**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. 5381 |  | Кобылянский А.В. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2018

**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. Протокола Диффи-Хеллмана**

**1.1 Основные параметры протокола.**

* Открытые параметры p и g

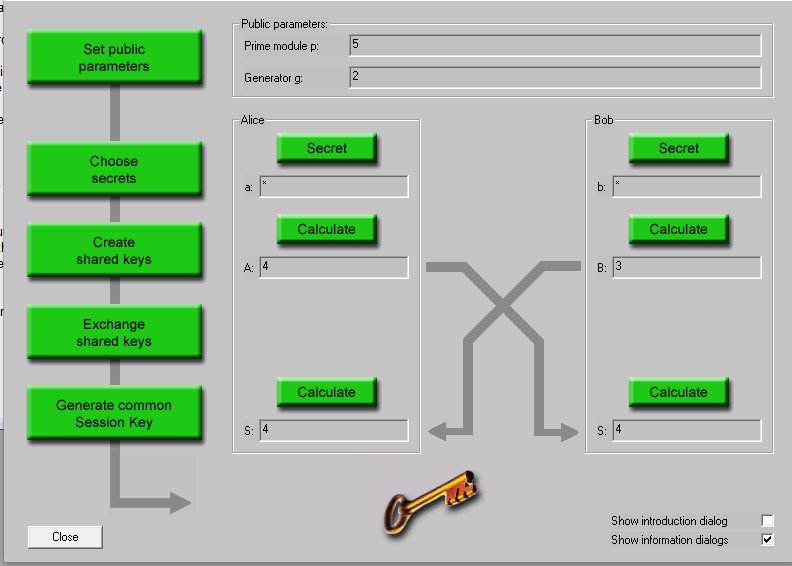
1. p – большое простое число порядка 300 десятичных цифр (1024 бита),
2. g – первообразный корень по модулю p.

* Секретные параметры, большие числа – x и y.
* Открытые ключи и

1. *,*

* Общий симметричный ключ K:

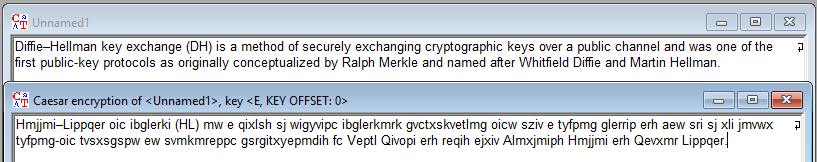
**1.2 Скриншот схемы протокола, реализованной в CrypTool**



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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Cryptool | p | g | a | b | A | B | S |
| Лекции | p | g | x | y |  |  | K |

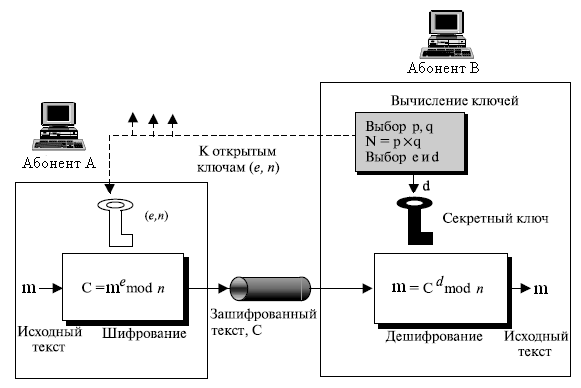
**1.4 Скриншот исходного, зашифрованного и расшифрованного текстов.**



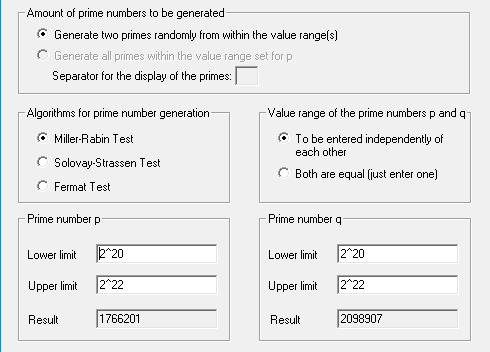
Текст зашифрован шифром цезаря с ключом (сдвигом) 4.

**2. Шифр RSA**

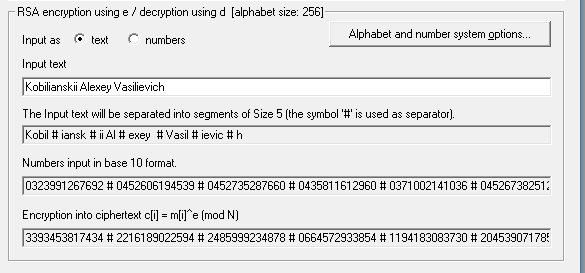
**2.1. Обобщенная схема шифра.**



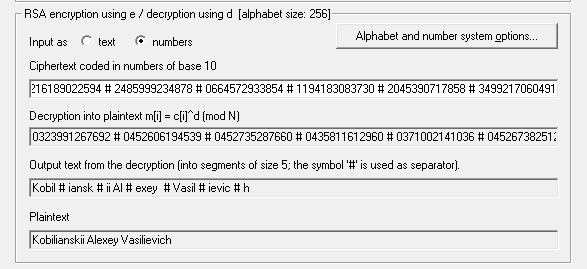
* 1. **Скриншот результата генерации ключей.**



* 1. **Скриншот результата шифрации.**



* 1. **Скриншот результата расшифровки.**



**3 Исследование шифра RSA**

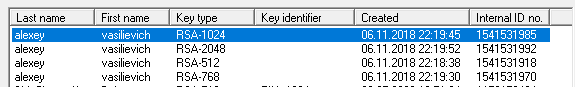
**3.1. Выбранный текст.**

RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem". The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1978. Clifford Cocks, an English mathematician working for the British intelligence agency Government Communications Headquarters (GCHQ), had developed an equivalent system in 1973, but this was not declassified until 1997.[1]

A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, and if the public key is large enough, only someone with knowledge of the prime numbers can decode the message feasibly.[2] Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem remains an open question.

RSA is a relatively slow algorithm, and because of this, it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

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



* 1. **Размер исходного текста.**

1563 символов.

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 512 | 768 | 1024 | 2048 |
| Encryption | 0.002 | 0.000 | 0.000 | 0.004 |
| Decryption | 0.018 | 0.032 | 0.048 | 0.194 |

1. **Атака грубой силы на RSA**

**4.1 Исходные данные для атаки, полученные от коллеги.**

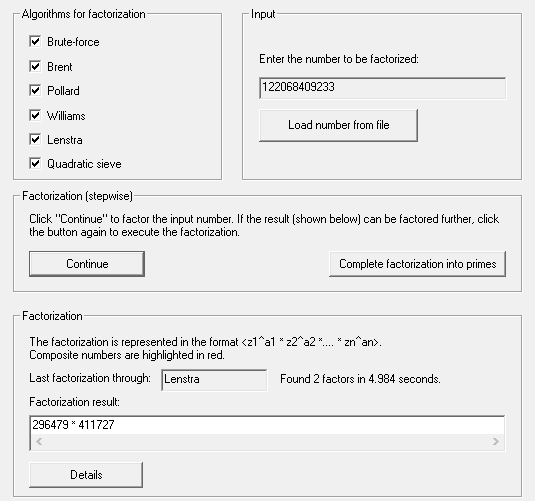
Текст:

105814092476 # 25174137024 # 121062305402 # 28848439765 # 22794363246 # 118545527422 # 15714143725 # 117978185712

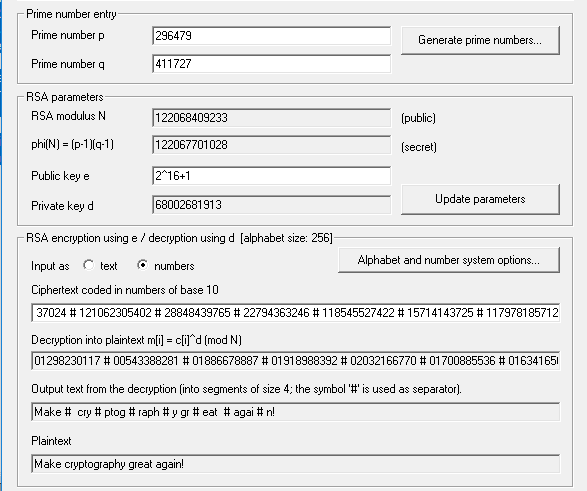
n = 122068409233

e = 2^16+1

* 1. **Результат факторизации (скриншот).**



**4.3 Расшифрованное в итоге сообщение.**



1. **Имитация атаки на гибридную криптосистему**
   1. **Текст передаваемого сообщения**

RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem". The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1978. Clifford Cocks, an English mathematician working for the British intelligence agency Government Communications Headquarters (GCHQ), had developed an equivalent system in 1973, but this was not declassified until 1997.[1]

Alexey

**5.3 Лог-файлы участников протокола**

I. PREPARATIONS

Alice composes a message M, addressed to Bob.

Alice chooses a random session key S:

E205DB0140CC0E13559E9A546AA07138

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:



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:



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).

**Вывод**

Шифр RSA представляет собой блочный алгоритм шифрования, где зашифрованные и незашифрованные данные должны быть представлены в виде целых чисел между 0 и n -1

Шифр RSA базируется на следующих двух фактах из теории чисел:

1. задача проверки числа на простоту является сравнительно легкой;
2. задача разложения чисел вида n = p\*q (р и q—простые числа) на множители является очень трудной, если мы знаем только n, а р и q—большие числа (это так называемая задача факторизации)

Для защиты от атаки необходимо ограничить количество ответов сервера для каждого сессионного ключа.