Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студент: .

ФИТ 2 курс 4 группа

Преподаватель: Буснюк Н. Н.

Минск 2020

**Практическое занятие №9**

**Тема «Криптографическая защита информации»**

Цель: Овладение навыков работы с известными криптографическими алгоритмами.

Теоретическое введение

Несмотря на достаточно большое число различных систем с открытыми ключами, одной из наиболее популярных остается криптосистема RSA, созданная в 1977 г. и названная в честь ее создателей Рона Ривеста, Ади Шамиpа и Леонарда Эйдельмана. Они воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, а разложение на множители произведения двух таких чисел – сложно.

В статье этих авторов, вышедшей в 1978 г., премия в сто долларов была назначена тому, кто первым расшифрует сообщение

68613754622061477140922254355882905759991125743198746951209308162982251457083569314766288398962801339199055182994515781515.

Метод шифрования был известен, единственное, что требовалось – разложить на два сомножителя 129-значное число, приведенное в этой статье.

Это было сделано только в 1994 г.

Задача была решена с помощью 600 человек и потребовала 220 дней и 1600 компьютеров, связанных через Internet.

Теоретические основы алгоритма RSA

Рассмотрим математические результаты, которые положены в основу этого алгоритма.

Определение 1. Сравнением целых чисел a и b будем называть соотношение между ними вида a = b + mk, означающее, что их разность (a – b) делится на заданное положительное число m, называемое модулем сравнения. При этом а называется вычетом числа b по модулю m.

Определение 2. Говорят, что два целых числа a и b сравнимы между собой и обозначают этот факт через a = b (mod m), если a и b имеют одинаковые остатки при делении на m.

Приведем некоторые очевидные свойства сравнений.

Пусть a = b (mod m) и с = d (mod m). Тогда:

1) a (+-) c = b (+-) d (mod m),

2) a\*c (+-) b\*d (mod m).

Легко также проверить, что операция сравнения по модулю m является эквивалентностью (выполняются свойства рефлексивности, транзитивности и симметричности), и, следовательно, можно говорить о разбиении множества целых чисел Z на непересекающиеся классы эквивалентности.

Теорема 1. (Малая теорема Ферма). Если p – простое число, то (x в степени (p – 1)) = 1 (mod p) для любого х, простого относительно p, и (x в степени p) = х (mod p) для любого х.

Определение 3. Функцией Эйлеpа Ф(n) называется количество положительных целых, меньших n и простых относительно числа n.

Теорема 2. Если n = pq, (p и q – отличные друг от друга простые числа), то Ф(n) = (p – 1)(q – 1).

Теорема 3. Если n = pq, (p и q – отличные друг от друга простые числа) и х – простое относительно p и q, то (x в степени Ф(n)) = 1 (mod n).

Следствия:

Если n = pq, (p и q – отличные друг от друга простые числа) и е – пpостое число относительно Ф(n), то отображение Е(e,n): x -> (x в степени e) (mod n) является взаимно однозначным на алгебраическом кольце вычетов Z(n).

Если е – пpостое число относительно Ф(n), то существует целое число d, такое, что e\*d = 1 (mod Ф(n)).

Пусть n = pq, где p и q – различные простые числа. Если e и d удовлетворяют уравнению (см. следствие 2), то отображения Е(e,n) и Е(d,n) являются инверсиями на кольце Zn.

Как Е(e,n), так и Е(d,n) легко рассчитываются, когда известны e, d, p, q.

Если известны e и n, но p и q неизвестны, то Е(e,n) представляет собой однонаправленную функцию; нахождение Е(d,n) по заданному n равносильно разложению n на простые сомножители.

Если p и q – достаточно большие простые числа, то разложение n – достаточно сложная вычислительная операция.

Это и заложено в основу системы шифрования RSA.

Пользователь i выбирает пару различных простых p(i) и q(i) и рассчитывает пару целых (e(i), d(i)), которые являются простыми относительно Ф(n(i)), где n(i) = p(i)\*q(i).

Итак, в реальных системах RSA реализуется следующим образом:

Каждый пользователь выбирает два больших простых числа p и q, и в соответствии с описанным выше алгоритмом выбирает два простых числа e и d; как результат умножения первых двух чисел устанавливается n. После этого {e, n} образует открытый ключ, а {d, n} – секретный (хотя можно взять и наоборот).

Открытый ключ публикуется и доступен каждому, кто желает послать владельцу ключа сообщение, которое зашифровывается указанным алгоритмом. После шифрования, сообщение невозможно дешифровать с помощью открытого ключа. Владелец же секретного ключа без труда может pасшифpовать принятое сообщение.

**Задание к выполнению**

1. Изучить теоретическое введение по данной теме.
2. Перенести в электронную тетрадь основные положения данной темы.
3. Реализовать пример шифрования сообщения в соответствии с вариантом:

|  |  |  |  |
| --- | --- | --- | --- |
| Номер варианта | Сообщение | p | Q |
| 14 | ADA | 53 | 47 |

1. Выбирается два простых числа ***p = 53*** и ***q = 47***
2. Вычисляется произведение ***n = p\*q***, в нашем примере ***n = 53\*47 = 2491***

Вычисляется функция Эйлера ***φ(n)***

***φ(n) = (p-1)\*(q-1)***

В нашем примере ***φ(n) = (53-1)\*(47-1) = 2392***. Функция Эйлера определяет количество целых положительных чисел, не превосходящих ***n*** и взаимно простых с ***n***.

1. Выбирается произвольное целое ***e***: ***0 <e < n*** взаимно простое с значением функции Эйлера ***φ(n)***. В нашем примере возьмём ***e = 17***. Пара чисел ***(e, n)*** объявляется открытым ключом шифра. В нашем примере ***(e, n) = (17, 2491)***
2. Вычисляется целое число ***d*** (обратное число по модулю от е) из соотношения

***(d\*e) mod φ(n) = 1***.

Операция ***mod*** вычисляет остаток от целочисленного деления двух чисел.

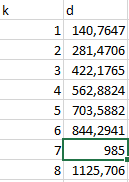
Это соотношение означает, что результатом деления произведения чисел ***e*** и ***d*** на значение функции Эйлера должно быть число 1. Поэтому ***d*** можно рассчитать по формуле

http://altaev-aa.narod.ru/security/images/im7.png,

придавая ***k*** последовательно значения 1, 2, 3, ... до тех пор, пока не будет получено целое число ***d***.

***Подсказка*.** Подбор ***k*** удобнее проводить в табличном процессоре Excel.

Найдём ***d*** в рассматриваемом примере:



при ***k = 1***, ***d*** – не целое, при ***k = 7***, ***d = 985***. Пара чисел ***(d, n)*** будет закрытым ключом шифра. В нашем примере ***(d, n) = (985, 2491)***.

RSA-шифрование сообщения ***T*** выполняется с помощью открытого ключа получателя ***(e, n)*** по формуле

http://altaev-aa.narod.ru/security/images/im9.png,

где ***Ti*** и ***Ci*** числовые эквиваленты символов исходного и зашифрованного сообщений (см. табл. 1).

**Таблица 1. Числовые эквиваленты русских букв, цифр и символа пробела**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | Т | U | V | W |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** | **32** | **33** | **34** | **35** | **36** | **37** |
| X | Y | Z | пробел | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

Рассмотрим пример шифрования RSA. Зашифруем сообщение «ADA» с помощью открытого ключа ***(17, 2491)***.

**Таблица 2. *Вычисление шифрограммы***

|  |  |  |
| --- | --- | --- |
| **Символы исходного сообщения, *Ti*** | **Коды символов *Ti*** | **Зашифрованные коды символов*Ci*** |
| A | 1 | ***117mod 2491 = 1*** |
| D | 4 | ***417mod 2491 = 168*** |
| A | 1 | ***117mod 2491 = 1*** |

Таким образом, мы исходное сообщение «ADA» представили в виде шифрограммы «1, 168, 1».

Расшифровка RSA-закодированного сообщения ***T*** выполняется с помощью закрытого ключа получателя ***(d, n)*** по формуле

http://altaev-aa.narod.ru/security/images/im10.png

Рассмотрим пример восстановления исходного сообщения. В предыдущем примере была получена пара ключей и шифрограмма «1, 168, 1», созданная открытым ключом данной пары. Восстановим исходное сообщение, применив закрытый ключ ***(d, n) = (985, 2491)*** той же пары.

**Таблица 3. *Восстановление сообщения***

|  |  |  |
| --- | --- | --- |
| **Зашифрованные коды символов *Ci*** | **Дешифрованные коды символов *Ti*** | **Символы исходного сообщения, *Ti*** |
| 1 | ***1985mod 2491 = 1*** | A |
| 168 | ***168985mod 2491 = 4*** | D |
| 1 | ***1985mod 2491 = 1*** | A |

Таким образом, мы восстановили исходное сообщение «ADA».