Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Основы Защиты Информации**

**Практическое занятие №9**

**Тема «Криптографическая защита информации»**

Студент: Городилов М. П.

ФИТ 2 курс 4 группа

Преподаватель: Буснюк Н. Н.

Минск 2020

**Цель**: Овладение навыками работы с известными криптографическими алгоритмами.

**Теоретические сведения**

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 число 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.

**Ход работы**

1.Задание

|  |  |  |  |
| --- | --- | --- | --- |
| Номер варианта | Сообщение | p | q |
| 8 | CBC | 29 | 73 |

2. Вычисляем произведение: **n = p\*q** = 29\*73 = 2117.

3. Вычисляем функцию Эйлера: **φ(n) = (p-1)\*(q-1)** = (29-1)\*(73-1) = 2016.

4. Выбирается произвольное целое ***e***: ***1 < e <* n** взаимно простое с значением функции Эйлера ***φ(n)***. ***e =*** 5. (Натуральные числа a и b называют взаимно простыми, если их наибольший общий делитель равен 1)

5. Открытый ключ шифра **(e, n)**: (5, 2117)

6. Найдем число ***d***:**(*d\*e*) *mod φ*(*n*) *= 1***

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

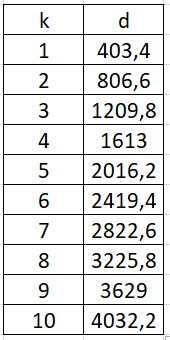


Рисунок 1.1. Поиск числа d через Excel

Из рисунка 8.1 видно, что d принимает целое значение, равное 1613, при k = 4.

7. Зашифруем сообщение «CBC»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **65** | **66** | **67** | **68** | **69** | **70** | **71** | **72** | **73** | **74** | **75** | **76** | **77** | **78** | **79** | **80** | **81** | **82** | **83** | **84** | **85** | **86** | **87** | **88** | **89** | **90** |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

Таблица 8.1 – Числовые эквиваленты латинских букв

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.

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

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

|  |  |  |
| --- | --- | --- |
| Символы исходного сообщения, *Ti* | Коды символов *Ti* (ASCII) | Зашифрованные коды символов *Ci* |
| C | 67 | 675*mod* 2117= 2006 |
| B | 66 | 665*mod* 2117= 56 |
| С | 67 | 675*mod* 2117= 2006 |

Таблица 8.2 – Вычисление шифрограммы

|  |  |  |
| --- | --- | --- |
| Зашифрованные коды символов *Ci* | Дешифрованные коды символов *Ti* (ASCII) | Коды символов исходного сообщения, *Ti* |
| 2006 | 20061613 mod 2117 | 67 |
| 56 | 561613 mod 2117 | 66 |
| 2006 | 20061613 mod 2117 | 67 |

Таблица 8.3 – Восстановление сообщения

**Вывод:** в ходе работы овладел навыками работы с известными криптографическими алгоритмами, а именно алгоритмом RSA.