С давних времен человечество волновали проблемы защиты информации. Необходимость защищать информацию возникла из потребностей тайной передачи сообщений, как военных, так и дипломатических. Например, у китайцев простая запись сообщения с помощью иероглифов делала его тайным для чужестранцев [1]. Греки нашли другое необычное решение для обеспечения тайны переписки: они брили наголо голову раба и выцарапывали на ней свое послание. Когда волосы на голове раба отрастали вновь, его посылали доставить сообщение. Получатель брил голову раба и прочитывал текст. Ясно, что способ этот очень ненадежен и вдобавок неэффективен. Всякий осведомленный о таком способе связи мог схватить раба, побрить ему голову и прочесть послание. Более того, на отправку сообщения и получение ответа таким способом уходило несколько недель [2]. Юрий Цезарь придумал способ получше. Каждую букву сообщения он заменял на другую, которая в латинском алфавите отстояла от исходной на три позиции дальше. Цезарь вошел в историю, а «шифр Юлия Цезаря», как его до сих пор называют, служит примером одной из первых систем шифрования [2]. Для обозначения всей области тайной (секретной) связи используется термин «криптология», который происходит от греческого «cryptos» - тайный и « logos» - сообщение [1. Существует два вида шифрования информации – симметричное шифрование и асимметричное относительно преобразования расшифрования. Поэтому можно выделить два класса криптосистем: · симметричные (одноключевые) криптосистемы; · асимметричные (двухключевые) криптосистемы (с открытым ключом). Системы шифрования с открытыми ключами применяются для организации конфиденциальной связи между пользователями в сети. Они являются эффективными системами криптографической защиты данных. Для зашифрования и расшифрования пересылаемых данных используются два разных ключа, их называют открытым и секретным (или закрытым) ключами. Именно поэтому системы носят название асимметричные. Открытый ключ может использовать любой пользователь (отправитель информации), который занимается зашифровыванием информации. Но с помощью этого ключа обратное расшифрование данных осуществить невозможно. Для расшифровывания информации используется второй ключ – секретный и им владеет только получатель зашифрованной информации. Секретный ключ невозможно определить исходя из знания открытого ключа. Схема асимметрической криптосистемы с открытым ключом представлена на рисунке 1. Рис. 1 – Схема асимметрической криптосистемы с открытым ключом Особенности асимметрических криптосистем: · Открытый ключ и зашифрованная информация (криптограмма) могут отправляться по незащищенному каналу, т.е. могут быть известны противнику. · Алгоритмы шифрования и расшифрования являются открытыми. · Защита информации производится за счет секретности закрытого ключа. В 1978 году три автора: Р.Райвест (Rivest), А.Шамир (Shamir) и А.Адлеман

(Adleman) предложили алгоритм шифрования данных RSA, который был назван по первым буквам фамилий его автора. Это первая серьезная система шифрования с открытым ключом, которая используется и сегодня. Основанием криптосистемы RSA является то, что большие числа сложно разложить на множители [3]. В криптосистеме RSA открытый и закрытый ключи, исходное сообщение и зашифрованное сообщения принадлежат множеству целых чисел Zn = { 0, 1, 2, … , N-1 }, где N – модуль: N = P*Q. P и Q – случайные большие простые числа. Они хранятся в секрете для обеспечения наибольшей безопасности. Множество Zn с операциями сложения и умножения по модулю N образуют арифметику по модулю N. Далее выбирается случайный открытый ключ, удовлетворяющий условиям: · 1секретный ключ φ(N); · НОД (открытый ключ, φ(N)) = 1, т.е. открытый ключ и φ(N) должны быть взаимно простыми. φ(N) - функция Эйлера, которая указывает количество положительных чисел в интервале от 1 до N. φ(N) = (P-1)*(Q-1) Потом вычисляется секретный ключ (по расширенному алгоритму Евклида): kсекретный = kоткрытый-1 (mod φ(N)) Открытый ключ используется для шифрования данных, а секретный – для их расшифрования. Для более детального изучения рассмотрим зависимость открытых ключей от закрытых в криптосистеме RSA на примере: P = 5; Q = 11; N = P*Q = 55; φ(N) = (P-1)*(Q-1) = 40. Для вычисления всех возможных открытых ключей необходимо найти все числа с учетом выполнения двух условий: · 1секретный ключ φ(N); · НОД (открытый ключ, φ(N)) = 1; Для получения искомого списка открытых ключей будет идти перебор всех возможных чисел, удовлетворяющих условиям [4]: · 1секретный ключ40; · НОД (открытый ключ, 40) = 1. Воспользуемся алгоритмом Евклида 39 раз для вычисления наибольших общих делителей. Пример: НОД (33, 40) = 1 40 = 1*33 + 7 33 = 4*7 + 5 7 = 1*5 + 2 5 = 2*2 + 1 2 = 2*1 + 0 => 33 – открытый ключ; Получаем следующий список открытых ключей: Открытые ключи 1 3 7 9 11 13 17 19 Открытые ключи 21 23 27 29 31 33 37 39 Для нахождения закрытых ключей воспользуемся расширенным алгоритмом Евклида 16 раз (по числу найденных открытых ключей): Пример: Открытый ключ = 33 q u1 u2 u3 v1 v2 v3 - 0 1 40 1 0 33 1 1 0 33 -1 1 7 4 -1 1 7 5 -4 5 1 5 -4 5 -6 5 2 2 -6 5 2 17 -14 1 Закрытый ключ = 17 Получаем следующие списки открытых и соответствующих им закрытых ключей: Открытые ключи 1 3 7 9 11 13 17 19 Закрытые ключи 1 -13 -17 9 11 -3 -7 19 Открытые ключи 21 23 27 29 31 33 37 39 Закрытые ключи -19 7 3 -11 -9 17 13 -1 Для удобства можно пересчитать все отрицательные значения по модулю 40. -13 27 (mod 40) -17 23 (mod 40) -3 37 (mod 40) -7 33 (mod 40) -19 21 (mod 40) -11 29 (mod 40) -9 31 (mod 40) -1 39 (mod 40) Списки открытых и соответствующих им закрытых ключей будут выглядеть так [5]: Открытые ключи 1 3 7 9 11 13 17 19 Закрытые ключи 1 -13 -17 9 11 -3 -7 19 Закрытые ключи 1 27 23 9 11 37 33 19 Открытые ключи 21 23 27 29 31 33 37 39 Закрытые ключи -19 7 3 -11 -9 17 13 -1 Закрытые ключи 21 7 3 29 31 17 13 39 Для того чтобы проиллюстрировать полученные результаты,

построим графики зависимости закрытого ключа от открытого (Рисунок 2): При построении данного графика была обнаружена симметричность расположения точек относительно двух осей (Рисунок 2): · y = x; · y = -x + 40. Построим еще несколько графиков зависимости закрытого ключа от открытого для различных P и Q (рис. 3-6). Рис. 2 – График зависимости закрытого ключа от открытого Рис. 3 - P=29, Q=79 Рис. 4 - P=53, Q=101 Рис. 5 - P=79, Q=127 Рис. 6 - P=101, Q=151 На этих графиках тоже наблюдается симметрия, относительно двух осей. · Для P=29, Q=79: φ(N) = 2184 Оси симметрии: y = x; y = -x +2184 · Для P=53, Q=101: φ(N) = 5200 Оси симметрии: y = x; y = -x +5200 · Для P=79, Q=127: φ(N) = 9828 Оси симметрии: y = x; y = -x +9828 · Для P=101, Q=151: φ(N) = 15000 Оси симметрии: y = x; y = -x +15000 Из вышеизложенного можно обобщить, что графики зависимости закрытых ключей от открытых в криптосистеме RSA симметричны относительно двух осей: · y = x; · y = -x + φ(N) Данную симметричность расположения точек на графике можно использовать при нахождении закрытых ключей, соответствующих найденным открытым ключам. При вычислении каждого закрытого ключа, целесообразно находить ещё и все симметричные ему значения, что поможет ускорить вычисления. Если точка с координатами (открытый ключ, закрытый ключ) принадлежит оси симметрии, то ей будет соответствовать еще одна точка с симметричными координатами, в противном случае ей будет соответствовать еще 3 точки. Рассмотрим принцип работы этого алгоритма на предыдущем примере, где P = 5; Q = 11. Имеем следующий список открытых ключей: Открытые ключи 1 2 7 9 11 13 17 19 Открытые ключи 21 23 27 29 31 33 37 39 Для нахождения закрытых ключей все так же будем использовать расширенный алгоритм Евклида: Открытый ключ = 1, закрытый ключ = 1 Точка с координатами (1,1) принадлежит оси симметрии y = x Можно найти еще 1 точку: (39,39). Открытый ключ = 3, закрытый ключ = 27 Точка с координатами (3,27) не принадлежит осям симметрии Можно найти еще 3 точки: (13,37), (27,3), (37,13). Открытый ключ = 7, закрытый ключ = 23 Точка с координатами (7,23) не принадлежит осям симметрии Можно найти еще 3 точки: (17,33), (23,7), (33,17). Открытый ключ = 9, по закрытый ключ = 9 Точка с координатами (9,9) принадлежит оси симметрии y = x Можно найти еще 1 точку: (31,31) Открытый ключ = 11, закрытый ключ = 11 Точка с координатами (11,11) принадлежит оси симметрии y = x Можно найти еще 1 точку: (29,29) Открытый ключ = 19, закрытый ключ = 19 Точка с координатами (19,19) принадлежит оси симметрии y = x Можно найти еще 1 точку: (21,21) При нахождении закрытых ключей алгоритм Евклида использовался 16 раз, а с использованием осей симметрии – всего 6 раз. То есть с использованием нового алгоритма производительность можно значительно увеличить. В данной статье были рассмотрены принципы систем шифрования с открытыми ключами (асимметрических криптосистем). В частности был разобран алгоритм поиска открытых и закрытых ключей криптосистемы RSA. Была обнаружена симметрия

на графиках зависимости закрытых ключей от открытых, что позволило выработать новый алгоритм их построения, который будет работать быстрее стандартного.