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

ОТЧЁТ

по лабораторной работе №7
по дисциплине «Криптография и защита информации»
Тема: Изучение ассиметричных шифров

Студент гр. 6304 _____ Корытов П.В.
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.

1. Протокол Диффи-Хеллмана

1.1. Формулировка задания

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. Выполнение задания

1. Запущена указанная утилита. Скриншот приведен на рис. 1

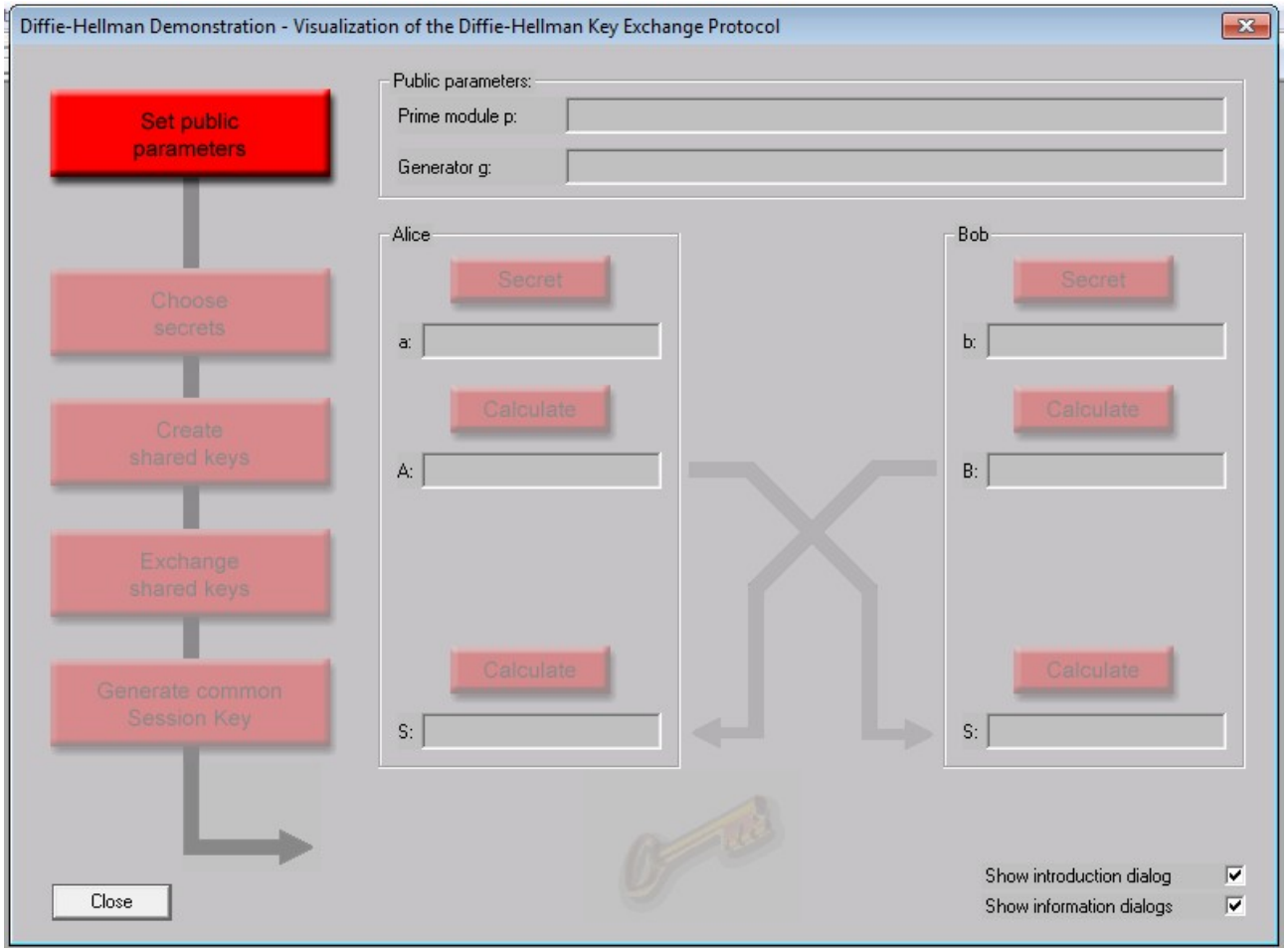

Рисунок 1. Утилита демонстрации протокола Диффи-Хеллмана

2. Сгенерированы параметры p (целое число) и g (генератор — натуральное число, не взаимно простое с p)

   `p = 164 459 422 689 066 243 011 729 968 057 438 442 455 606 356 397 837 044 700 733 361 991 165 383 163 799;`

   `g = 90 781 356 746 102 774 580 779 638 749 722 545 280 765 577 832 398 664 019 008 562 895 851 301 528 787`

   p и g известны всем.
3. Сгенерированы секреты: `a = 34 596 549 621 750 295 858 653 977 034 480 662 835 051 928 581 964 288 778 519 325 445 061 945 869 844;`

   `b = 54 016 829 575 119 166 230 209 367 614 889 841 297 334 189 509 706 697 680 060 831 553 422 514 175 088`

   a — секрет Алисы, b — секрет Боба. Требования к секретам: $1 < a < p$, $1 < b < p$.
4. Вычислены общие ключи:

$$A = g^a \bmod p; B = g^b \bmod p$$

A = 34 467 817 907 976 045 230 452 302 928 382 669 365 886 312 181 386 385 984 225 792 489 434 184 933 013;

B = 142 731 903 542 858 044 148 169 623 036 564 507 677 299 220 545 763 907 701 621 198 404 943 777 173 031

5. Произведен обмен ключами: Боб получает A, Алиса — B.
6. Стороны вычисляют сессионный ключ.

$$S = B^a \bmod p = (g^b)^a \bmod p = (g^a)^b \bmod p = A^b \bmod p$$

Таким образом, на обеих сторонах получается общий ключ.

S = 63 200 196 764 079 390 461 001 096 815 969 006 477 048 291 593 113 196 450 925 629 549 919 736 524 995

На рис. 2 представлены результаты работы

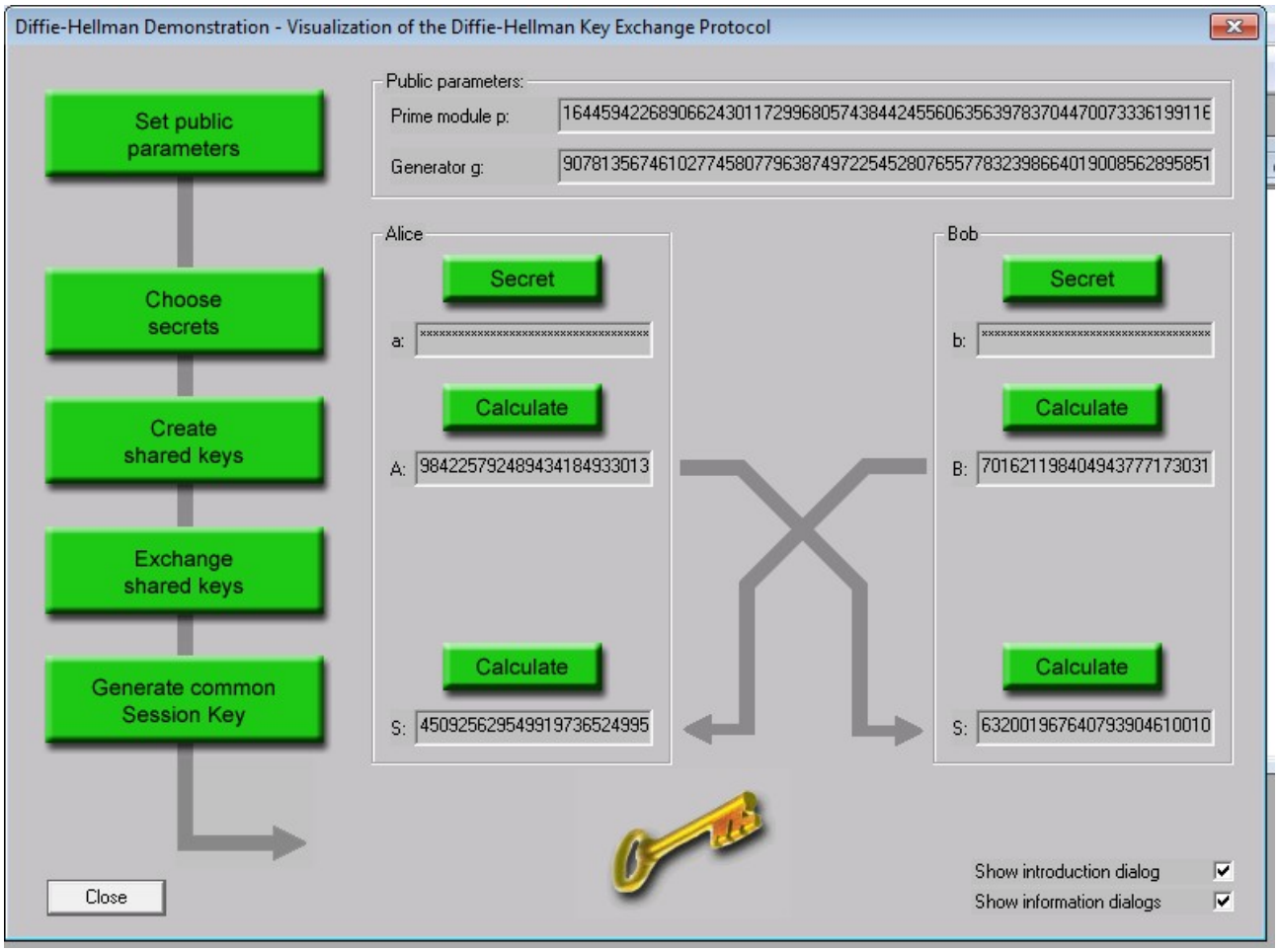

Рисунок 2. Результаты работы

Логи работы в приложении А.

2. Шифр RSA

2.1. Описание шифра

1. Вычисление ключей:
   (a) Генерация двух больших простых чисел p, q (держатся в секрете)
   (b) $n = p \bullet q$
   (c) Выбор взаимо просто $e < n$, взаимно простого с $\varphi(n)$
   $\varphi(n)$ — функция Эйлера:

$$\varphi(p) = p - 1; \varphi(p^n) = p^n - p^{n-1},$$

   если p — простое число,

$$\varphi(a) = \varphi(p_1^{n_1}) \dots \varphi(p_k^{n_k}),$$

   если $a = p_1^{n_1} \dots p_k^{n_k}$ — натуральное число.
   (d) Вычисление d из $e \bullet d = 1 \bmod \varphi(n)$
   (e) (e, n) — открытый ключ, d — закрытый ключ
2. Шифрование:
   (a) Открытый текст разбивается на блоки $m_i : m_i < n$
   (b) Каждый блок открытого текста преобразуется в шифротекст по формуле:

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

3. Расшифровка:
   (a) Шифротекст разбивается на блоки $c_i : c_i < n$
   (b) Каждый блок шифротекста преобразуется в открытый текст по формуле:

$$c_i^d \bmod n$$

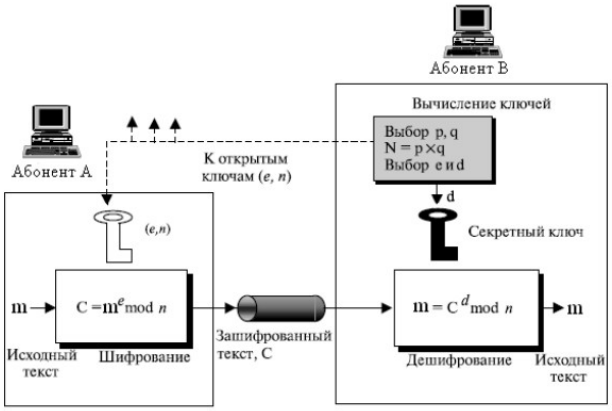

Рисунок 3. Иллюстрация работы шифра RSA

2.2. Формулировка задания

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

2.3. Выполнение задания

- Запущена демонстрационная утилита. Скриншот представлен на рис. 4

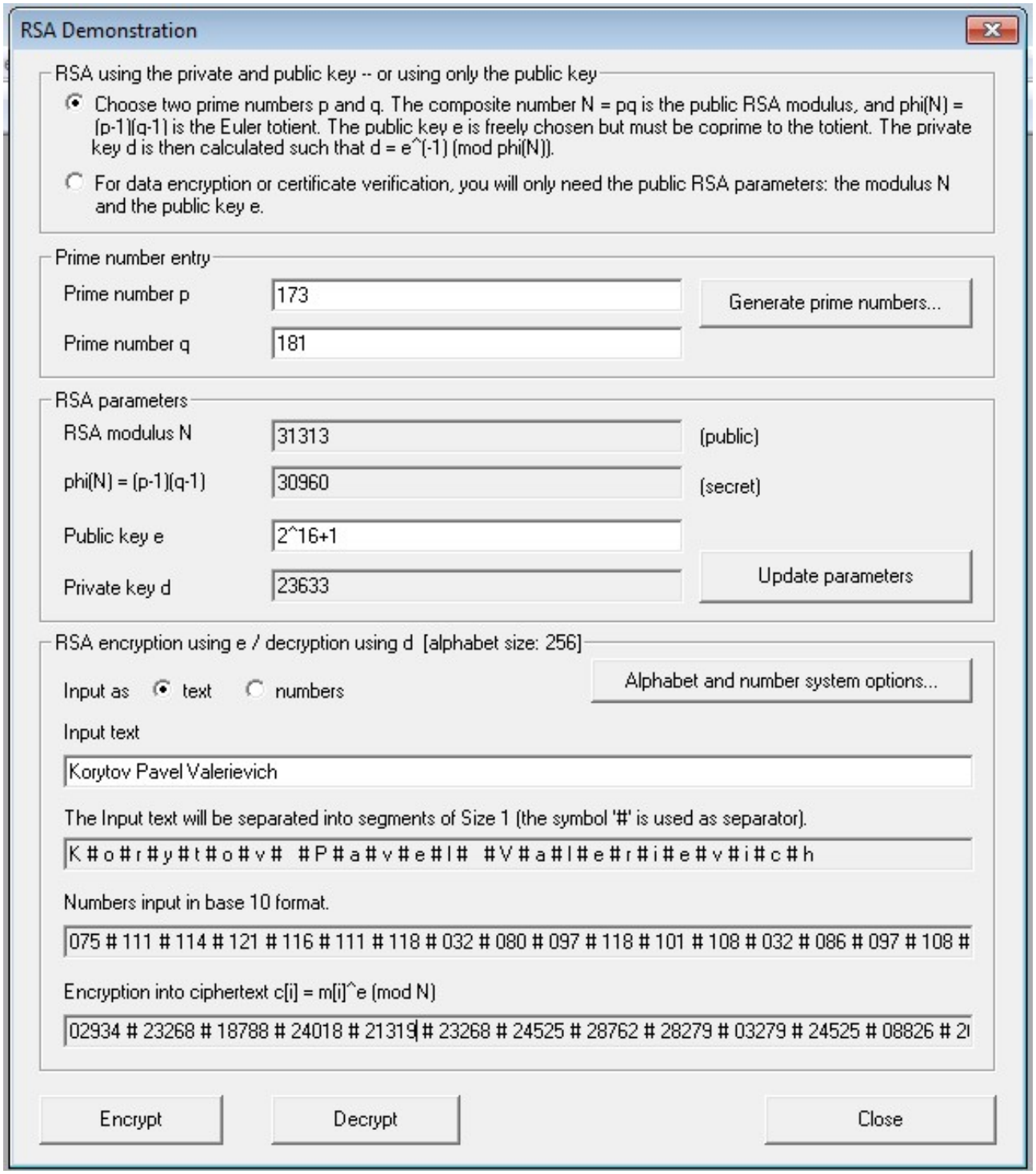

Рисунок 4. Вид утилиты RSA Demonstration

- Сгенерированы небольшие простые числа:

$$p = 173, q = 181$$

Проведены вычисления

$$n = p \bullet q = 31313$$

$$\varphi(n) = (p-1)(q-1) = 30960$$

$$e = 2^{16} + 1$$

$$d = 23633$$

- Произведено зашифрование текста `Korytov Pavel Valerievich`.
  Шифротекст: `02934 # 23268 # 18788 # 24018 # 21319 # 23268 # 24525 # 28762 # 28279 # 03279 # 24525 # 08826 # 20029 # 28762 # 18711 # 03279 # 20029 # 08826 # 18788 # 07910 # 08826 # 24525 # 07910 # 20607 # 14422`
  "#" — разделитель.
- Произведено расшифрование. Результат: `Korytov Pavel Valerievich` — совпадает с исходным текстом.

3. Исследование шифра RSA

3.1. Формулировка задания

1. 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. Выполнение задания

1. Выбран текст на английском языке.
2. Сгенерированы пары ассиметричных ключей с длинами 512, 768, 1024, 2048 бит.

Korytov	Pavel	RSA-1024	16.11.2019 18:09:03	1573916943
Korytov	Pavel	RSA-2048	16.11.2019 18:09:15	1573916955
Korytov	Pavel	RSA-512	16.11.2019 18:07:07	1573916827
Korytov	Pavel	RSA-768	16.11.2019 18:08:53	1573916933

Рисунок 5. Сгенерированные пары

3. Произведено зашифрование и расшифрование одного текста парами с разной длиной.

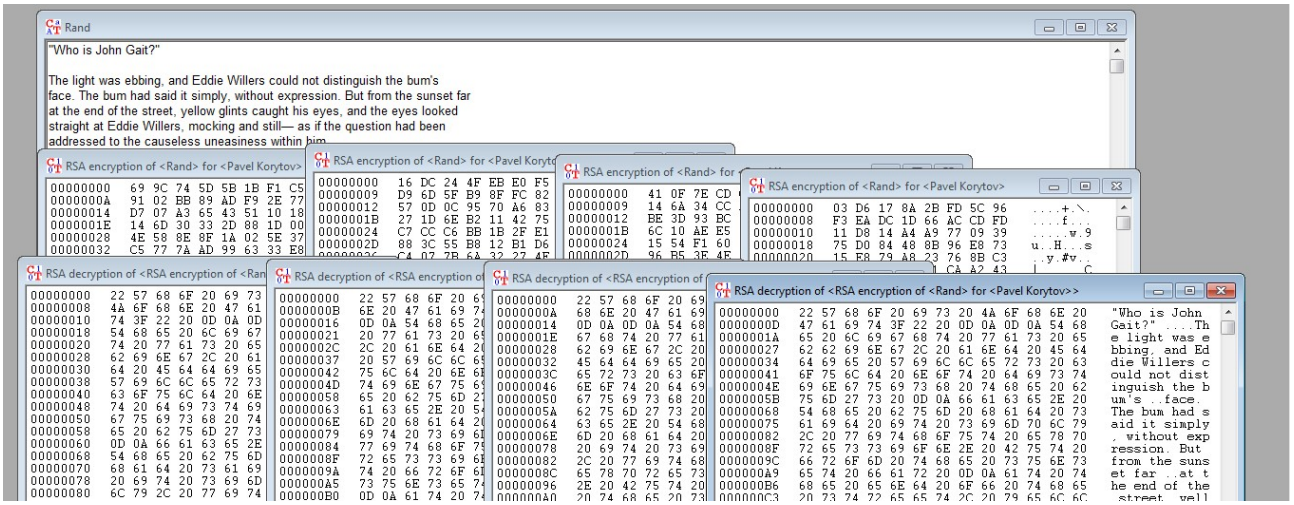

Рисунок 6. Результаты шифрования и дешифрования

Длина ключа (бит)	Время зашифрования (с)	Время расшифрования (с)
512	0.015	0.109
768	0.016	0.168
1024	0.014	0.312
2048	0.031	1.063

4. Атака грубой силы на RSA

4.1. Формулировка задания

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->RSA Demonstration 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. Выполнение задания

1. Произведено зашифрование сообщения:
   I shall choose friends among men, but neither slaves nor masters. And I shall choose only such as please me, and them I shall love and respect, but neither command nor obey. And we shall join our hands when we wish, or walk alone when we so desire.

$$p = 131, q = 211 \Rightarrow n = 27641$$

$$e = 11$$

   Сообщение передано коллеге.
2. Получено сообщение:

```
22927 # 09646 # 29122 # 09646 # 29122 # 25690 # 09646 # 04892 #
30548 # 23971 # 25721 # 12139 # 13191 # 30548 # 28919 # 24345 #
23971 # 28919 # 30548 # 28919 # 24345 # 09646 # 30548 # 12139 #
29122 # 23971 # 25721 # 25721 # 09646 # 12139 # 28919 # 30548 #
29122 # 09676 # 20616 # 13191 # 04892 # 09676 # 28919 # 21239 #
30548 # 13191 # 20616 # 30548 # 09646 # 23971 # 04892 # 28919 #
24345 # 30548 # 09676 # 12139 # 30548 # 28919 # 24345 # 09646 #
30548 # 09676 # 20616 # 24491 # 09676 # 31396 # 09676 # 24491 #
20776 # 23971 # 25721 # 03022 # 30548 # 14895 # 24345 # 13191 #
12139 # 09646 # 30548 # 22172 # 24345 # 13191 # 30548 # 24491 #
09646 # 20616 # 21239 # 30548 # 09676 # 20616 # 24491 # 09676 #
31396 # 09676 # 24491 # 20776 # 23971 # 25721 # 30548 # 04892 #
09676 # 27523 # 24345 # 28919 # 12139 # 26239 # 30548 # 03072 #
23971 # 20616 # 20616 # 13191 # 28919 # 30548 # 03072 # 25721 #
23971 # 09676 # 29122 # 30548 # 28919 # 13191 # 30548 # 25690 #
```

```
09646 # 30548 # 24491 # 09646 # 18680 # 09646 # 20616 # 24491 #
09646 # 04892 # 12139 # 30548 # 13191 # 18680 # 30548 # 29122 #
09676 # 20616 # 13191 # 04892 # 09676 # 28919 # 09676 # 09646 #
12139 # 03022
```

$$n = 32111, e = 5$$

3. Проведена факторизация n: $n = 163 \bullet 197$. Произведено дешифрование: Remember also that the smallest minority on earth is the individual. Those who deny individual rights, cannot claim to be defenders of minorities.

5. Имитация атаки на гибридную криптосистему

6. Описание атаки

Шифрование в 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.

Для атаки злоумышленник перехватывает цифровой конверт с зашифровнным сообщением и зашифрованным секретным ключом.

6.1. Формулировка задания

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.

6.2. Выполнение задания

1. Подготовлен текст на английском языке

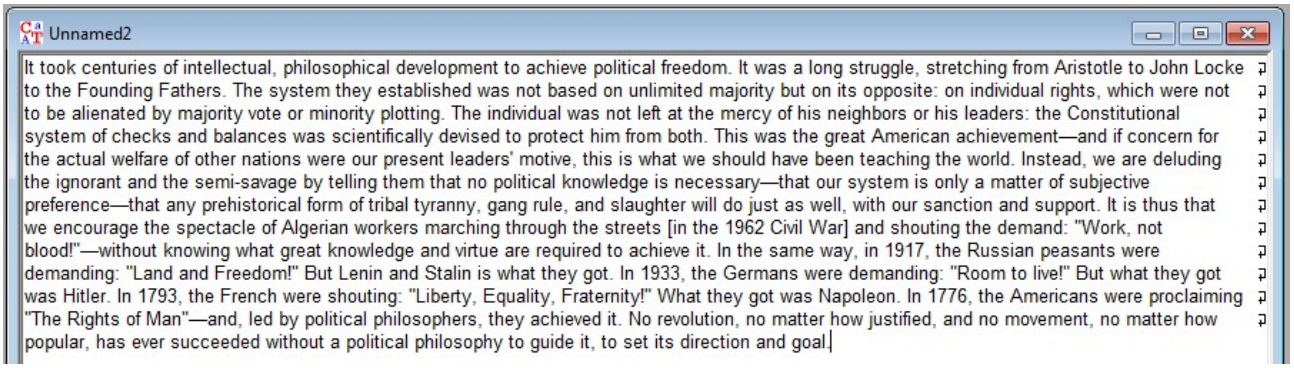

Рисунок 7. Исходный текст

2. Проведена демонстрация атаки с помощью указанной утилиты

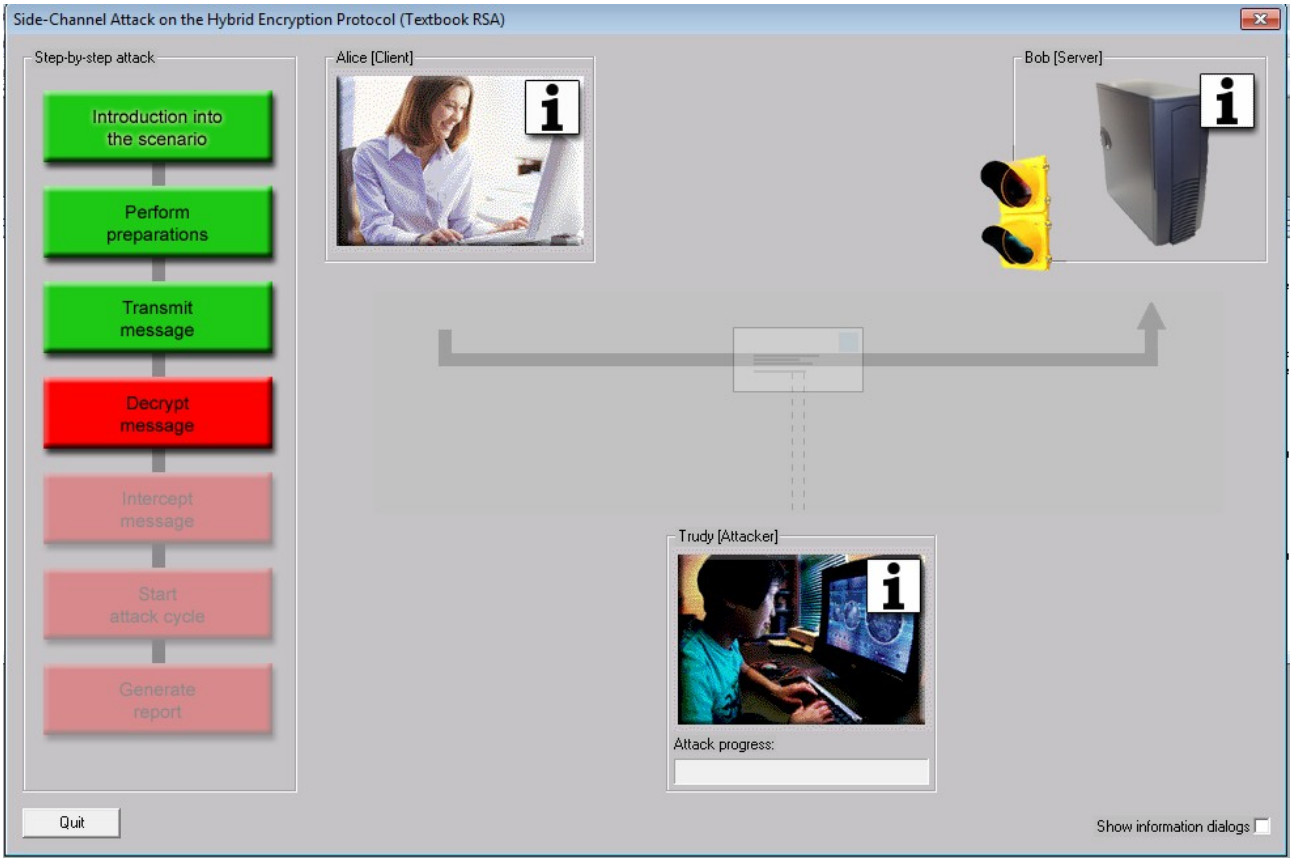

Рисунок 8. Вид утилиты

Лог атаки в Приложении Б.

7. Выводы

Исследован протокол Диффи-Хеллмана и ассиметричный шифр RSA.

Протокол Диффи-Хеллмана позволяет двум пользователям создать общий сеансовый ключ без обмена секретными ключами, чтобы обмениваться сообщениями по незащищенному каналу. Недостаток протокола — уязвимость к атаке Man-In-The-Middle.

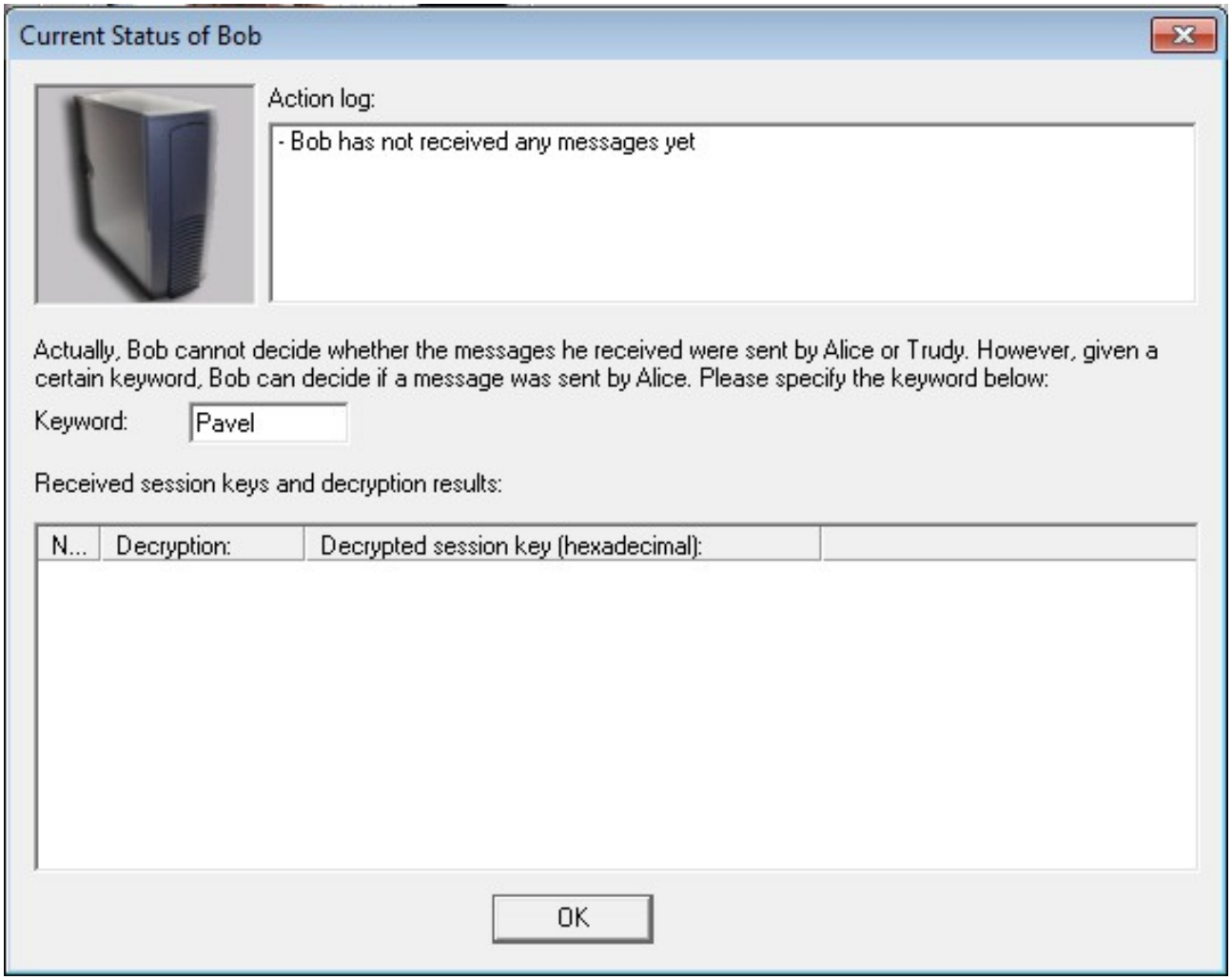

Рисунок 9. Настройка “сервера”

RSA — асимметричный блочный шифр. Длины ключей — 512, 768, 1024, 2048 бит, но 512 и 768 в настоящее время считаются недостаточными.

Криптостойкость алгоритма основана на вычислительно сложной задаче факторизации числа.

Недостаток алгоритма — относительно долгое время работы. Для компенсации этого недостатка используются гибридные системы — асимметричный шифр используется для передачи ключа симметричного шифрования.

Атака на гибридную систему основана на многократной модификации перехваченного сообщения; она позволяет восстановить сеансовый ключ, но не закрытый ключ получателя.

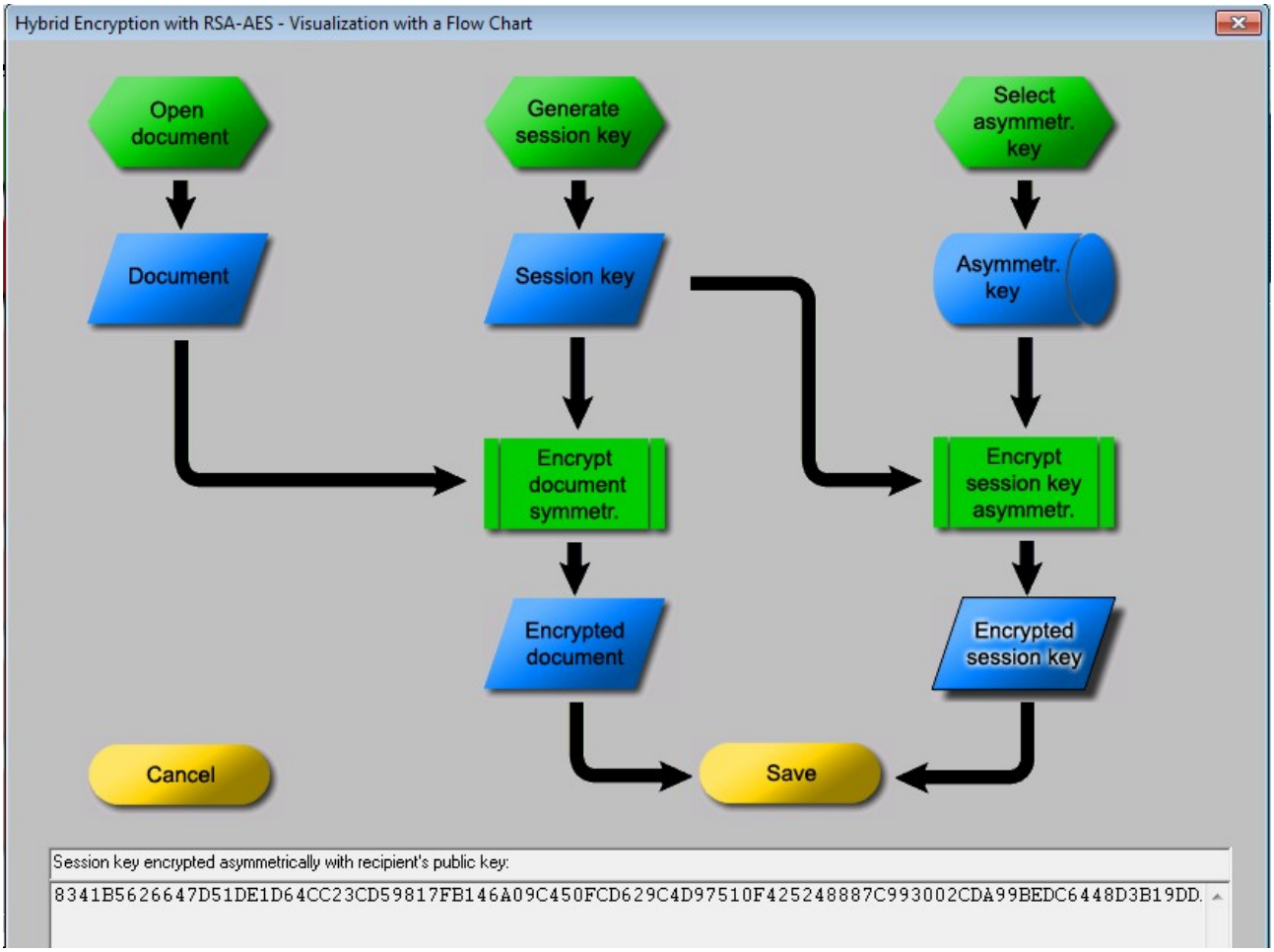

Рисунок 10. Работа гибридной схемы

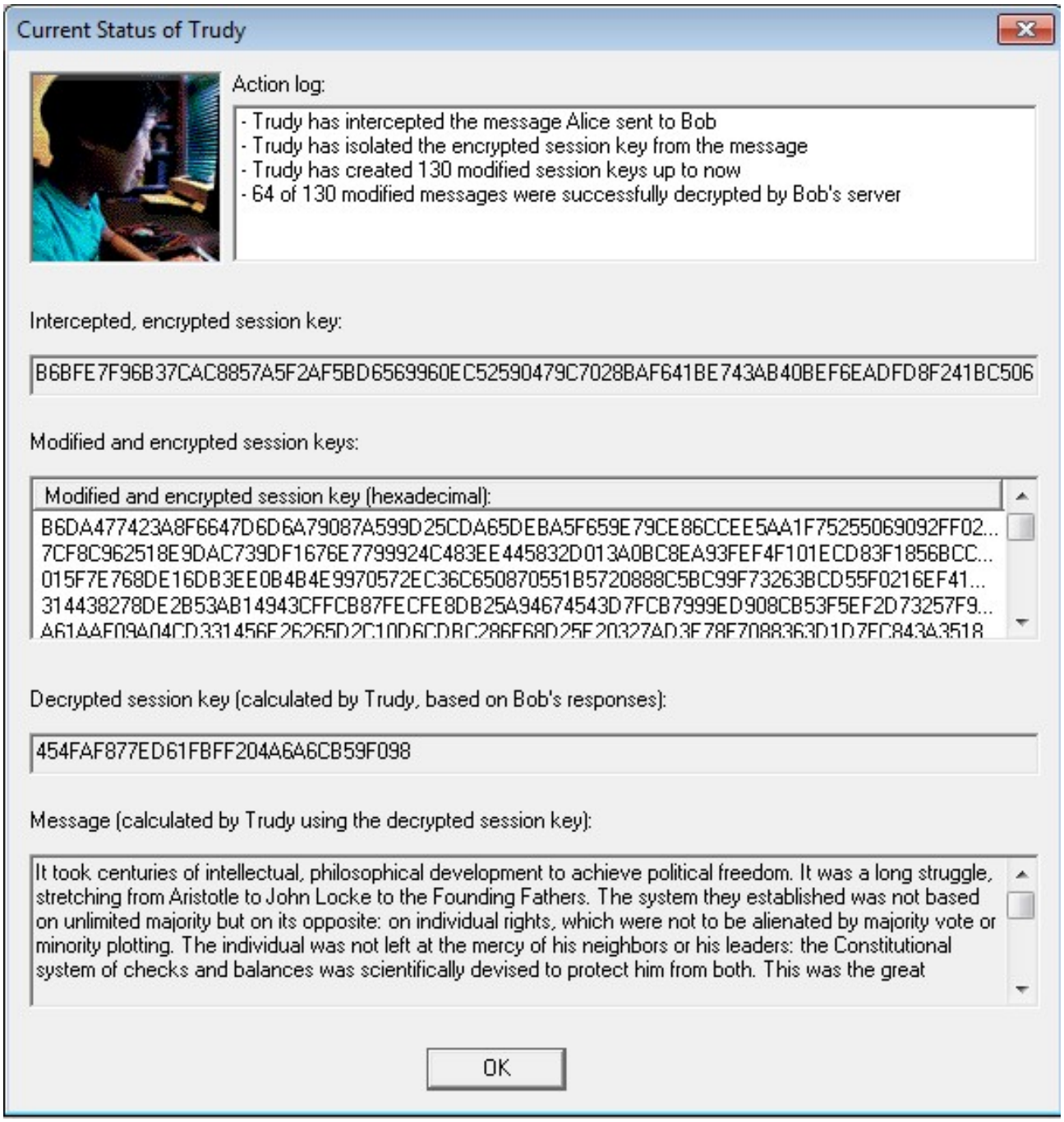

Рисунок 11. Результаты атаки

ПРИЛОЖЕНИЕ А

Логи протокола Диффи-Хеллмана

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

p: 164459422689066243011729968057438442455606356397837044700733361991165383163799

g: 907813567461027745807796387497225452807655778323986640190085628958513015287 87

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

a: 345965496217502958586539770344806628350519285819642887785193254450619458698 44

b: 540168295751191662302093676148898412973341895097066976800608315534225141750 88

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):
345965496217502958586539770344806628350519285819642887785193254450619458698 44

b (reduced mod p):
540168295751191662302093676148898412973341895097066976800608315534225141750 88

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: 344678179079760452304523029283826693658863121813863859842257924894341849330 13

B: 142731903542858044148169623036564507677299220545763907701621198404943777173031

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: 632001967640793904610010968159690064770482915931131964509256295499197365249 95

SB: 6320019676407939046100109681596900647704829159311319645092562954991973652499 5

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

ПРИЛОЖЕНИЕ Б

Логи Side Channel Attack

```
I. PREPARATIONS

Alice composes a message M, addressed to Bob.

Alice chooses a random session key S:
454FAF877ED61FBFF204A6A6CB59F098

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:
B6BFE7F96B37CAC8857A5F2AF5BD6569960EC52590479C7028BAF641BE743AB40BEF6EADFD8F241BC5063D99E

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:
B6BFE7F96B37CAC8857A5F2AF5BD6569960EC52590479C7028BAF641BE743AB40BEF6EADFD8F241BC5063D99E

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).
```