Лабораторная работа №3.
Исследование криптографической системы RSA

Цель работы: Ознакомить студентов с классической криптосистемой с открытым ключом RSA и вариантами ее использования.

Теоретические пояснения

1. Идея криптосистемы RSA

Наиболее широко распространенной системой с открытым ключом является криптосистема RSA (Rivest, Shamir, Adleman). Идея системы состоит в том, что очень сложно разложить произведение двух простых чисел на сомножители, т.е. найти эти сомножители. Сама же идея системы RSA исключительно проста.

Пусть p и q – два случайно выбранных простых числа (каждое примерно по 100 десятичных разрядов). Обозначим: $n = pq$ и $\varphi(n) = (p-1)(q-1)$, где $\varphi(n)$ – функция Эйлера от n. Случайно выбирается большое число $d > 1$, такое, что $(d, \varphi(n)) = 1$, и вычисляется e, $1 < e < \varphi(n)$, удовлетворяющее сравнению: $ed \equiv 1 \bmod \varphi(n)$.

Числа n, e и d называются соответственно модулем, экспонентой зашифрования и экспонентой расшифрования.

Числа n и e образуют открытый ключ, а p,q, $\varphi(n)$ и d секретную лазейку. При этом секретная лазейка включает в себя взаимозависимые величины. Так, если известно p (и, конечно, n и e), то остальные числа лазейки вычисляются просто:

$q = n/p$; $\varphi(n) = (p-1)(q-1)$; d находится из условия: $ed \equiv 1 \bmod \varphi(n)$.

Зашифрование обеспечивается возведением числового фрагмента текста S в степень e по модулю n. Расшифрование достигается возведением результата предыдущего шага в степень d.

При зашифровании получаем $S^e \equiv C \bmod n$. Здесь C – зашифрованный фрагмент текста. При расшифровании $C^d = S^{ed} = S^{1+\varphi(n)k} = S^{\varphi(n)k} S \equiv S \bmod n$.

(6)

Справедливость (6) легко видна, так как из сравнения $ed \equiv 1 \bmod \varphi(n)$ следует, что $ed = 1 + \varphi(n)k$, где k – некоторое целое.

Пример. Пусть $p = 11$, $q = 13$. Тогда $n = 143$, $\varphi(n) = 120$.
Выберем d из условия: $(d, \varphi(n)) = 1$, например, $d = 37$, тогда из сравнения: $ed \equiv 1 \bmod \varphi(n)$ находим $e = 13$. Действительно, $13*37 = 481 \equiv 1 \bmod 120$.

Для зашифрования возьмем фрагмент текста, который закодирован, например, числом $S = 42$. $42^{13} \equiv 3 \bmod 143$, т.е. шифр фрагмента $C = 3$.

Для расшифрования возведем число 3 в степень 37: $3^{37} \equiv 42 \bmod 143$. Таким образом, легальный получатель вычисляет значение исходного кода фрагмента.

2.Использование систем с открытым распределением ключей для абонентских сетей

Рассмотрим несколько близких задач, в которых абоненты обмениваются секретной информацией по открытому каналу.

1). Пусть несколько абонентов A, B, C, договорились об обмене информацией. Они могут выбрать некоторое общее простое число p, такое, что p-1 раскладывается на простые сомножители в первой степени. Число вида $N = p_1p_2p_3\ldots p_k$ называется эвклидовым числом. Каждый из участников выбирает два числа меньших и взаимно простых с p-1 так, чтобы:

$a_1a_2 \equiv b_1b_2 \equiv c_1c_2 \equiv 1 \bmod (p-1)$.

Пусть абонент A хочет передать сообщение S абоненту B. Он кодирует свое сообщение возведением в степень a_1: $S^{a1} \equiv S_1 \bmod p$ и передает его B. Тот в свою очередь кодирует полученное сообщение возведением в степень b_1 : $S_1^{b1} \equiv S_2 \bmod p$ и возвращает его A. A возводит его в степень a_2 и передает его B: $S_2^{a2} \equiv S_3 \bmod p$. B возводит его в степень b_2 и читает сообщение. Справедливость результата следует из сравнения: $a_1b_1a_2b_2 \equiv 1 \bmod (p-1)$.

Пример. Пусть абоненты A, B и C выбрали число p = 103. Это число простое, причем 103-1 = 102 – эвклидово число, так как представляется в виде произведения простых чисел в первых степенях: 102 = 2*3*17. Каждый из участников выбирает пару секретных ключей:

A: $a_1 = 25$, $a_2 = 49$,

B: $b_1 = 19$, $b_2 = 43$,

C: $c_1 = 35$, $c_2 = 35$.

Пусть теперь A посылает к B сообщение S = 67. Он возводит его в степень 25 и находит остаток по модулю 103: $67^{25} \equiv 86 \bmod 103$. B возводит его в степень $b_2 = 19$ и отправляет результат к A: $86^{19} \equiv 96 \bmod 103$. A возводит полученное сообщение в степень 49 и передает его B: $96^{49} \equiv 21 \bmod 103$. B получив сообщение, возводит его в степень 43 и читает исходный текст: $21^{43} \equiv 67 \bmod 103$. Таким образом, S = 67.

Открытым ключом в этой системе является модуль p. Недостатком такой системы является большое число передач от одного абонента к другому.

2). Пусть имеется абонентская сеть и требуется обеспечить связь между любой парой пользователей. Если из одного центра заранее передать открытые ключи g и p каждому пользователю, то они могут выработать общий ключ следующим образом. Пусть абонент A сам придумал ключ k_1, а абонент B ключ k_2 (это индивидуальные секретные ключи абонентов). A посылает к B сообщение $g^{k1} \bmod p$, а B посылает к A сообщение $g^{k2} \bmod p$. B возводит полученное сообщение в степень k_2, а A в степень k_1. В результате они выработают одинаковый общий ключ: $g^{k1k2} = g^{k2k1} \equiv K \bmod p$, после чего возможен обмен информацией по открытому каналу с использованием любой классической (симметричной) криптосистемы.

3.Криптографические протоколы

В традиционных (классических) криптографических системах предполагалось, что два лица, которые обмениваются секретной информацией, полностью доверяют друг другу и пытаются защитить свои сообщения от третьих лиц (перехватчиков, криптоаналитиков).

Криптография с открытым ключом значительно расширила класс задач, решаемых с помощью криптографических методов. В результате появилась необходимость в интерактивных , многоразовых двусторонних обменах сообщениями между участниками, которые не всегда доверяют друг другу, в передаче информации между несколькими участниками. Последовательность действий участников обмена информацией, использующих криптографические приемы для решения нетрадиционных задач, называют криптографическими протоколами.

4.Банки и клиенты

Рассмотрим задачу, в которой клиенты банка $v_1, v_2, \ldots v_k$ передают шифрованное распоряжение ответственному работнику банка B (банкиру). При этом кроме конфиденциальности должна обеспечиваться узнаваемость клиента, чтобы по полученному сообщению банкир B сумел идентифицировать автора сообщения и выполнить именно его распоряжение.

Банкир B выбирает некоторое число N = PQ, где P и Q – большие простые числа. Каждый из клиентов v_i (i = 1,2,3,…,k) также выбирают свои значения $n_i = p_iq_i$, причем

желательно, чтобы $N > n_i$. Затем как банкир, так и клиенты находят значения $\varphi(N)$ – банкир и $\varphi(n_i)$ – все клиенты.

После чего каждый выбирает свой открытый ключ D - ,банкир и d_i – клиенты из условий:

$0 < D < \varphi(N)$, $(D, \varphi(N)) = 1$ – банкир и

$0 < d_i < \varphi(n_i)$, $(d_i, \varphi(n_i)) = 1$ – клиенты.

Затем банкир и клиенты находят свои секретные ключи T и t_i из сравнений:

$DT \equiv 1 \bmod \varphi(N)$, $0 < T < \varphi(N)$ – банкир,

$dt \equiv 1 \bmod \varphi(n_i)$, $0 < t < \varphi(n_i)$ – клиенты.

После этих операций открыто публикуется телефонная книга с открытыми ключами:

B: N, D

v_i: n_i, d_i.

Пусть теперь некоторый клиент v_i хочет передать распоряжение m банкиру B. Он шифрует его сначала своим секретным ключом (возводя m в степень t_i по mod n_i, а затем открытым ключом банкира: $m_1 \equiv m^{ti} \bmod n_i$, $m_2 \equiv m_1^D \bmod N$. Сообщение m_2 передается по открытому каналу связи. Банкир, получив сообщение m_2 сначала расшифровывает его своим секретным ключом T, а затем открытым ключом d_i клиенты v_i. В результате получает: $m_3 \equiv m_2^T \bmod N$, $m_4 \equiv m_3^{di} \bmod n_i$. При этом $m_4 = m$, т.е. банкир B расшифровывает переданное ему распоряжение, при этом заодно и идентифицирует (узнает) клиента. Это похоже на проверку подписи клиента и иногда называется “электронная подпись”. Если клиент из открытой телефонной книги узнает, что банкир выбрал число $N < n_i$, то изменив порядок шифровки получит тот же результат, если банкир также изменит порядок расшифровки.

Пример. Пусть банкир выбрал простые числа P = 23, Q = 11; клиент v: p = 13, q = 7. После чего и банкир и клиент вычисляют сначала функции Эйлера: $\varphi(23*11) = 220$; $\varphi(13*7) = 72$, затем выбирают открытые и вычисляют секретные ключи, например: D = 71, T = 31; d = 29, t = 5. Открыто публикуются числа: P*Q = 253, p*q = 91, D = 71, d = 29. Секретным ключом банкира является число T = 31, а секретным ключом клиента t = 5.

Пусть клиент решил дать секретное поручение банкиру в виде числа m = 41. Он шифрует его своим секретным ключом t, а затем открытым ключом банкира D:
$41^5 \equiv 6 \bmod 91$, $6^{71} \equiv 94 \bmod 253$. Это сообщение (число 94) по открытому каналу передается банкиру. Банкир расшифровывает сообщение сначала своим секретным ключом T, а затем открытым ключом клиента d: $94^{31} \equiv 6 \bmod 253$, $6^{29} \equiv 41 \bmod 77$. Банкир принимает указание клиента в виде числа 41.

Использованные источники

1. Ерош И.Л., Дискретная математика. Математические вопросы криптографии. Учебное пособие. СПбГУАП. 2001г.
2. Ерош И.Л. Дискретная математика. Теория чисел. Учебное пособие. СПбГУАП.2001г.

Порядок выполнения лабораторной работы

1. Прочитайте теоретический материал и рассмотрите отдельно каждый вариант применения RSA, запустите программу на компьютере.
2. Общий ключ для двух пользователей. Выберите некоторое простое число p и число g – примитивный корень по модулю p. Примитивным корнем g по модулю p называется число, все степени которого $g_1, g_2, \ldots g_{n-1}$ различны. Придумайте некоторые произвольные числа k_1 и k_2 (ключи). Выполните на компьютере последовательность

действий, обеспечивающих выработку общего ключа k для двух пользователей. Вручную проверьте правильность вычислений.

3. Передача шифрованных сообщений. Возьмите два простых числа p и q, найдите их произведение n= pq и функцию Эйлера φ(n), выберите d из условия (d, φ(n)) = 1. Введите эти данные в компьютер и посмотрите, какой закрытый ключ будет вычислен. Для абонента A, имеющего только открытую информацию введите некоторый символ и автоматически получите его ASCII-код. Нажмите кнопку «Зашифровать» и запишите полученное сообщение. Передайте это сообщение абоненту B, нажмите кнопку «Расшифровать» и убедитесь, что расшифрование выполнено правильно. При ошибках (Ваших) в выборе простых чисел и вычислении φ(n) и d зашифрование будет невозможным. В этом случае проанализируйте свои ошибки.
4. Сообщение от клиентов банку. Представив себя банкиром B, выберите простые числа P и Q; затем представив себя клиентами v_i , выберите несколько пар простых чисел p_i и q_i , вычислите и за банкира и за клиентов значения функций Эйлера и все открытые ключи. Введите полученные данные в компьютер. Выберите номер клиента и некоторый символ и введите их в компьютер, автоматически получив ASCII-код. Зашифруйте его и передайте банку, получите протокол с этапами зашифрования и расшифрования. Проанализируйте этот протокол и запишите, какие действия выполняются согласно этому протоколу. Если результат положительный, то Вам будет предложено использовать сформированные Вами данные для посимвольной передачи неизвестного Вам сообщения от выбранного Вами клиента банку. Запишите полученное после расшифровки сообщение. Представив себя клиентом, выдающим банку себя за другого, воспользуйтесь открытой информацией и попытайтесь передать сообщение банку. Проанализируйте результат.
5. Оформите отчет. Отчет должен содержать:
   a) Титульный лист с указанием университета, кафедры, дисциплины, названия лабораторной работы, № группы, фамилии студента и преподавателя.
   b) Все решения, выполненные вручную.
   c) Комментарии при проверке решений на компьютере.