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):

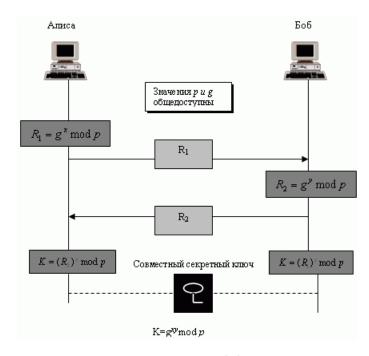


Рис. 1.1 – протокол Диффи-Хеллмана

- 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 х и у 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:

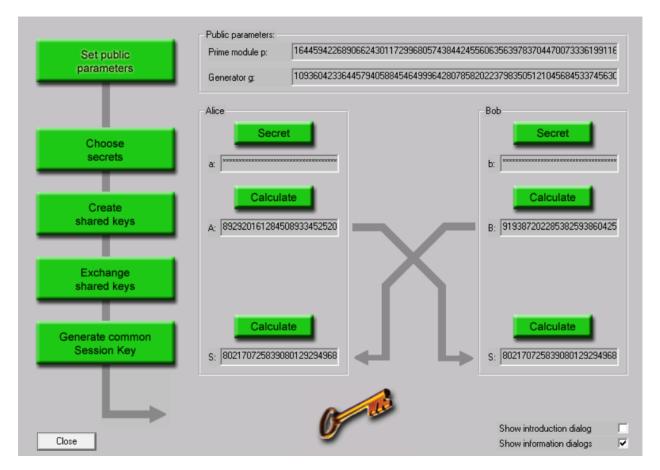


Рис. 1.2 – визуализация алгоритма Диффи-Хеллмана

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 q:

p:

164459422689066243011729968057438442455606356397837044700733361991165383163799

q:

1093604233644579405884546499964280785820223798350512104568453374 56309950888104

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

a:

8051117169729272892726748204530151558639265586979541020993226611 5266325794450

b:

 $1328834380265905656896401330798546589715977665108160560720619398\\55936954075515$

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):

8051117169729272892726748204530151558639265586979541020993226611 5266325794450

b (reduced mod p):

1328834380265905656896401330798546589715977665108160560720619398 55936954075515

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:

8929201612845089334525202623415330136728882128652852692416840299 4936741417507

B:

9193872022853825938604257670610539958512847364207951272200296480 5630641494088

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:

8021707258390801292949688739496387737590478805881816732112259345 5110740473335

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:

8021707258390801292949688739496387737590478805881816732112259345 5110740473335

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:

8021707258390801292949688739496387737590478805881816732112259345

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

Starting example for the CrypTool version family 1.x (CT1)

CrypTool 1 (CT1) is a comprehensive and free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.

This text file was created in order to help you to make your first steps with CT1.

1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links.

The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the main window or by using the search keyword "Starting page" within the index of the online help. Press F1 to start the online help everywhere in CT1.

2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (classic)"

3) There are several examples (tutorials) within the online help which provide an easy way to gain an understanding of cryptology. These examples can be found via the menu "Help -> Scenarios (Tutorials)".

4) You can further develop your knowledge by:

- Navigating playfully through the menus. You can press F1 at any selected menu item to get more information.

- Reading the included readme file (see the menu "Help-> Readme").

- Viewing the included coloribly presentation. This presentation can be found on several ways: e.g. in the "Help" menu of this application, or via the "Documentation" section found at the "Starting" page of the online help.

- Viewing the webpage www.cryptool.org.

March 2018 The CrypTool Team

Рис. 1.3 – Исходный текст

00000000	25 F4 68 OC E9 D6 CD 07 FF 02 E8 EE 1	4 CB 57 OF SD 34 D1 72 2D 5D CC 62 7	0 07 44 AF 84 E4 C2 64 F9 EE CF 9A A4 E2 CD 7C E2 BD F2 D8 8E 17 2F 6E 26 S.	k
00000001	OC 97 EC FD 82 FA 77 17 50 BE F8 D2 6	2 FB 5F 5C C5 7B 04 EE 6E C5 FD 56 0		w.Pb\.(nV.4X (10.d.v
00000062	29 59 A2 2F 5F 65 01 B1 22 1E CE 57 5	8 89 21 1A 4C 2E 89 28 92 5E C2 9F 5		f.7_e#WX.1.L>.r.^Q.Q2V\39W
00000092	87 9E 02 OF 05 E4 E2 EC A6 SA FC 02 5	E FF 92 26 40 4F 50 E6 C6 F2 96 6D D		
000000004	22 CD 27 12 5A A7 1A BE 69 OF FC A9 5	F C6 AF 59 15 9D 1E 2C 14 4E 6B A0 B	F 82 FA 7C A4 9E 61 95 AF A8 F1 1A A4 49 A4 9A B0 4B 02 7E C0 C0 C4 FA 80	'.EiY,Nk .aIK.~0
000000F5	A0 32 71 AB 45 31 0A FE 80 C0 55 9A 5	F OB 86 16 84 2C C2 19 EC F5 52 C8 2		lq.ElU,Rb.guj'
00000126	09 9E 51 2F 89 F9 EF 8E CA 5B E9 07 4	4 7E CE 28 12 2A 61 75 E6 82 04 01 2		.Q/[D+.*zu230\q.\Q.\
00000157	12 F4 F7 A0 A9 9C 6E 12 C4 B7 26 SE 1	B F5 FB BD 92 06 DD 5A D6 C5 59 79 4		n&ZYyE<.'W<(/JAK.(
00000188	BC 65 C6 OB 07 69 2D CB OB DB 80 CC 1	F A9 22 26 D5 B6 4C 0A 5D D6 E1 F6 9		ei36L.]Jo/.[.X.O'.s.kAgT'
00000189	81 0A 06 4B 3D 31 6E 6C DB AF 73 CE 5	E 71 DO 22 6B 70 1C 12 28 E2 FB 06 1		.K=lnls.^q.#kp*g(gl.E=48?[p?
000001EA	65 4E 26 4D DE 82 72 D9 B7 AF 77 5C I	A 52 7C 6C 9F OA 84 62 27 62 06 65 C		NAM F
00000218	BA E4 E7 CF C3 2B 00 41 B3 9E 5D E6 2	F 6C 60 22 16 A8 E8 27 39 1D 50 92 9	8 83 A5 14 3D A8 CE C2 92 D0 85 93 41 FF OF D9 7C FF 6A 33 40 C4 CC 2A 30	+.A1./1*#79.P=U.A1.138*0
00000240	18 8D 66 74 6D C5 85 D1 C1 49 CB 21 D	D 22 52 D6 10 B2 91 17 6A 56 FC 9C D		ftmI.1."R1aWo.eR.YP
0000027D	SE 90 48 71 24 DE 20 F2 B5 9E FC 46 E	7 AB 09 E5 A1 0A B2 9E AF 5F 0C D4 6	6 42 25 0B CD 1A B0 74 91 AF CD F7 79 BC AA BE 98 6E 9E 0B 42 DB BD 99 7B	Hq5F
000002AE	C4 1C 48 E1 58 B1 59 1B 5F 19 76 29 5	2 22 A1 D5 FC 92 B9 BF SE O1 A6 64 4	FE BE 14 C2 6A F2 FA 7B E2 60 CA BO FB BE DA 6F 5C 97 A4 D1 B4 AB D2 B2	H.X.Bv*."dAj(.'o\7
000002DF	CA DO 64 B9 AC 6D E1 92 27 A5 DB 7A 6	B 6A 19 0A 9A P6 4E 44 B0 9B 3E PE B	F 92 92 B7 61 77 56 19 3E 3E 41 F5 1B BA 15 75 5A BF 00 E2 AD C8 FF 81 DD	.d.,m.,',.skj,ND.,>awV.>>A,uZ
00000310	78 DO 4C 39 SC DE A7 FO 6A 4C 2F 19 4	A AO CA FO 77 94 B5 EC 52 2C BB 59 0	A OC 40 8A F7 4B 1A B9 57 D9 47 9D 02 AA 98 B2 62 02 F2 07 8C AC 4F 7A 27 (.	L9jL/.JwS<9KW.GbOs7
00000341	50 AD E2 41 59 0B 2E A1 52 E4 4A AB 5	9 C9 01 E2 17 1D C2 E8 E8 C9 DB A9 F	8 42 25 A4 E1 E0 B2 63 B0 SC 07 57 C5 B9 04 FA EA BA SC B9 DF 12 0E FD 29 X.	.ASR.J
00000372	33 35 AF SA 54 SA 2A C7 E9 DD 9E 51 3	7 8B 04 22 7F 43 A7 11 D1 5A 9B F3 2	5 EF 68 44 A4 00 8E B4 DC 80 B7 26 02 83 A3 A2 EF 06 71 D0 7A 57 58 3C 58 38	5T.*Q.[.".C2s.hDsq.mWX <x< td=""></x<>
000003A3	08 17 57 D5 7C EF C8 5B 43 92 62 83 4	E 98 07 D9 4D F0 66 64 1C 58 10 25 A	5 E4 34 DO E6 14 3F AF DE OD OB 5F F4 CO E1 CE 60 9F D2 2D 4F 8A 84 69 DE	W. [C.c.NM.fd.X.54?
000003D4	27 F2 FF DA B7 97 68 EC 76 66 EE 58 7	1 10 40 80 70 51 17 37 67 3C 2D E4 5	B4 D7 E1 FF OD 9D 81 E1 6C 8D FA 4E 65 20 38 FD FF FE B0 6C 85 C8 0E F9 '.	k.vf.[q.8.pQ.7q <u1.ne 8<="" td=""></u1.ne>
00000408	ES BE 66 BO EC SE 18 D8 43 DO 8C 2E 3	D FB 90 1A 0B 66 E9 C0 0B 50 0C A6 B	2 B5 15 19 FC 91 9C 71 4D 66 45 CB 54 2F 1F 93 CB 0C 11 A0 3D 5E E0 B5 EB	f>C=fPqMfE.T/=
00000426				F.WA.m2.E_% a)QV6.cSh32
00000467				n'4M.].2WeBppF (4.2'Be/-5
00000498	7E CO B2 6B CD 9E 23 6A B4 E7 CA F6 3	D 62 77 06 01 09 4E 62 62 07 FA 8B F		.k#j#bwNbb/xT.V>.RT#.HLLV
00000409	2D F5 A0 6A 7A E9 C6 6D FD 34 1E FF 4	6 47 71 60 9C 02 96 2D 8C 64 9C C4 A	7 19 OF 5B 80 1A 60 8B 21 52 26 FA DD 71 84 9E 58 C7 EF 3B 79 FA 4D 5D 7A	.js.m.4FGq'<.6d<['.!8sqX/y.M]=
000004FA				gs .ThD#>sf.r.Q.So.!C
00000528				yi\o:.)Qgwa2[]G <j%v(8< td=""></j%v(8<>
0000055C				p2D=.:gAi#.^L6.).sbmW.]*.
0000058D				'S.'E>[A
000005BE				54pT.sR/\N@o.^@:g.OX
000005EF)>.#RY"v6R24waX).
00000620				ImJVCdX<.msI*,.>.3+
00000651	4D 7C 66 35 3D 3E 1C F6 97 6C FF 77 3	2 6C 45	MI MI	#5=>1.w.1E

Рис. 1.4 – Зашифрованный текст

Starting example for the CrypTool version family 1.x (CT1)

CrypTool 1 (CT1) is a comprehensive and free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.

This text file was created in order to help you to make your first steps with CT1.

1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links.

The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the main window or by using the search keyword "Starting page" within the index of the online help. Press F1 to start the online help everywhere in CT1.

2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (classic)"

3) There are several examples (tutorials) within the online help which provide an easy way to gain an understanding of cryptology. These examples can be found via the menu "Help -> Scenarios (Tutorials)".

4) You can further develop your knowledge by:

- Navigating playfully through the menus. You can press F1 at any selected menu item to get more information.

- Reading the included readme file (see the menu "Help -> Readme").

- Viewing the included colorful presentation. This presentation can be found on several ways: e.g. in the "Help" menu of this application, or via the "Documentation" section found at the "Starting" page of the online help.

- Viewing the webpage www.cryptool.org.

March 2018 The CrypTool Team

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:
- а) Генерация двух больших простых чисел p и q (p и q держаться в секрете).
 - b) Вычисление n = p * q
- с) Выбор произвольного е (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:
 - а) 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:
- а) Шифротекст представляется блоками c_i : $c_i < n$.
- b) Каждый блок шифротекста преобразуется в открытый текст по формуле:

$$m_i = c_i^d mod n$$

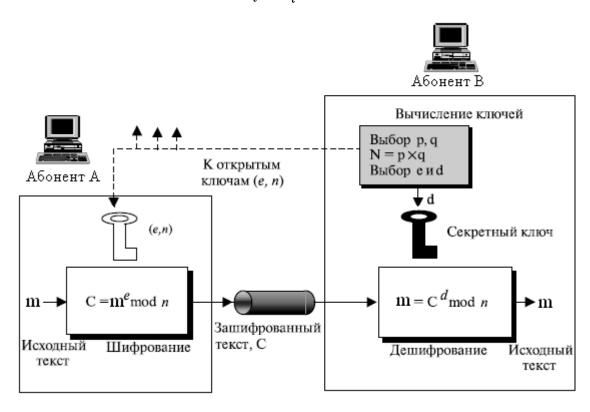


Рис. 2.1 – Схема шифра RSA

3. Генерация ключей

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

rime number p	10067	Generate prime numbers
Prime number q	10061	
SA parameters		
RSA modulus N	101284087	(public)
ohi(N) = (p-1)(q-1)	101263960	(secret)
Public key e	12333	
Private key d	8046597	<u>U</u> pdate parameters
SA encryption using	e / decryption using d [alphabet size:]	2561
nput as 🕝 text		Alphabet and number system options
	r encryption or decryption either as text	t or as hex dump.

Рис. 2.2 – Генерация ключей

Зашифруем с их помощью сообщение:

8382_mironchik

Процесс зашифрования представлен на рис. 2.3.

Input text

8382_mironchik

The Input text will be separated into segments of Size 3 (the symbol '#' is used as separator).

838 # 2_m # iro # nch # ik

Numbers input in base 10 format.

03683128 # 03301229 # 06910575 # 07234408 # 06908704

Encryption into ciphertext c[i] = m[i]^e (mod N)

98166235 # 43837704 # 52695318 # 19573168 # 13969603

2.3 – Зашифрование сообщения

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

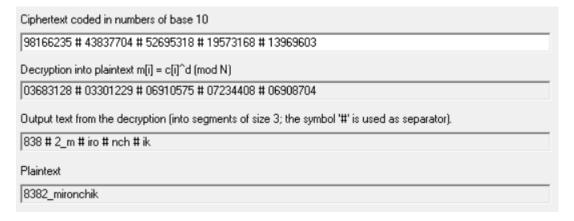


Рис. 2.4 – Расшифрование сообщения

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).

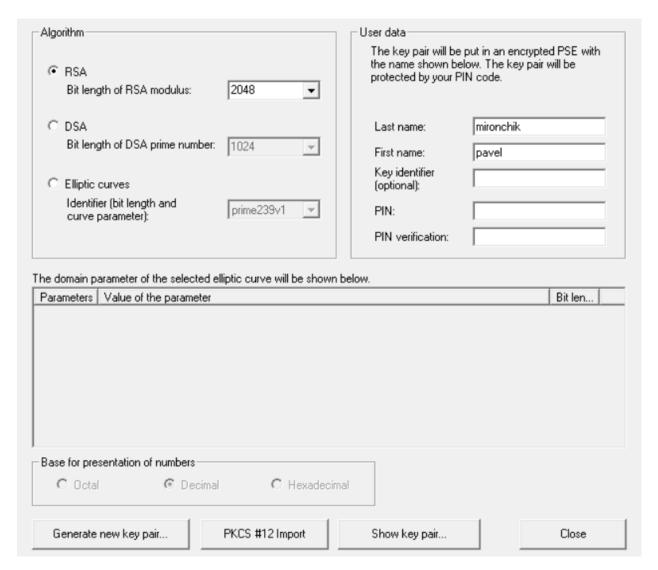


Рис. 3.1 – Генерация ключей

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	Os
768	Os
1024	Os
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 р и q так, чтобы n = pq > 256.
- 4. Задайте открытый ключ е.
- 5. Зашифруйте произвольное сообщение и передайте его вместе с, n и е 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:

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.

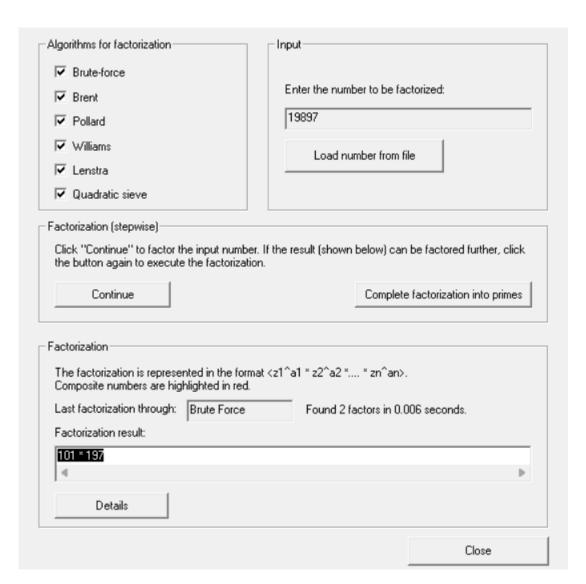


Рис. 4.1 – Результат факторизации

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

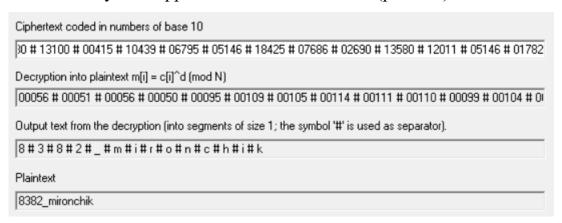


Рис. 4.2 – Дешифрование сообщения

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.

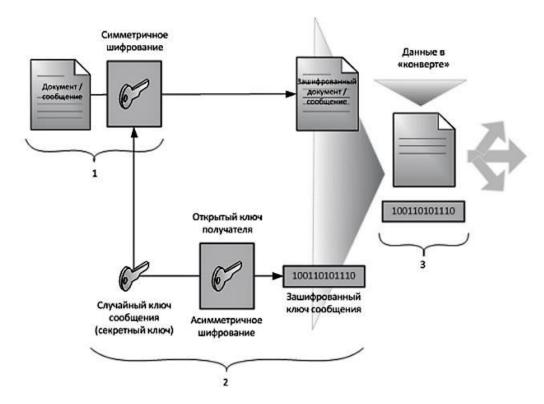


Рис. 5.1 – Модель гибридной системы

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 ${\tt M}$ with the session key ${\tt S}$.

Alice chooses Bob's public key e: 010001

Alice asymmetrically encrypts the session key S with Bob's public RSA key e: 58D651A5EA861D51DC63D91F49B80E501C3800E31F2D64EA165A09EA4B680894

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: 58D651A5EA861D51DC63D91F49B80E501C3800E31F2D64EA165A09EA4B680

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, c 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.