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

ОТЧЕТ

по лабораторной работе №7

по дисциплине «Криптография и защита информации»

Тема: Изучение асимметричных протоколов и шифров

Студент гр. 8383 _____ Ларин А.

Преподаватель _____ Племянников А.К.

Санкт-Петербург

2021

Цель работы

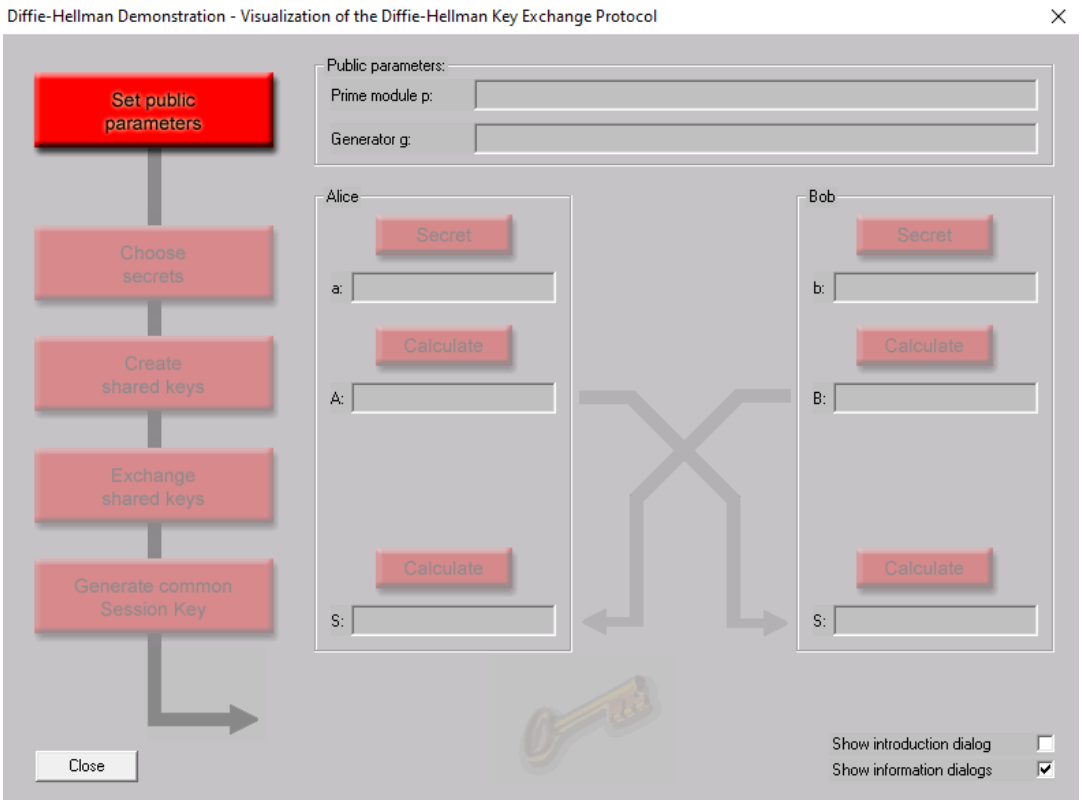
Исследовать протокол Диффи-Хеллмана, шифр RSA и получить практические навыки работы с ними, в том числе с использованием приложения Cryptool 1 и 2.

1. Протокол Диффи-Хеллмана

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
5. расшифровки произвольного сообщения. Шифр выберите самостоятельно.

Выполнение

1. 

2. Взято простое число длиной 512 бит

p =
176155186961158300932057809006104039769658901203065582639342718
634662509281568350719427763002472885080421423996729425429644693
787474277365540570690344929 27

g =
884693076013597300352006373093104283927492894974169339348514522
754608779027472160246723213430297658140187312442186289529131694
533802448055753161466049289 3

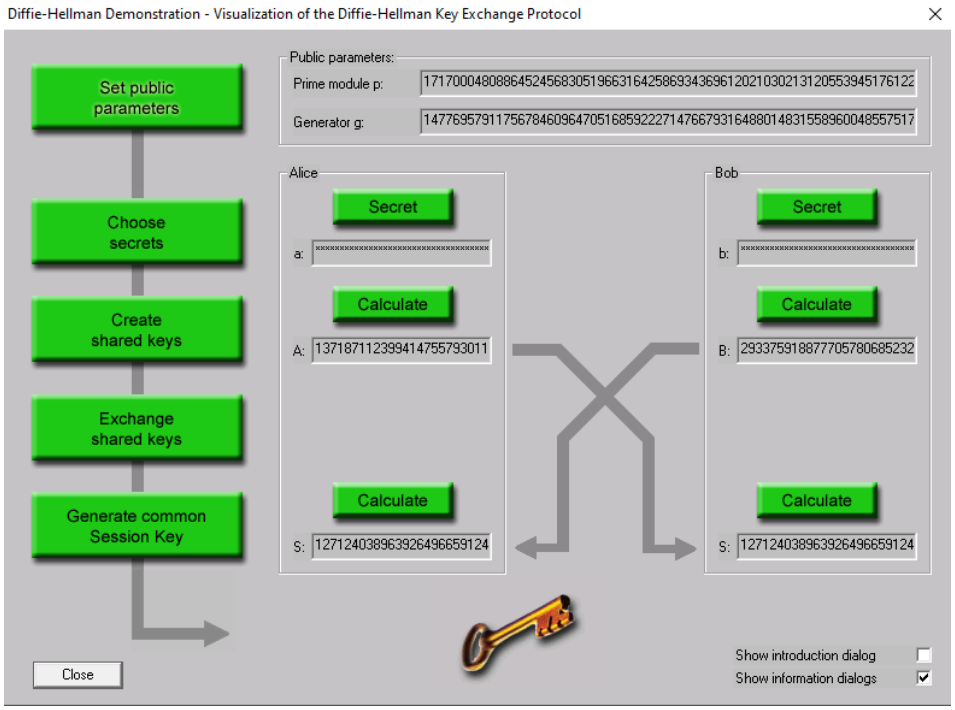
a =
637391219838910720241606235828437788892010630976952090829851060
125851088326949354696349753593970678734540943802803451139345254
093168887309246094153719364 4

b =
118268643592312616110524044658982955816283713483652446726646827
054134391444667637130853864173715914799635468175603585134302864
610611992416413355336488627 5

A =
951508424412132566465965888925252973440016955731200189526006081
262013533191111798426168369273278007487625368035954602730861638
190187166552936134968336482 8

B =
115493431028993142735389368224748114567916397426791305483795024
275447590707182847964122597440773359815736289516073692552922512
814060947524133274634059802 95

S =
123451354940584800197240103742290248348815847642198864111179731
491800276085381678648549713707138508112413899891956976139961444
636387118888702314162148278 9



4. Взят открытый текст larin anton
   Зашифрованый AES текст 54 CE F6 D9 F2 F1 1D 1F 51 83 6D C7 20 9E 5D B8
   После расшифровки получен текст larin anton

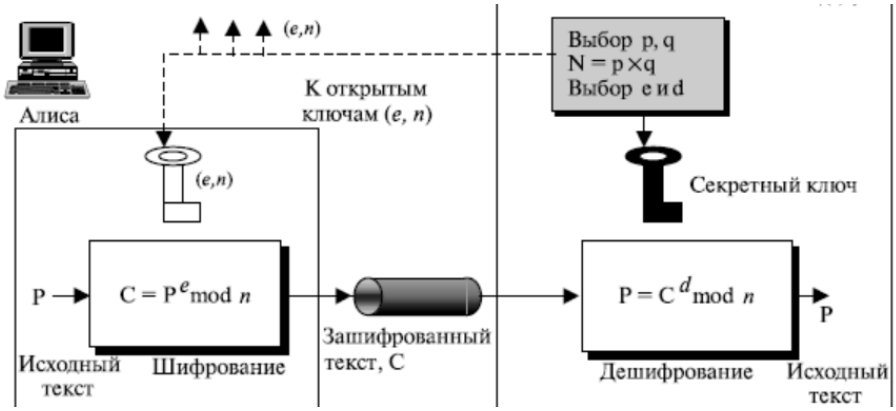
2. Шифр RSA

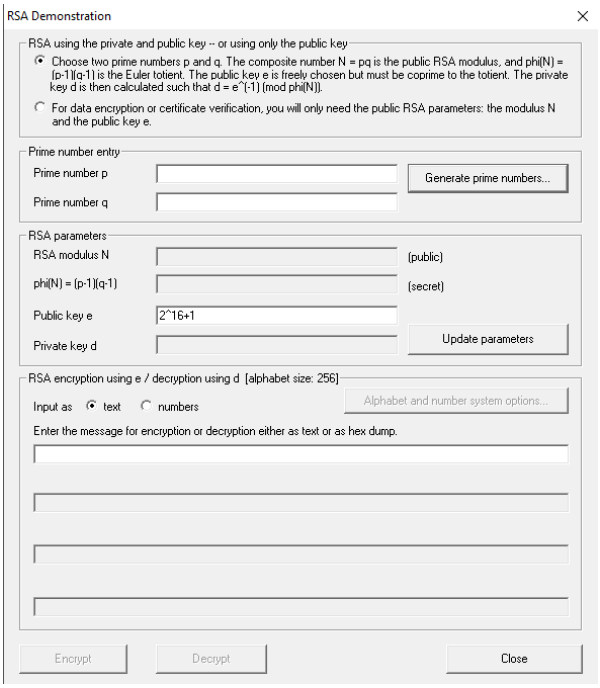
Задание

1. Запустите утилиту Indiv.Procedures→RSA Cryptisystem→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.

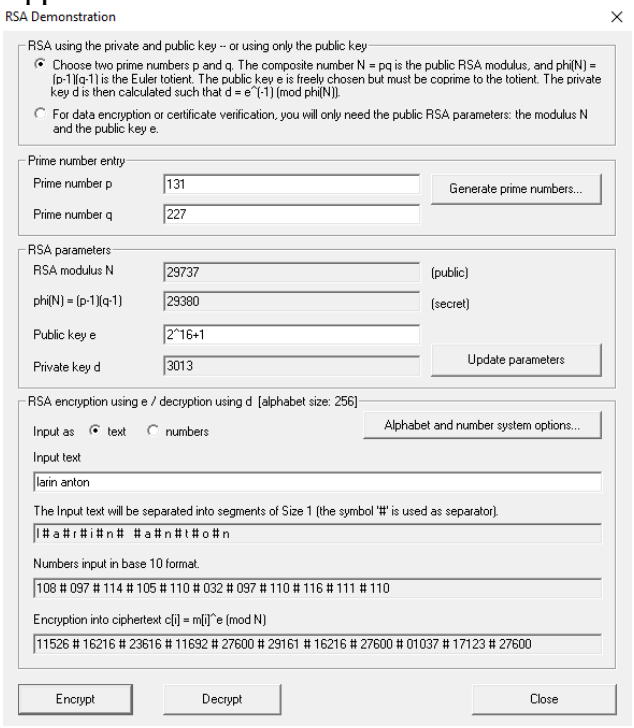
Выполнение

1.

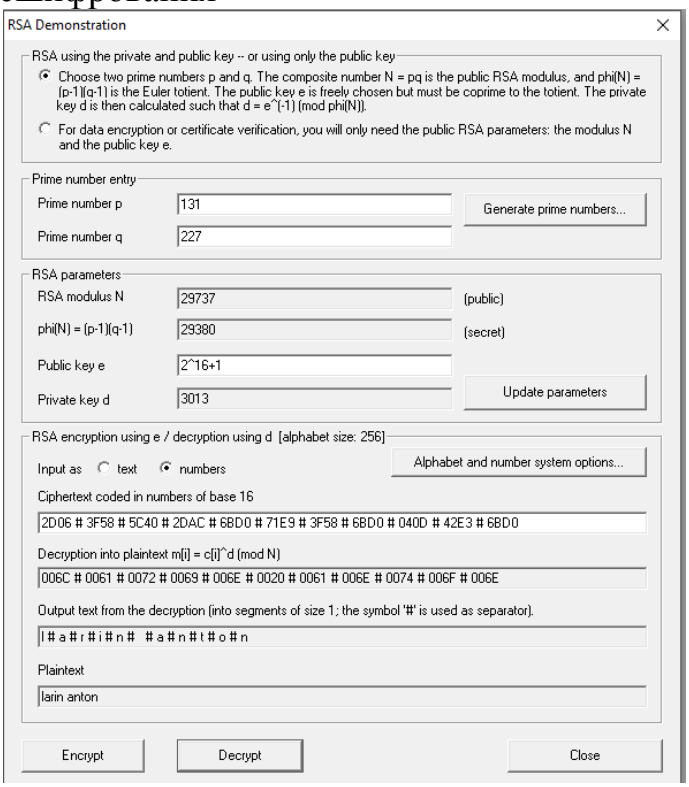




2. В качетсве обрабатываемого текста взят «larin anton»
3. p = 131
   q = 227
   n = 29737
   $\varphi(n) = 29380$
   e = 2^16+1
   d = 3013
4. Результат зашифрования:



5. Результат расшифрования



6. Исходный и расшифрованных текст совпадают

3. Исследование шифра RSA

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 Зафиксировать время зашифровки.
5. Проверить корректность расшифровки. Зафиксировать скриншоты результата.

Выполнение

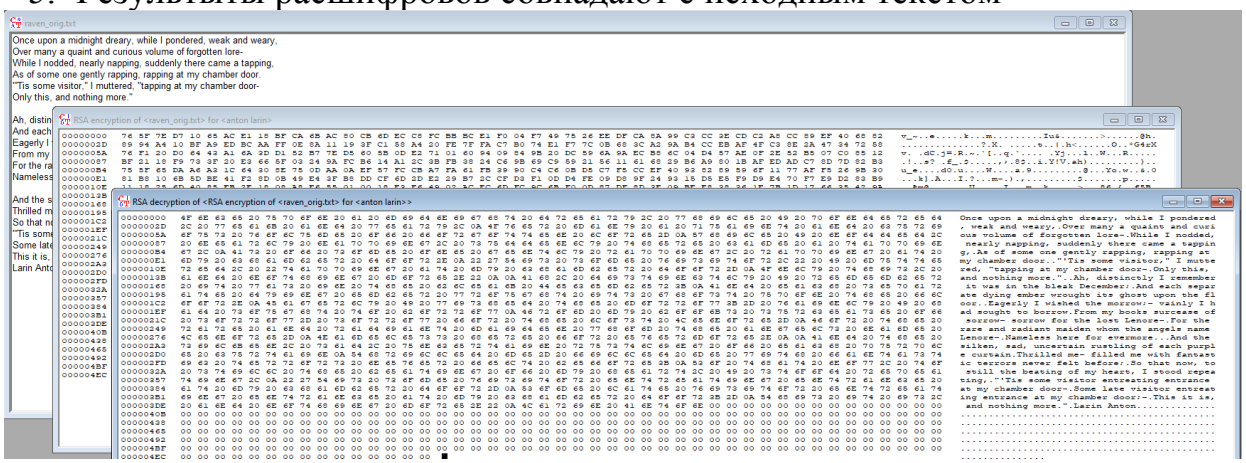
1. Взят исходный текст с тремя параграфами поэмы Raven. и ФИ в конце Его размер ~ 1000 символов (1021 байт)
2. Сгенерированы ключи длиной 512 байт (2.124 сек.), 768 (0.078), 1024 (0.157), 2048 (1.797)
3. Зашифрован один открытый текст разными ключами

	512	768	1024	2048
	0	0	0	0

4. Расшифрован один открытый текст разными ключами

	512	768	1024	2048
	0	0.014	0.016	0.046

5. Результыты расшифровов совпадают с исходным текстом



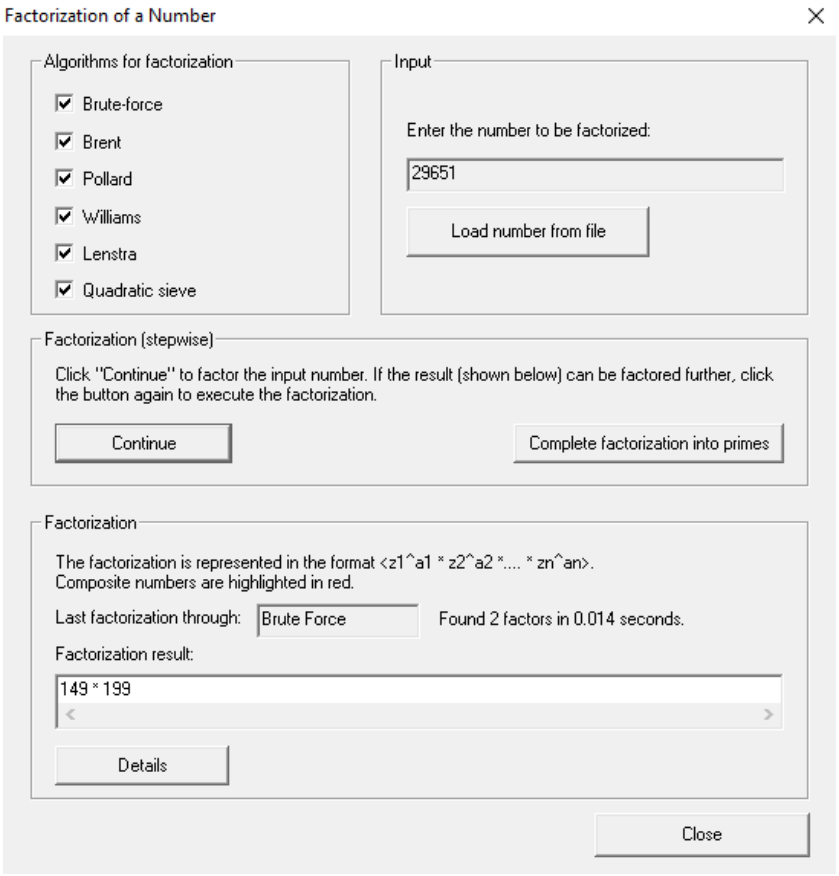
4. Атака грубой силы на RSA

Задание

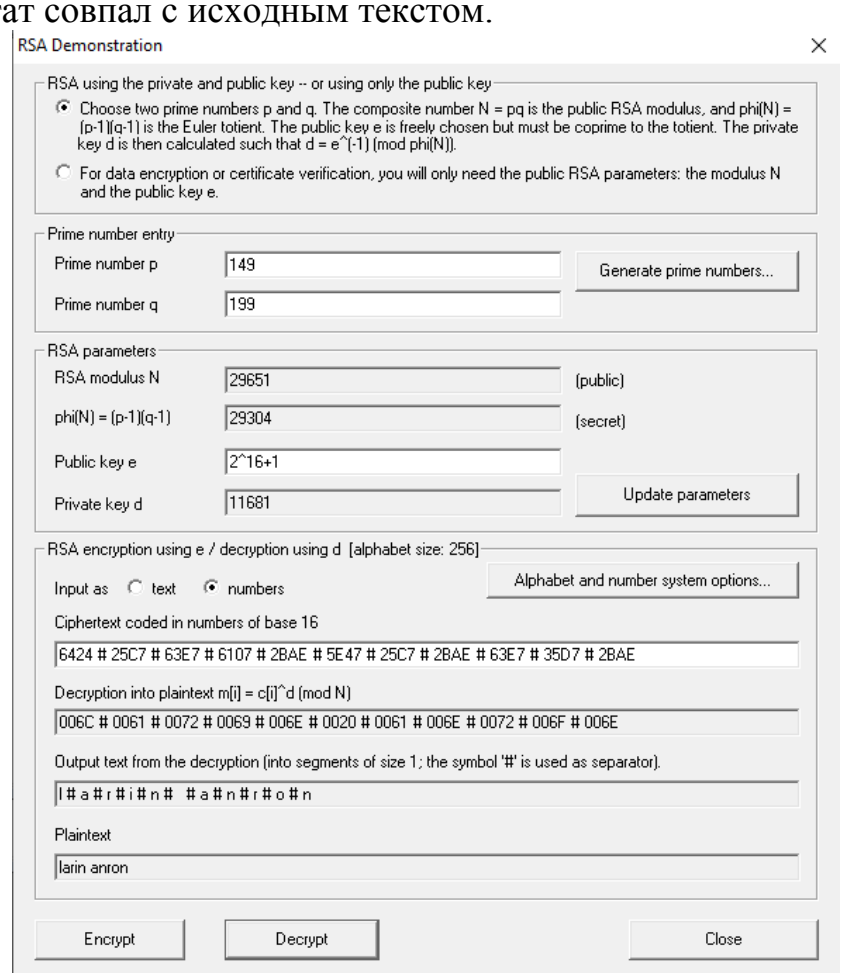
1. Запустите утилиту Indiv.Procedures→ RSACryptosystem→ RSA Demonstration
2. Установите переключатель в режим «Choose two prime...».
3. Выберите параметры p и q так, чтобы n=pq> 256.
4. Задайте открытый ключ e.
5. Зашифруйте произвольное сообщение и передайте его вместе c, n и e коллеге. В ответ получите 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.

Выполнение

1. Запущена утилита
2. Выставлен параметр two primes
3. p = 199
   q = 149
   n = 29651
   d = 11681
4. e = 2^16+1
5. Задано сообщение «larin anton»
   Получено зашифрованное сообщение:
   6424 # 25C7 # 63E7 # 6107 # 2BAE # 5E47 # 25C7 # 2BAE # 4F3E # 35D7 # 2BAE
6. На вход получаем публичный ключ e, n
7. Факторизация числа n = 29651 даёт исходные 149, 199 (0.014)



8. Полученые числа использованы для расшифровки шифротекста. Результат совпал с исходным текстом.



5. Имитация атаки на гибридную криптосистему

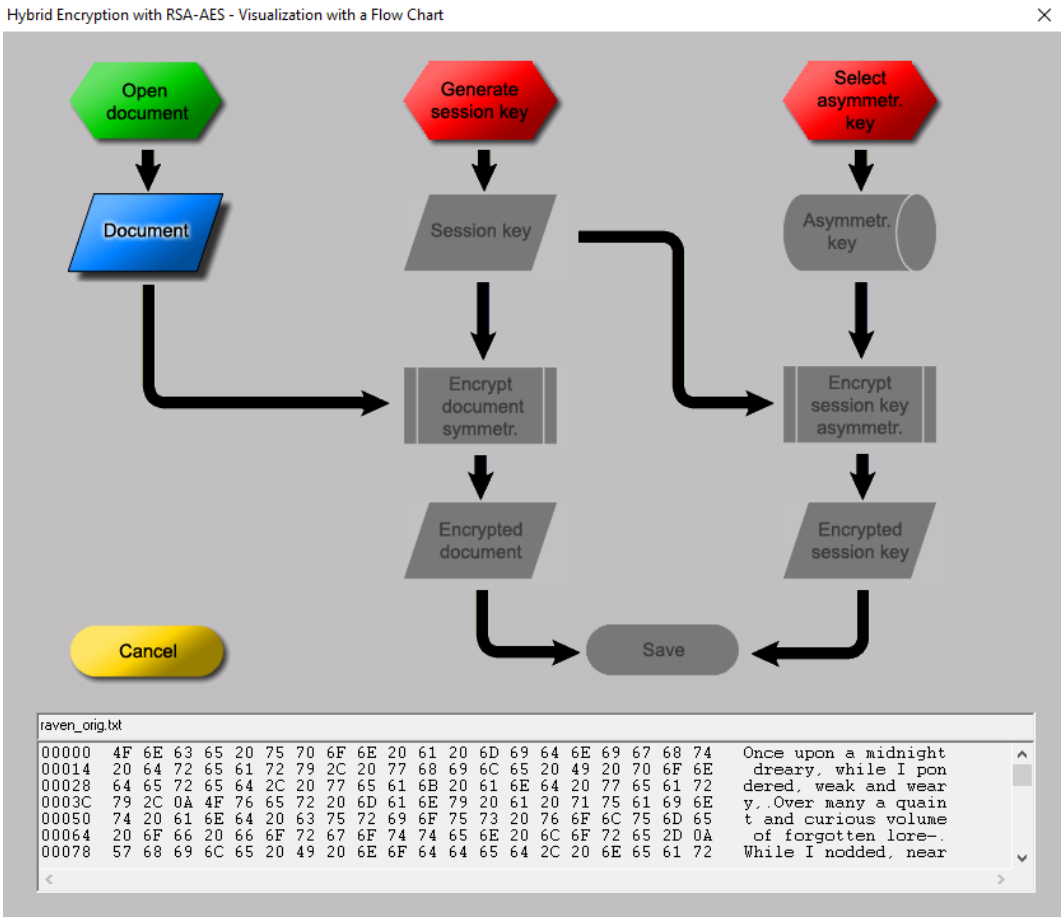
Задание

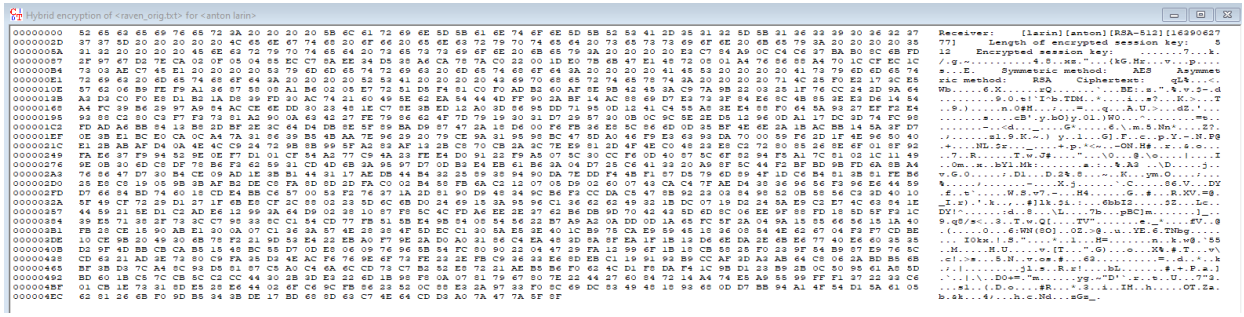
1. Подготовьте текст передаваемого сообщения на английском с вашим именем в конце.
2. Запустите утилиту Analysis->Asymmetric Encr...->Side-Channel attack on «Textbook RSA»...
3. Настройте сервер, указав в качестве ключевого слова ваше имя, используемое в конце текста.
4. Выполните последовательно все шаги протокола.
5. Сохраните лог-файлы участников протокола для отчета.

Выполнение

1. Выбраны те же три параграфа и larin anton в конце
2. 

3. В качестве ключевого слова указано Anton
4.





5. Получившийся лог
   I. PREPARATIONS

   Alice composes a message M, addressed to Bob.

   Alice chooses a random session key S:
   328783660C28B17CB14CBFCFAD815A66

   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:
   6676643AA8D34E6BB06AD415892BF55CF4C27C7DD6F36DA9FADA461F0CC7ACC83C772D760C24A6F97018B41AE37D45A5C7F88206A8987AC

0E35EEA65C2D9E686402857B7FD15556C407E9640BB3BC4EE236A3D44
33E8BD156FFC7F8BC5EA657A

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:
6676643AA8D34E6BB06AD415892BF55CF4C27C7DD6F36DA9FADA461
F0CC7ACC83C772D760C24A6F97018B41AE37D45A5C7F88206A8987AC
0E35EEA65C2D9E686402857B7FD15556C407E9640BB3BC4EE236A3D44
33E8BD156FFC7F8BC5EA657A

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.

1. Исследован протокол Диффи-Хеллмана, для криптопреобразования на основе открытых ключей. Он позволяет обеим сторонам общения получить идентичную копию секретного ключа. Вручную проделаны шаги для обмена при поощи Cryptool. В конце у обеих сторон оказались идентичные ключи S. При помощи полученного ключа произведена зашифровка открытого текста.
2. Изучена работа шифра RSA - асимметричного блочного шифра. При помощи Cryptool были проделаны шаги алгоритма генерации открытого(n, e) и закрытого(d) ключа, зашифровки и корректной расшифровки сообщения
3. Исследован шифр RSA. Выбраны различные длины ключей (512, 768, 1024, 2048 бит). С их помощью зашифрован и расшифрован один и тот же текст длиной 1021 символ. По временным затратам можно сделат ьвывод, что время зашифровки и расшифровки зависит от длины ключа не более чем линейно, и не играет решайющей роли, т. к. все расшифровки выполнены за небольшое время, а зашифровки за принеблежимо малое.
4. Был изучен принцип работы атаки на RSA методом грубой силы. Он заключается в факторизации n, т. е. разложении его на p, q такие, что p*q=n, что позволит восстановить закрытый ключ. Задача факторизации является вычислительно сложной, что означает, что для большого n она не выполнима ра разумное время. Результат для малоых p,q получен за 0.014 и был корректен.
5. Была изучена атака на гибридную криптосистему. Она относится к классу атак man-in-the-middle, подразумевающая третье лицо, прослушивающее открытый канал, по которому передуются сообщения (предп. зашифрованные). При помощи инструмента CrypTool была произведена пошаговая атака. В качестве открытого текста взяты первые три параграфа поэму Raven и строка Larin Anton, которая использовалась для

проверки верности расшифрования. Атака полагает возможность прослушивания, прехвата, модифицирования сообщения и прослушивания из побочного канала, о том было ли сообщение корректно расшифровано (по содержанию ключевого слова). Атака заключается в замены старших бит корверта шифровкой ключа, сдвигом влево и посылкой серверу. Если ответ сервера положитльный, то старший бит нулевой. Дальше сдвигая сообщение и проваряя ответы сервера можно восстановить всё сообщение, что было проверено демонстрацией в Cryptool.