

****

**3.3 Результаты генерации ключевых пар различной длины.**

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

Параметры генерации:



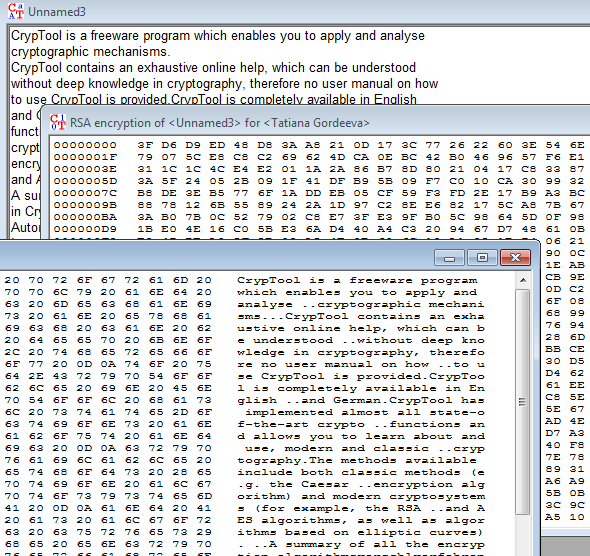
*Таблица 1. Результат генерации ключей*

|  |  |  |
| --- | --- | --- |
| **Размер ключа** | **Exponent** | **Modulus** |
|  | 13389384268704827010053510348139964482974101245538588299377854141718596696602567097710836419401541834528724652076892458901890212123220497621109295257406989 | 65537 |
|  | 1545892289900529391179244305688506053565622477189298177408971722611222871909820200544821841286024260698469134551571392464712033448965926629191731608188491426514734202185277776337169997867396644760968636717309304771195531369322610521 | 65537 |
|  | 178977747708237964343414796272859963723120284872705819813823752948098298726511278050957314187091083713431940529084369965551165791555732996934837380145102512656223393784347724573966385567447297881565874930200590561028805673827645336299181887691127174080879991052101592272604514424920740915918439406260789129127 | 65537 |
|  | 32273842804530610394212777613657422181223863682151478189889969553386779773093994786061772000750915692049287713150926809778700636348195693591307299646202021260905075027146533877622111903829261798798048175054745665255169747626200397141674120784382434160463982780782609723251907967004209163555165572358570583193496916151533440633787178153035582540769625414703471440645049021601989989249587519153771683675339630240817215036861951130326018220576672933688911674953937002529188560335602435630653316822921931225419671436398639484603214825279630082425229193615971300120475682663699423301048218863199048660796035551893939303379 | 65537 |

**3.4 Размер исходного текста.**Размер исходного текста 1161 знак.

**3.5 Таблица затрат времени на зашифровку и расшифровку при использовании ключей разной длины.**

Пример зашифровки и расшифровки текста (ключ 2048 бит)



*Таблица 2. Затраты времени на зашифровку и расшифровку при использовании ключей разной длины*

|  |  |  |
| --- | --- | --- |
| **Длина ключа** | **Время зашифровки, c** | **Время расшифровки, c** |
| 512 | 0 | 0,008 |
| 768 | 0 | 0,018 |
| 1024 | 0 | 0,022 |
| 2048 | 0,002 | 0,094 |

**4 Атака грубой силы на RSA**

**4.1 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.

**4.2 Исходные данные для атаки, полученные от коллеги**

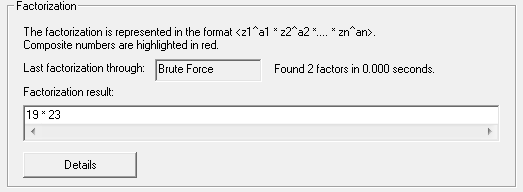
Полученные данные:

|  |  |  |
| --- | --- | --- |
| **Сообщение** | **e** | **n** |
| 261 # 225 # 174 # 174 # 063 # 149 # 041 # 411 # 428 # 147 # 372 # 428 | 2^16+1 | 437 |

**4.3 Результат факторизации (скриншот).**

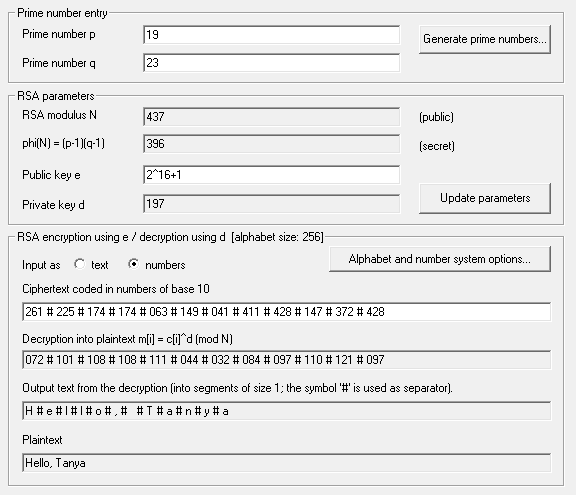
Запустим утилиту Indiv.Procedures->RSACryptosystem- >RSADemonstration и установим переключатель в режим «For data encryption…» Выполним факторизацию модуля n командой Factorize…

Результат факторизации:

****

**4.4 Расшифрованное в итоге сообщение.**

Результат расшифровки сообщения, полученного от коллеги:



В результате расштфровки был получен корректный текст.

**5 Имитация атаки на гибридную криптосистему**

**5.1 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.

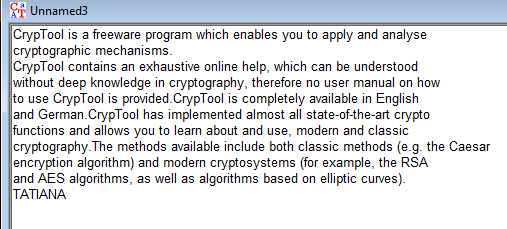
**5.2 Описание цели атаки**

*Цель атаки* - завладеть симметричным секретным ключом, который зашифрован 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.

**5.3 Текст передаваемого сообщения**

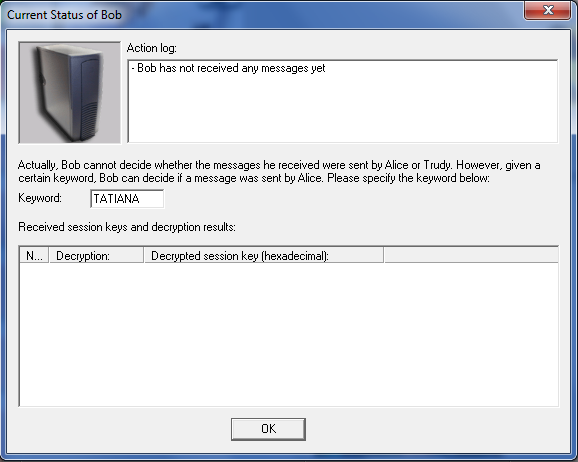
Текст сообщения:



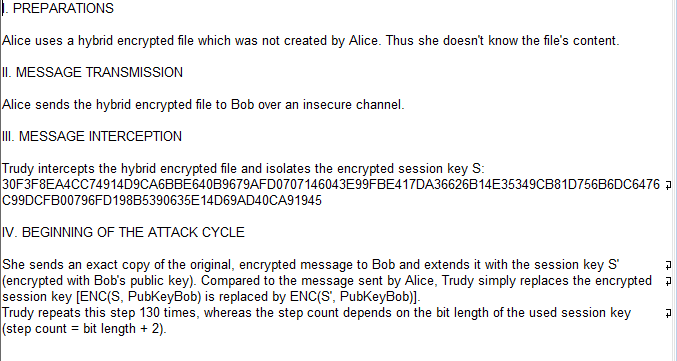
**5.4 . Лог-файлы участников протокола**

Запустим утилиту Analysis->Asymmetric Encr…->Side-Channel attack on «Textbook RSA»…Настроим сервер, указав в качестве ключевого слова TATIANA, используемое в конце текста. Выполним последовательно все шаги протокола.

Настроенный сервер:



Лог-файлы участников протокола:



Атака на гибридную систему прошла успешно.

**5 Вывод**

* В ходе данной лабораторной работы был исследован протокол получения симметричного секретного ключа Диффи-Халфмана. На основе рассмотрения работы демоприложения были изучены шаги и основные параметры протокола. Также ключ, полученный алгоритмом, был применен для шифрования и расшифрования текста. В результате расшифрования был получен корректный текст.
* Была изучена основная схема алгоритма шифрования RSA. После генерации открытых и закрытых ключей было произведено шифрование текста. Затем текст был расшифрован. Результат расшифровки совпал с исходным текстом, можно сделать вывод, что расшифрование корректно.
* Также в ходе лабораторной работы была исследована зависимость времени шифрования и расшифрования в зависимости от длины ключа. Для этого были сгенерированы 4 ключа различной длины (512, 768, 1024 и 2048 бит). Можно сделать вывод, что шифрование, происходит быстрее расшифрования, но при этом обе операции выполняются достаточно быстро. Самые большие затраты времени были при самой большой длине ключа.
* В ходе изучения атаки грубой силы на RSA был успешно факторизован модуль n, что привело к успешной атаке. В итоге было получено корректное расшифрованное сообщение.
* Был изучен процесс атаки на гибридную криптосистему. При рассмотрении процесса демоприложении атака завершилась успешно.