УДК 004

ТЕОРИЯ ЧИСЕЛ В ШИФРОВАНИИ ДАННЫХ

Березин М. А., студент группы ИПБ-24, I курс
Научный руководитель: Бурцев А. И., к. ф.-м. н., доцент
Рыбинский государственный технический университет
имени П.А. Соловьева
г. Рыбинск.

Сохранение секретности при передаче информации всегда было важным вопросом безопасности. До развития компьютерных технологий, шифрование данных осуществлялось вручную, однако с развитием информационных технологий стали появляться новые методы защиты данных. В данной работе рассматриваются методы теории чисел, используемые в системе шифрования RSA. Эта система получила свое название по фамилиям её создателей: Рональда Ривеста, Ади Шамира и Леонарда Адлемана. Асимметрично-ключевая криптографическая система RSA, была впервые представлена в 1977 году. Её преимуществом стал тот факт, что она стала первой системой, пригодной как для шифрования данных, так и для генерации цифровых подписей. Основной идеей, стоящей за RSA, является использование свойств простых чисел и их произведений. Система основывается на трудности факторизации больших чисел, что делает её безопасной. Создатели стремились разработать одностороннюю функцию, которую было бы крайне трудно инвертировать, что и было достигнуто с помощью теории чисел.

В RSA используются два ключа: открытый и закрытый. Открытый ключ, состоящий из произведения двух больших простых чисел и экспоненты, может быть свободно распространён. В то время как закрытый ключ, необходимый для расшифровки, хранится в секрете. Безопасность системы зависит от сложности задачи факторизации, что делает выбор простых чисел критически важным. Кроме того, RSA не только обеспечивает конфиденциальность, но и позволяет устанавливать подлинность с помощью цифровых подписей. Это достигается путём шифрования сообщения с использованием закрытого ключа отправителя, что позволяет получателю проверить подлинность сообщения с помощью открытого ключа.

Таким образом, асимметрично-ключевая криптография не только защищает данные, но и подтверждает их целостность и подлинность. Важно отметить, что в отличие от симметрично-ключевой криптографии, которая использует для шифрования подстановку и перестановку символов, асимметрично-ключевая криптография опирается на математические функции и свойства чисел. Это делает её более гибкой и безопасной в контексте современных требований к защите информации. В условиях, когда использование приложений зависит от персональной тайны, асимметрично-

ключевая криптография становится незаменимым инструментом для обеспечения безопасности данных.

Асимметрично-ключевая криптография использует два ключа: секретный (или же частный) и открытый (или же публичный). На их основе и проходит процесс шифрования или дешифрования. Если представить это процесс как запирание и отпирание замка, то замок закрытый открытым ключом можно открыть только соответствующим секретным ключом. Шифрование и дешифрование в асимметрично-ключевой криптографии являются математическими функциями, которые работают с числами, которые в свою очередь являются представлениями исходного текста и зашифрованного текста.

Зашифрованный текста можно представить, как следующую функцию:

$$C = f\,(K_{public},\, P),$$

где f — функция шифрования,

K_{public} — открытый ключ доступа,

P — исходный текст, который может быть представлен следующим образом:

$$P = g\,(K_{private},\, C),$$

где g — функция дешифрования,

$K_{private}$ — секретный ключ доступа,

C - зашифрованный текст.

Однако стоит заметить, что функция f, являющаяся односторонней функцией, нуждается в так называемой «лазейке», чтобы мы могли расшифровать сообщение, а перехвативший его как-либо образом злоумышленник на это был не способен.

Прежде чем перейти к понятию «лазейки» стоит разобраться с двумя моментами, играющими очень важную роль во всём алгоритме шифрования RSA.

Во-первых, это Эйлеровская функция phi, позволяющая узнать количество чисел меньших n и взаимно простых с n. Так как в алгоритме шифрования RSA с данным понятием связаны лишь простые числа нам достаточно знать лишь что $\varphi(n) = n-1$, где n — простое число.

Во вторых, алгоритм быстрого возведения в степень по модулю, который выглядит следующим образом: $x=(x \cdot x) \bmod n$. То есть в процессе шифрования не возводить в степень сразу всё число, а циклически умножать его на само себя, и после этого брать от произведения модуль по числу n.

Главная идея асимметрично-ключевой криптографии заключается в понятии «лазейка» в односторонней функции.

Хотя понятие функции знакомо из математики, в криптографии ему даётся неофициальное определение. Функция — правило, по которому связывают одни элемент из множества A, называемый доменом, и один элемент из множества B, который в свою очередь называется диапазоном. Односторонней функцией называется функция обладающая следующими свойствами:

1. f вычисляется просто. То есть при данном x, $y=f(x)$ может быть вычислен очень легко.

2. f^{-1} (функция обратная данной) вычислить очень трудно. То есть при данном y, $x=f^{-1}(y)$ практически невозможно вычислить.

«Лазейкой» же называется односторонняя функция с третьим свойством:

3. При данном y и секретной «ловушке», x может быть очень легко вычислен.

Например:

Когда n является большим числом, функция $y = x^k \bmod n$ - «лазейка» в односторонней функции. То есть при заданных x, k и n значение функции y может быть легко вычислено по алгоритму быстрого возведения в степень по модулю, который был описан ранее. Но при заданных y, k и n, величину x практически невозможно вычислить, так как всё упирается в проблему дискретного логарифма. В этом случае вычисление функции f^{-1} займёт огромное количество времени.

Однако если мы знаем «лазейку» и k', такое, что $k \cdot k' = 1 \bmod \varphi(n)$ (Эйлерова функция phi, описанная раннее), то мы сможем использовать значение $x = y^k \bmod n$, чтобы вычислить x. Это и есть алгоритм, используемый в криптографической системе RSA.

Теперь можно перейти к самому алгоритму шифрования. Обобщённо его можно представить следующим образом:

Пункт первый - генерация ключей:

1. Выбрать два больших простых числа p и q, такое что $p \neq q$

2. Вычислить число $n = p \cdot q$

3. Вычислить значение эйлеровой функции от n, т.е. $\varphi(n)=(p-1)\cdot(q-1)$, т.к. p и q простые числа.

4. Выбрать число e, такое что $1 < e < \varphi(n)$, а также y взаимно простое с $\varphi(n)$.

5. Вычислить число $d = e^{-1} \bmod \varphi(n)$, т.е. d равное инверсии e по модулю $\varphi(n)$.

Таким образом, числа e и n составляют открытый ключ, а число d — секретный.

Шифрование происходит путём возведения числа P (представления исходного текста в числовом виде) в степень e по модулю n: $C = P^e \bmod n$, где e и n составляют открытый ключ. Таким образом мы получаем число C, являющееся численным представлением зашифрованного текста. Дешифрование же происходит путём возведения числа C в степень d по модулю n: $P = C^d \bmod n$, где d является секретным ключом. Данное действие позволяет получить исходное сообщение, представленное в виде числа P.

На основе описанного алгоритма была написана программа. Программа реализована на языке C++ и позволяет шифровать и дешифровать сообщения любого размера.

В заключении можно сказать, что криптографическая система RSA представляет собой один из наиболее важных и широко используемых методов шифрования в современном цифровом мире. Основанная на сложных математических принципах RSA обеспечивает высокий уровень безопасности и конфиденциальности при передаче данных, что делает её незаменимой в таких сферах, как электронная коммерция, банковские операции и защита личной информации.

Несмотря на свои преимущества, система RSA не лишена уязвимостей, особенно в свете быстрого развития вычислительных технологий и методов криптоанализа. Поэтому необходимо продолжать исследование и разработку новых и более защищенных методов шифрования, а также регулярно обновлять алгоритмы и ключи для поддержания уровня безопасности. Кроме того, применение RSA в сочетании с другими криптографическими методами, такими как шифрование с симметричными ключами, может обеспечить более комплексный подход к защите информации. В конечном счете, успешное использование RSA и подобных технологий требует осознания их особенностей, методов защиты и возможных угроз.

Таким образом, криптографическая система RSA продолжает оставаться неотъемлемым инструментом в обеспечении безопасности данных, и ее значение будет только возрастать в условиях постоянно развивающегося информационного пространства.

Список литературы

1. Фороузан Б.А. Математика криптографии и теория шифрования. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016.

2. https://www.geeksforgeeks.org/bigint-big-integers-in-c-with-example/

3. https://ru.khanacademy.org/computing/computer-science/cryptography/