**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. 6381 |  | Шевелева А.М. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2019

Цель работы.

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

Основные теоретические положения

Протокол Диффи-Хеллмана

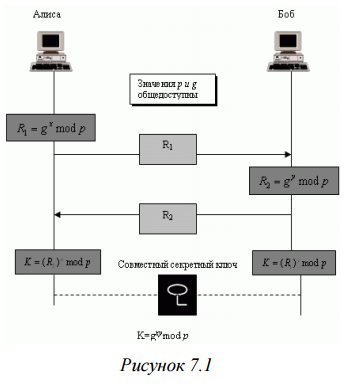
1. Запустите утилиту Indiv.Procedures->Protocols->Diffie-Hellman demonstration… и установите все опции информирования в ON.

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.

Основные параметры 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.

Протокол Диффи-Хеллмана состоит из следующих операций:

1. Устанавливаются открытые параметры p, g:

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

b) g – первообразный корень по модулю p.

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

3. На каждой стороне вычисляется открытый ключ:

a) 𝑅1 = 𝑔𝑥𝑚𝑜𝑑 𝑝,

b) 𝑅2 = 𝑔𝑦𝑚𝑜𝑑 𝑝.

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

𝐾 = 𝑅2𝑥𝑚𝑜𝑑 𝑝 = 𝑅1𝑦𝑚𝑜𝑑 𝑝

Обобщенная схема шифра RSA

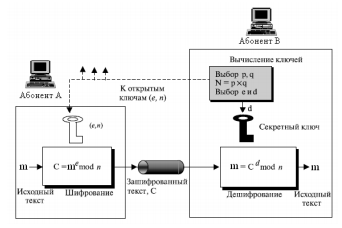


Схема RSA представляет собой блочный шифр, в котором и открытый, и шифрованный текст представляются целыми числами из диапазона от 0 до n-1 для некоторого n.

Алгоритм шифрования RSA состоит из следующих операций:

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 φ(n).

d) Вычисление 𝑑: 𝑒 ∗ 𝑑 = 1 𝑚𝑜𝑑 𝜑(𝑛).

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

2. Шифрование:

a) Открытый текст разбивается на блоки 𝑚𝑖 : 𝑚𝑖 < 𝑛.

b) Каждый блок открытого текста преобразуем в шифротекст по формуле: 𝑐𝑖 = 𝑚𝑖𝑑𝑚𝑜𝑑 𝑛

3. Расшифровка:

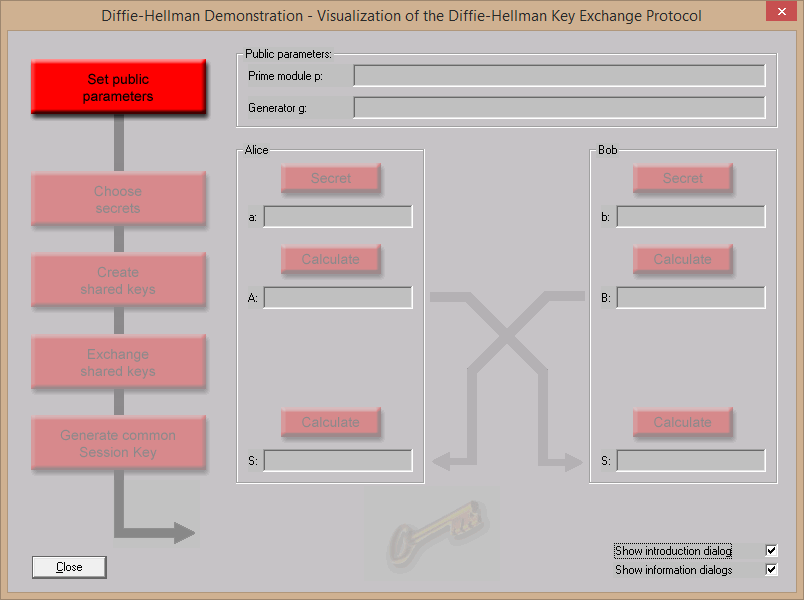
a) Шифротекст разбивается на блоки с𝑖 : с𝑖 < 𝑛.

b) Каждый блок шифротекста преобразуем в открытый текст по формуле: m𝑖 = c𝑖𝑑𝑚𝑜𝑑 𝑛

Выполнение работы.

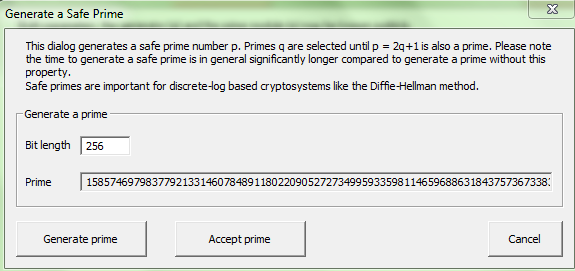
Схема протокола, реализованная в Cryptool.

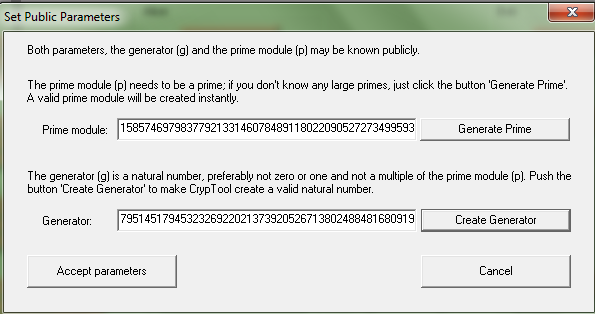
Запустим утилиту *Indiv. Procedures->Protocols->Diffie-Hellman demonstration…* и установим все опции информирования в ON

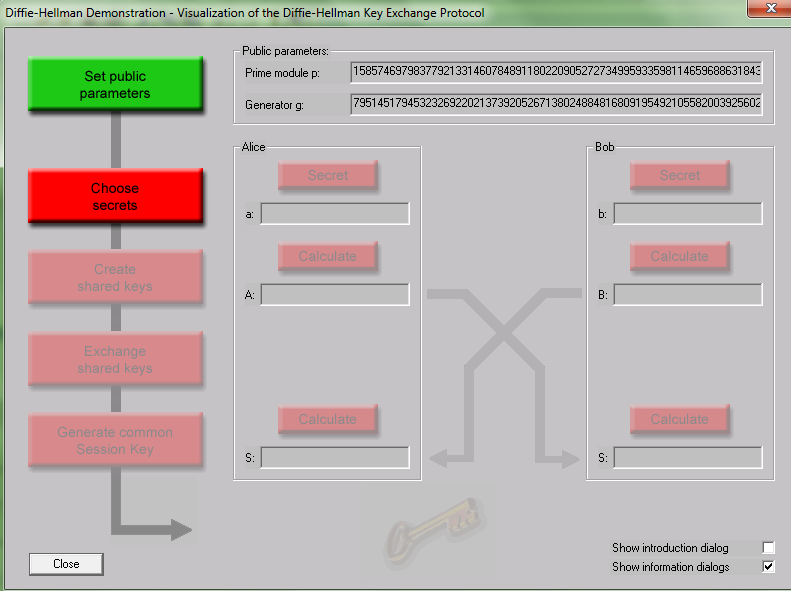


Выполним последовательно все шаги протокола

На данном шаге генерируем p (prime) и g (generator):

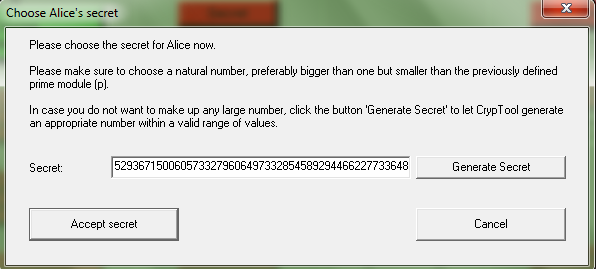




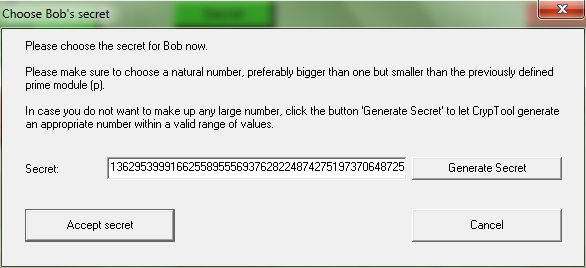


На следующем шаге генерируем секрет для Alice и Bob:

Секрет Alice:

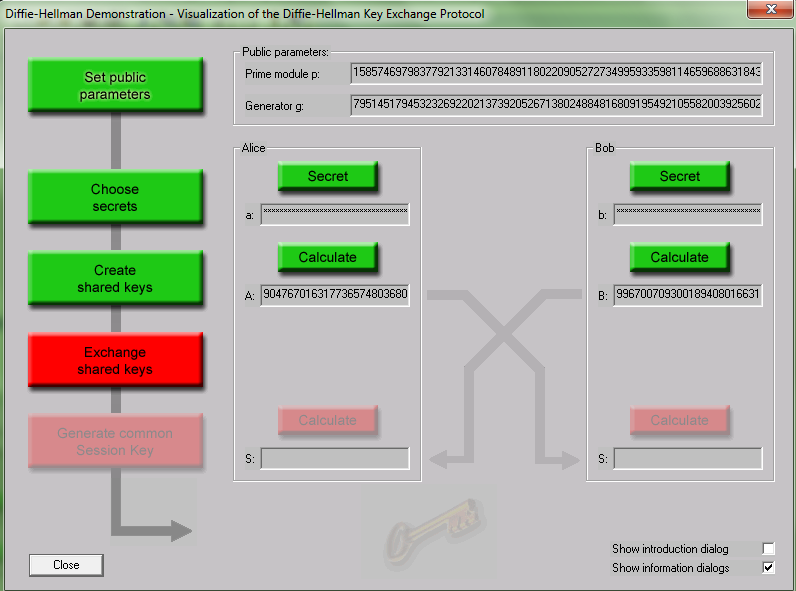


Секрет Bob:



На шаге 3 генерируются открытые ключи для обмена между Alice и Bob:

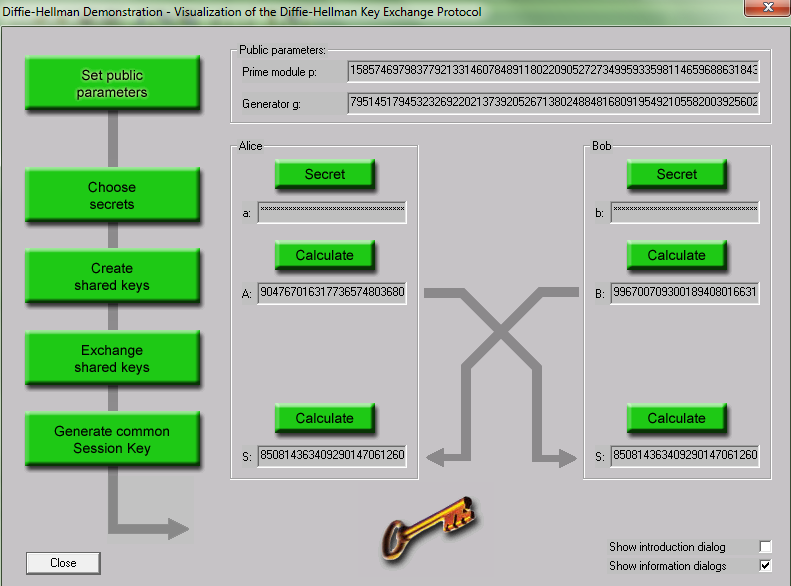
Результат генерации открытых ключей:

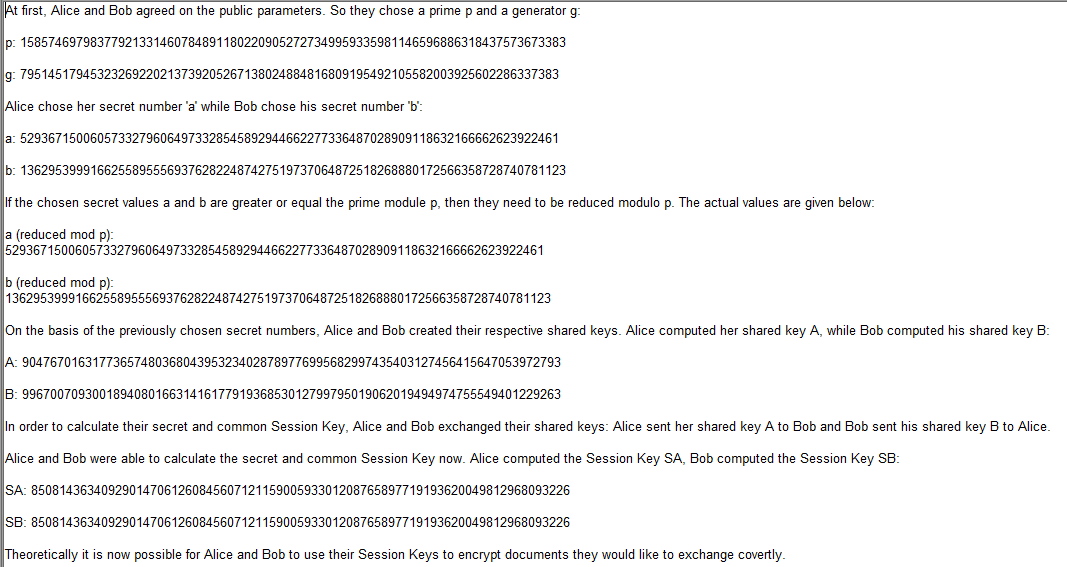


Стадия обмена открытыми ключами.

На последнем шаге создаём закрытый ключ.

Процедура прошла успешно: закрытые ключи, сгенерированные Alice и Bob, совпали.

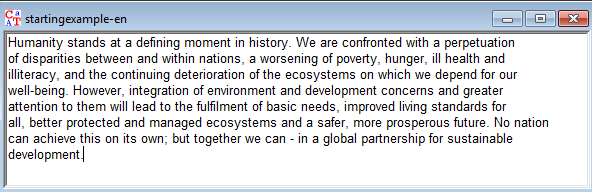




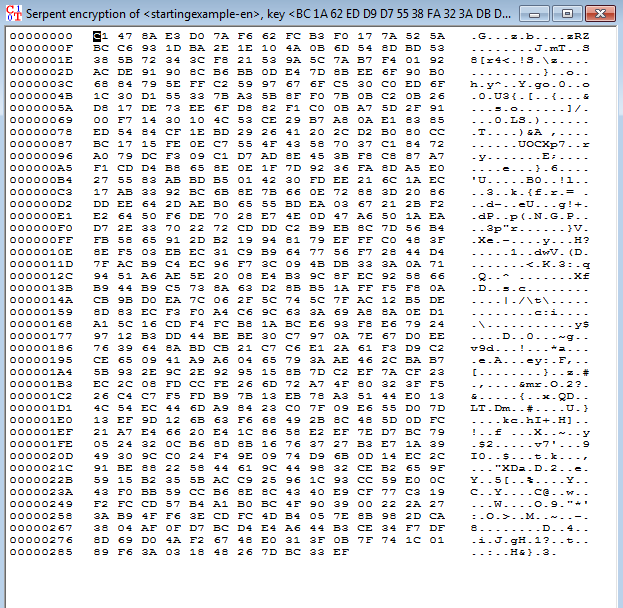
Используем полученный общий ключ для зашифровки и расшифровки произвольного сообщения. В качестве алгоритма шифрования используем симметричный шифр Serpent (с длиной ключа 256 бит). Однако для его использования нужно предварительно перевести полученный ключ из десятичной системы исчисления в шестнадцатеричную.

Результат конвертации: BC1A62EDD9D75538FA323ADBDD9591D18128E60C1F75121ACFE63DFAEBC6B62A

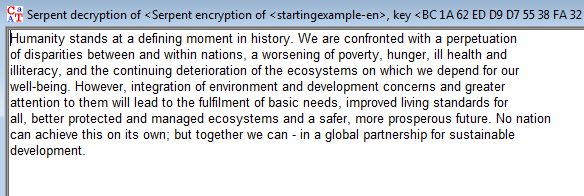
В качестве сообщения выступил следующий текст:



Шифротекст:



Результат дешифрации:



Шифр RSA

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

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

Сгенерируйте открытый и закрытый ключи.

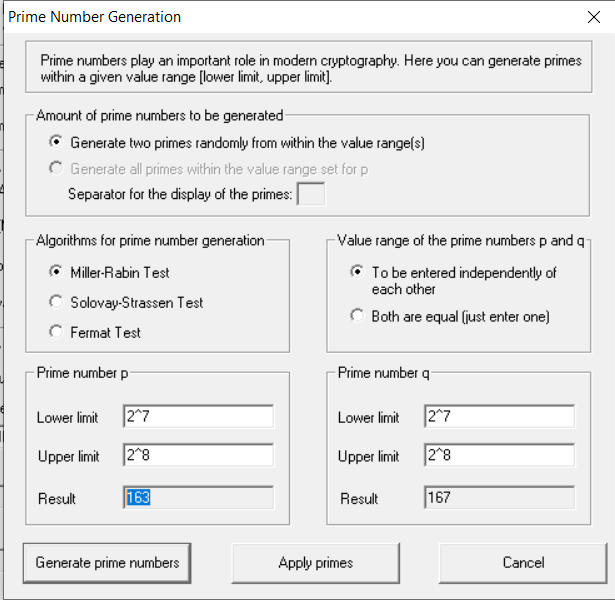
Зашифруйте сообщение. Сохраните скриншот результата.

Расшифруйте сообщение. Сохраните скриншот результата.

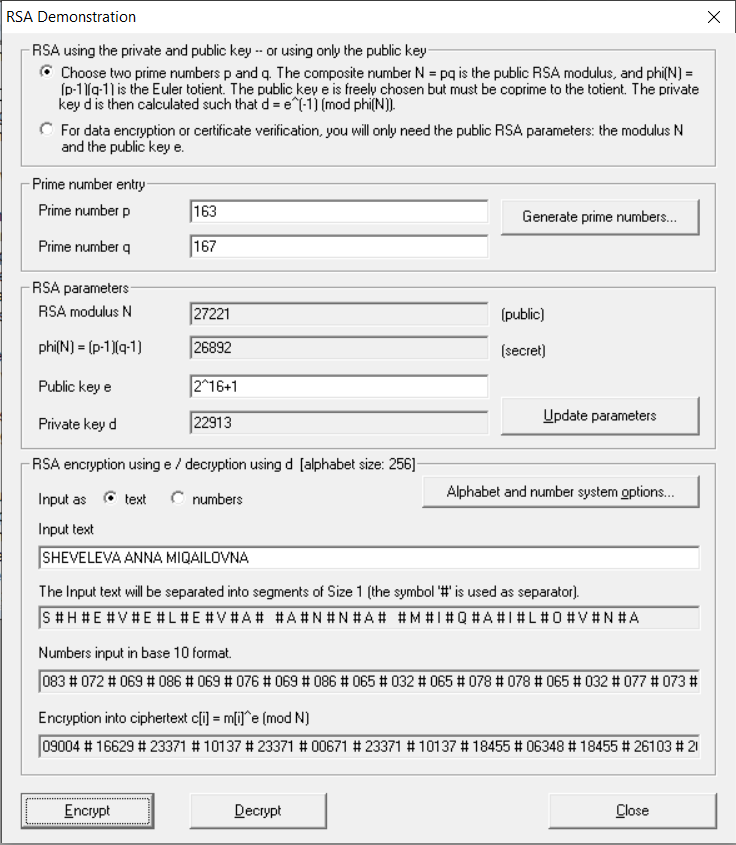
Для изучения шифра RSA воспользуемся утилитой *Indiv. Procedures->RSA Cryptisystem->RSA Demonstration…*

В качестве обрабатываемого сообщения зададим ФИО и сгенерируем открытый и закрытый ключи.

Результат генерации ключей:



Результат шифрования:



Дешифрация:



Исследование шифра RSA

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

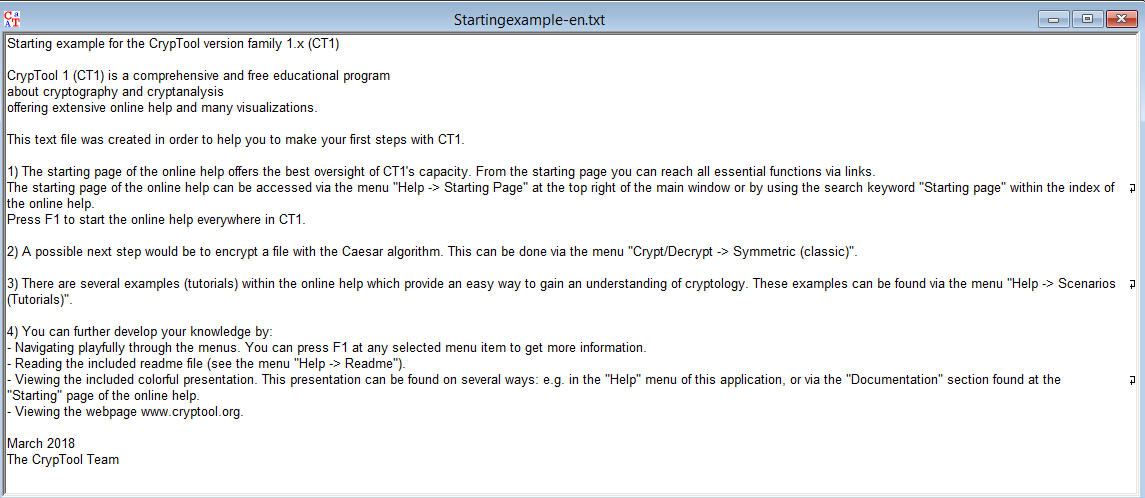
2. Сгенерировать пары ассиметричных RSA-ключей утилитой Digital Signatures->PKI->Generate/Import Keys с различными длинами (4 варианта).

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.

Исходный текст



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

|  |  |  |
| --- | --- | --- |
| Длина ключа | Время зашифровки, c | Время расшифровки, c |
| 512 | 0 | 0.034 |
| 768 | 0 | 0.069 |
| 1024 | 0 | 0.222 |
| 2048 | 0 | 1.793 |

Атака грубой силы на RSA

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

2. Установите переключатель в режим «Choosetwoprime…».

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->RSA Demonstration и установите переключатель в режим «Fordata encryption…»

7. Выполните факторизацию модуля n командой Factorize…

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

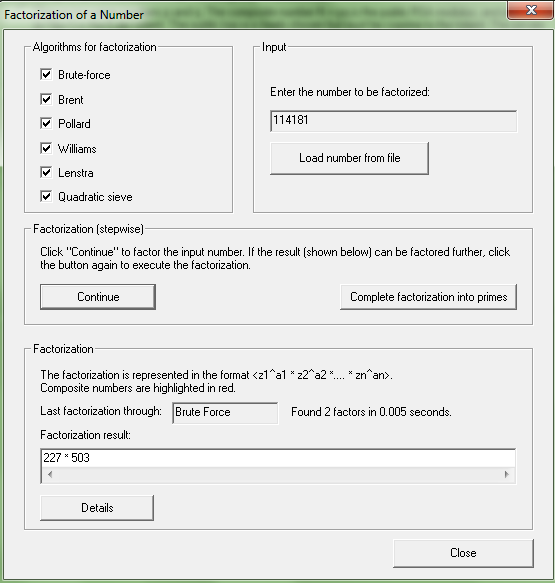
Исходные данные для атаки, полученные от коллеги:

N=114181

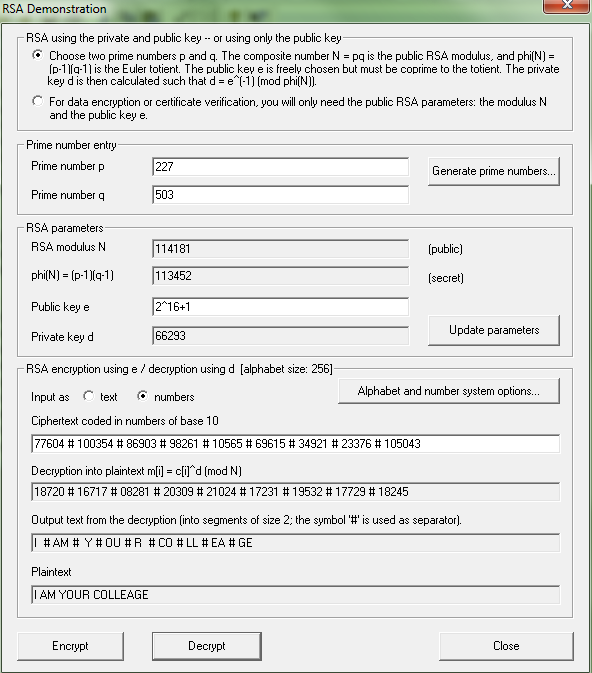
e=2^16+1

Шифротекст: 77604 # 100354 # 86903 # 98261 # 10565 # 69615 # 34921 # 23376 # 105043

Результат факторизации:



После выполнения процедуры дешифрации с учётом всех параметров получено следующее сообщение:



Имитация атаки на гибридную криптосистему

Задание

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

2. Запустите утилиту Analysis->AsymmetricEncr…->Side-Channel attackon «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.

Шифрование при помощи гибридной модели осуществляется следующим образом:

1. Сообщение шифруется симметричным секретным ключом.

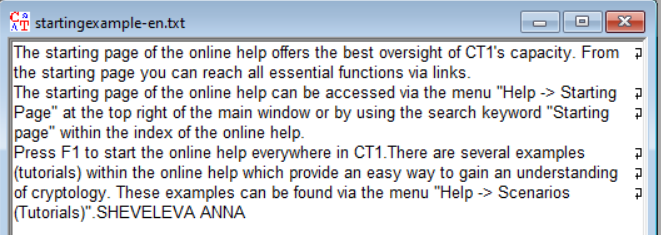
2. Секретный ключ шифруется открытым ключом.

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

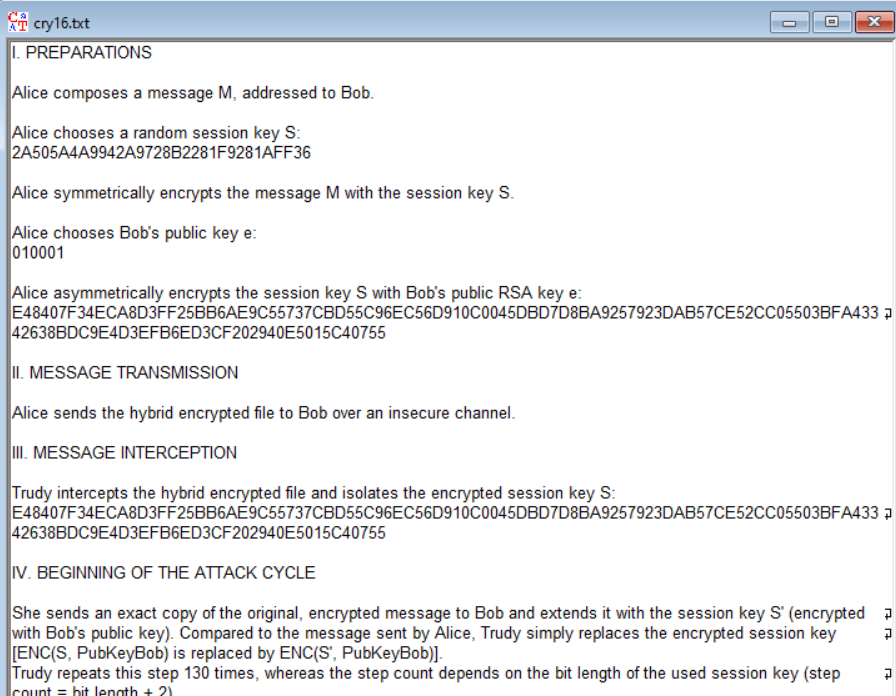
4. Получатель сначала расшифровывает секретный ключ, затем расшифровывает секретным ключом шифротекст сообщения.

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.

Текст передаваемого сообщения:



Лог-файлы участников протокола:



Выводы.

Были получены следующие основные выводы:

1. Протокол Диффи-Хеллмана − криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. K=gab mod p, числа g и p несекретны, a и b секретны и сгенерированы получателем и отправителем отдельно друг от друга.

2. Ассиметричный шифр RSA включает в себя генерацию ключа и само шифрование с использованием математических функций. Схема RSA представляет собой блочный шифр, в котором и открытый, и шифрованный текст представляются целыми числами из диапазона от 0 до n-1 для некоторого n.

Данный шифр используется для передачи симметричных сессионных ключей, так как алгоритм применим только для сообщений, не превосходящих длиной длину ключа из-за сложности операций шифрования.

3. Были сгенерированы 4 ключа различной длины, на которых исследовалась зависимость времени шифрования и расшифрования в зависимости от длины ключа.

|  |  |  |
| --- | --- | --- |
| Длина ключа | Время зашифровки, c | Время расшифровки, c |
| 512 | 0 | 0.034 |
| 768 | 0 | 0.069 |
| 1024 | 0 | 0.222 |
| 2048 | 0 | 1.793 |

Время расшифровки прямо пропорционально размеру ключа шифра.

4. Атака грубой силы основана на переборе простых чисел, чтобы найти разложение числа. Для этого требуется перебрать не более чем чисел.

5. Была исследована имитация атаки на гибридную криптосистему. Можно сделать вывод, что злоумышленник может извлечь секретный ключ, изменяя значения зашифрованного ключа, отправляя запрос на сервер и анализируя его ответ. Но этого можно избежать, проверяя целостность данных на сервере.