**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

Цель: Овладеть навыками 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.

**Практическая часть**

Реализовать пример шифрования сообщения в соответствии с вариантом:

|  |  |  |  |
| --- | --- | --- | --- |
| Номер варианта | Сообщение | P | Q |
| 8 | CBC | 29 | 73 |

1. Находим произведение p и q
2. Находим значение функции Эйлера для n
3. Выбирается произвольное целое e: 0 < e < n взаимно простое с значением функции Эйлера φ(n). В нашем примере возьмём e = 5. Пара чисел (e, n) объявляется открытым ключом шифра. В нашем примере (e, n) = (5, 2117)
4. Вычисляется целое число ***d*** (обратное число по модулю от е) из соотношения
5. Придаём ***k*** последовательно значения 1, 2, 3,.. до тех пор, пока не будет получено целое число ***d***

|  |  |  |  |
| --- | --- | --- | --- |
| k |  |  |  |
| 1 | 2016 | 5 | 403.4 |
| 2 |  |  | 806.6 |
| 3 |  |  | 1209.8 |
| 4 |  |  | 1613 |

Таблица 1. – Подбор значений k

Пара чисел (d, n) будет закрытым ключом шифра. В нашем примере (d, n) = (1613, 2117).

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

Числовые эквиваленты латинских букв указаны в таблице 1.

|  |  |  |
| --- | --- | --- |
| A – 1 | B – 2 | C – 3 |
| D – 4 | E – 5 | F – 6 |
| G – 7 | H – 8 | I – 9 |
| J – 10 | K – 11 | L – 12 |
| M – 13 | N – 14 | O – 15 |
| P – 16 | Q – 17 | R – 18 |
| S – 19 | T – 20 | U – 21 |
| V – 22 | W – 23 | X – 24 |
| Y – 25 | Z – 26 |  |

Таблица 2. – Числовые эквиваленты латинских букв

Расшифровка осуществляется по формуле:

**Вывод:** Я овладел навыками криптографической защиты информации.