ТЕОРИЯ ЧИСЕЛ В АССИМЕТРИЧНОМ ШИФРОВАНИИ

Протько М.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Борисенко О.Ф. И.О. – канд. физ.-мат. наук, доцент

С широкой распространенностью информационных технологий растет потребность в специалистах широкого профиля, способных не только создавать программное обеспечение, но и исключать вмешательство третьих лиц в процессе его работы, тем самым, защищая конфиденциальность себя и клиента. Чтобы обеспечить данные возможности, необходимо глубокое понимание основ шифрования, начинающихся с теории чисел.

Ключевые слова: криптографическая стойкость, RSA алгоритм, ассиметричное шифрование, случайная величина

Один из известных алгоритмов шифрования, использующийся и на данный момент, это алгоритм RSA – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Рассмотрев его поподробнее, можно ознакомится с основными принципами шифрования.

Для того, чтобы создать криптографический стойкий шифр (способный противостоять расшифровке без знания ключа, анализу повторяемости, «грубой силе») необходимо найти одностороннюю функцию, используя которую на некотором множестве, можно было бы получить иное соответствующее данному множество, обратимое при знаниях неких дополнительных условий (аргументов функции, в т.ч. ключей). Или же:

$$f(m, n) = c \quad (1)$$

$$f(c, e) = m, \quad (2)$$

где m – начальное множество, c – конечное (зашифрованное), n и e – открытий и закрытый ключи соответственно.

Причем невозможно найти такую $f^{-1}(c) = m$ за конечный промежуток времени, такой, что после дешифровки информация все еще будет востребована.

Односторонняя функция RSA выглядит так:

$$E(m)=m^e \; c= E(m) \bmod n \quad (3)$$

Алгоритм построения RSA следующий:

1. Выбрать два случайных простых числа p и q
2. Найти модуль:
$$n = p \cdot q \quad (4)$$
3. Найти функцию Эйлера:
$$\varphi(n) = (p-1)\cdot(q-1) \quad (5)$$
4. Найти взаимно простое число e, 1<e< φ(n), где e – взаимно простое с значением φ(n) , где e – открытая экспонента
5. Найти d из уравнения
$$d\cdot e \equiv 1 \pmod{\varphi(n)}, \quad (6)$$

где d – секретная экспонента

При применении алгоритма на практике, были найдены следующие нюансы:

1. Нахождение случайных чисел, в особенности, когда в последовательности их больше двух, довольно затруднительно (не существует абсолютно удобных алгоритмов для решения данной задачи)

2. После нахождения случайных чисел, их нужно проверить на простоту, причем сделать это необходимо при минимальном количестве вычислений (за достаточно короткое время), т.е. количество проводимых тестов (Ферма, Люка, и т.д) ограничено.

3. Нахождение d из уравнения в пункте 5 может требовать оптимизации вычислений с использованием теории чисел, причем, чем больше значения e и φ(n), тем сложнее ее найти.

Решение каждого из вышеперечисленных вопросов требует финансовых и временных затрат. Из чего следует вывод: для того, чтобы создать алгоритм шифрования, необходимо четко знать в каких сферах он будет применятся (шифрование номеров банковских карт, электронная подпись, сертификация информации и т.д), какими средствами данный алгоритм будет реализовываться (вычислительные мощности при вычислении ключей, максимальное время расшифровки/шифровки, объемы шифрования)

Список использованных источников:

1. *НОУ ИНТУИТ. Лекция 11: Основные положения теории чисел, используемые в криптографии с открытым ключом[электронный ресурс]: https://intuit.ru/studies/courses/691/547/lecture/12389*
2. *Асимметричное шифрование на практике [электронный ресурс]:https://habr.com/ru/post/449552/*
3. *Информация о числах. Свойства и характеристики одного числа[электронный ресурс]: https://aboutnumber.ru/197*
4. *Тест простоты Люка [электронный ресурс]:https://ru.wikipedia.org/wiki/Тест_простоты_Люка*

5. Асимметричный алгоритм для генерации коротких серийных номеров [электронный ресурс]: https://habr.com/ru/post/69623/

6. Стройникова Е.Д. Основы прикладной алгебры: учеб.-метод. пособие/ Е.Д.Стройникова.-Минск:БГУИР,2010.-120 с.:ил.