БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра системного анализа и компьютерного моделирования

КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ (КРИПТОСИСТЕМА RSA)

Методические материалы к лабораторной работе «Исследование криптосистемы RSA» по спецкурсу криптографический инжиниринг

для студентов специальности 1-98 01 01 Компьютерная безопасность

2023 г.

СОСТАВИТЕЛИ:

П.П. Коржуков, старший преподаватель кафедры системного анализа и компьютерного моделирования Белорусского государственного университета.

Текст представлен в авторской редакции.

РЕКОМЕНДОВАНА К РАЗМЕЩЕНИЮ В ЭЛЕКТРОННОЙ БИБЛИОТЕКЕ БГУ:

Кафедрой системного анализа и компьютерного моделирования Белорусского государственного университета
(протокол № 8 от 14 февраля 2023 г.);

Данная дисциплина предназначена для студентов специальности 1-98 01 01 Компьютерная безопасность (по направлениям) (направление 1-98 01 01-02 Компьютерная безопасность (Радиофизические методы и программно-технические средства)).

Криптографический инжиниринг ссылается на теорию и практику инжиниринга криптографических систем, т.е. устройства шифрования и расшифрования, аппаратно-программные системы цифровой сигнатуры и аутентификации, системы генерации, распределения и управления ключами. Криптографический инженер проектирует, реализовывает, тестирует и проверяет криптографические системы. В область интересов криптографического инжиниринга входит криптоанализ криптографических систем с целью проверки их устойчивости и надежности по отношению к атакам, а также построение контрмер против них, чтобы сорвать такие нападения или уменьшить вероятность их успешности.

Знание основ теории и общего математического введения в алгоритмы в криптографии без показа или знания, как они реализуются, не достаточно. Проблемы создания криптосистем находятся в деталях: в практической реализации. В этом курсе делается акцент на реализацию алгоритмов криптографии в реальном программном или аппаратном обеспечении. Здесь исследуется криптографическая система с открытым ключом RSA.

Криптографический инжиниринг
Павел Павлович
Коржуков
korzhukov@bsu.by 398-02-22
зима 2023

Асимметричное шифрование устроено несколько сложнее симметричного. В нём используются уже два ключа. Данные шифруются одним ключом, а расшифровываются другим. Первый ключ (открытый) можно держать у всех на виду, а вот второй (закрытый) нужно хранить в секрете, прятать от недругов.

Такой подход снимает некоторые вопросы безопасности в компьютерной криптографии. В интернете невозможно вообще не передавать никому никакие ключи. Это необходимо. Вот асимметричное шифрование помогает с решением этого вопроса. Часть ключей можно безопасно пересылать, это не нарушит секретности.

КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

Асимметричное шифрование основано на использовании двух чисел в паре. Одно из этих чисел – открытый ключ, который доступен всем. С помощью этого числа кто угодно может зашифровать нужное ему сообщение. Но расшифровать его быстро с помощью этого же числа не получится простым способом.

Для расшифровки берут второе число – закрытый ключ. Он должен быть секретным.

Это не могут быть два случайных ключа. Открытый и закрытый ключ всегда связаны между собой алгоритмом, который задаёт их значения. Смысл в том, что внутри этого алгоритма есть третье, тоже секретное, число, которое связано с обоими ключами.

1 Криптосистема RSA

1.1 Формирование системы RSA

1. Выбираем два различных простых числа p и q.
2. Вычисляем $n = pq$ и
   $\varphi(n) = (p - 1)(q - 1)$.
3. Выбираем число e, взаимно простое с $\varphi(n)$.
4. Вычисляем число d из уравнения
   $de \equiv 1 \pmod{\varphi(n)}$.
5. Определяем открытые ключи e и n.
6. Определяем закрытые ключи d, p, q и $\varphi(n)$.

1.2 Алгоритм шифрования

1. Дан текст сообщения M.

Шифротекст C вычисляется по формуле

$C = E_k(M) = M^e \bmod n$.

1.3 Алгоритм дешифрования

1. Дан шифротекст C.
2. Текст сообщения M вычисляется по формуле

$M = D_k(C) = C^d \bmod n = (M^e)^d \bmod n = M$.

1.4 Цифровая подпись

1. Есть абонент A и текст для подписи M.
2. Определяются закрытые ключи системы RSA, а именно d, p, q и $\varphi(n)$.
3. Определяются открытые ключи e и n.
4. Закрытым ключом вычисляется

$C = M^d \bmod n$.

Сообщение C рассматривается как подпись абонента A, потому что закрытый ключ d известен только ему.

5. Проверка подписанного документа вычисляется по формуле

$C^e = (M^d)^e \bmod n = M$,

используя открытый ключ e.

1.5 Пример

На первый случай здесь используются маленькие числа и просто шифруется аббревиатура RSA.

Пусть $p = 17$ и $q = 31$. Тогда $n = pq = 527$, причем имеет место $\varphi(n) = (p - 1)(q - 1) = 480$.

Для открытого ключа выберем небольшое число $e = 7$, взаимно простое с $\varphi(n)$. Решая уравнение

$de \equiv 1 \pmod{\varphi(n)}$

относительно d с помощью алгоритма Евклида, находим для закрытого ключа соответствующее число $d = 343$.

Проверка: $7 \cdot 343 = 2401 \equiv 1 \pmod{480}$.

Теперь представим сообщение RSA в виде последовательности чисел, содержащихся в интервале [0, 526]. Для этого буквы R, S и A закодируем пятимерными двоичными векторами, воспользовавшись двоичной записью их порядковых номеров в английском алфавите

R = 18 = (10010), S = 19 = (10011), A = 1 = (00001).

Тогда сообщение M принимает вид

RSA = (100101001100001).

Чтобы уложиться в заданный интервал [0, 526], разобьем строку на две подстроки не более 9 бит в каждой и получим новое представление кода

RSA = (100101001), (100001) = ($M_1 = 297$, $M_2 = 33$).

Далее последовательно шифруем M_1 и M_2

$C_1 = E_к(M_1) = M_1^e \equiv 297^7 \pmod{527} = 474$.

При этом провели ряд упрощений для расчётов:

$297^7 = ((297^2)^3\ 297) \bmod 527 = (200^3 \pmod{527}\ 297) \bmod 527$.

$C_2 = E_k(M_2) = M_2^e \equiv 337 \bmod 527 = 407$.

В итоге получаем шифротекст $y_1 = 474$ и $y_2 = 407$.

Для расшифровки этого шифротекста нужно выполнить определенную последовательность действий. Вычислить

$D_k (C_1)^{343} = (C_1)^{343} \bmod 527$.

Отметим, что при возведении в степень удобно воспользоваться тем обстоятельством, что

$343 = 256 + 64 + 16 + 4 + 2 + 1$.

На основании этого представления получаем

$474^2 \equiv 174 \pmod{527}$, $474^4 \bmod 527 = 237$,
$474^8 \bmod 527 = 307$, $474^{16} \bmod 527 = 443$,
$474^{32} \bmod 527 = 205$, $474^{64} \bmod 527 = 392$,
$474^{128} \bmod 527 = 307$, $474^{256} \bmod 527 = 443$,
в силу чего имеет место быть

$474^{343} \bmod 527 \equiv (443 \cdot 392 \cdot 443 \cdot 237 \cdot 174 \cdot 474) \bmod 527 = 297$.

Аналогично получается и со второй подстрокой

$407^{343} \bmod 527 = 33$.

Возвращаясь к буквенной записи, получаем после расшифровывания двух подстрок – RSA.

Стойкость системы RSA

Теперь проанализируем вопрос о стойкости системы RSA. Можно показать, что сложность нахождения секретного ключа системы RSA определяется сложностью разложения числа n на простые множители. В связи с этим нужно выбирать числа p и q таким образом, чтобы задача разложения числа n была достаточно сложна в вычислительном плане. Для этого рекомендуются выполнять следующие требования:

1) числа p и q должны быть достаточно большими. Их длина в десятичной записи должна быть не менее 100 знаков. При этом они должны не слишком сильно отличаться друг от друга и в то же время быть не очень близкими друг другу;

2) числа p и q должны быть такими, чтобы наибольший общий делитель чисел $(p - 1)$ и $(q - 1)$ был небольшим числом. Лучше всего, чтобы НОД $(p – 1, q - 1) = 2$;

3) числа p и q должны быть сильно простыми числами.

Определение. Простое число p называется сильно простым, если выполняется следующий ряд условий:

а) число $p + 1$ имеет большой простой делитель;
б) число $p - 1$ имеет большой простой делитель r;
в) число $r - 1$ имеет достаточно большой простой делитель.

Перечисленные условия для сильной простоты можно также записать в следующем виде:

$p \equiv s - 1 \pmod{s}$,
$p \equiv 1 \pmod{r}$,
$r \equiv 1 \pmod{t}$,
где p, r, s, t – большие простые числа.

Если не соблюдать указанные рекомендации по выбору чисел p и q, число n может быть эффективно разложено на множители современными компьютерными системами.

Чтобы повысить скорость шифрования с помощью алгоритма RSA, нужно выбирать малую шифрующую экспоненту e открытого ключа. Но если число e достаточно малое по величине, то есть риск, что найдутся e абонентов с тем же значением шифрующей экспоненты. Тогда, если некоторое секретное сообщение m было зашифровано и передано всем e абонентам, то злоумышленник может однозначно восстановить его с помощью китайской теоремы об остатках.

2 Лабораторная работа № 4

Задание

1. Зашифровать несколько сообщений. Первое передаваемое сообщение начинается фразой «n Фамилия Имя Отчество … …». Другие – на Ваше усмотрение.
2. Дешифрировать сообщения из пункта 1.
3. В сообщение вставьте «свою» цифровую подпись.
4. Дешифрируйте сообщение и проверьте подпись.
5. Большие простые числа возьмите из контрольной работы № 1. Не менее 9 значащих цифр.