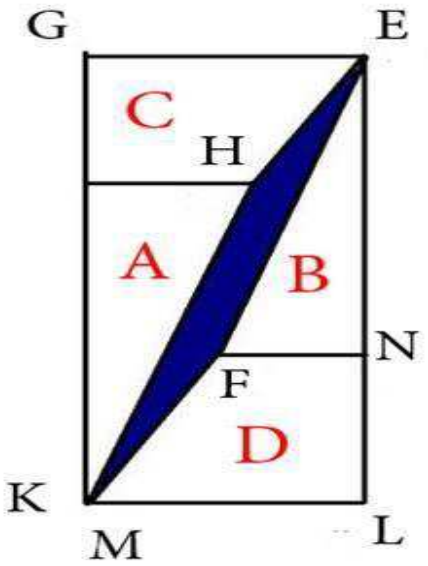
Но площадь прямоугольника окажется равной 65 клеткам, то есть на одну клетку больше, чем площадь первоначально взятого квадрата. Судя по рисунку, длина прямоугольника должна содержать $x + x + x + y = 2x + y = 2 * 5 + 3 = 13$ единиц; ширина прямоугольника x, то есть 5 единиц. Из этого следует, что площадь прямоугольника содержит 5*13=65.



Но у этого прямоугольника не будет получаться точного слияния линий EFK и EHK в одну диагональ EK прямоугольника, так как линия EFK и EHK не прямые, а ломаные с очень небольшим изломом в точках F и H. Площадь прямоугольной фигуры KLEG действительно содержит 65 клеток, но в ней есть ромбовидная щель EFKH, площадь которой как раз составляет одну клетку. Разгадка заключается в том, что точки E, F, K, H не лежат на прямой линии.

Древнегреческий философ Платон говорил: «Когда мы стремимся искать неведомое нам, то становимся лучше, мужественнее и деятельнее, тех, кто полагает, будто неизвестное нельзя найти и незачем искать».

ЛИТЕРАТУРА

1 Больцано Б. Парадоксы бесконечного. – Одесса, 1911.

2 Лямин А. А. Математические парадоксы и интересные задачи. – М., 1911.

3 Ф.Ф. Нагибин, Е.С. Канин «Математическая шкатулка» Москва, «Просвещение», 1988г.

УДК 512.624.95

Студ. А.Н. Зайцев
Науч. рук. асс. Т.Г. Шагова
(кафедра высшей математики, БГТУ)

КРИПТОСИСТЕМА RSA

RSA – криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровую под-

пись, была разработана в 1977 году и названа в честь ее разработчиков Ronald Rivest, Adi Shamir и Leonard Adleman.

Алгоритм RSA работает следующим образом. Берем два достаточно больших простых числа p и q и вычисляем их произведение $n = p \cdot q$; число n называют модулем. Вычисляем функцию Эйлера $\varphi(n)$. В нашем случае $\varphi(n) = (p-1)(q-1)$. Затем выбираем число e, такое, что $1 < e < \varphi(n)$ и взаимно простое с $\varphi(n)$. Вычисляем число d таким образом, что $ed - 1$ делится на $\varphi(n)$, то есть d является обратным элементом к числу e по модулю $\varphi(n)$. Пара чисел (n; e) называется открытым ключом, а (n; d) – закрытым.

Пусть теперь Алиса хочет послать Бобу сообщение M. Алиса создает с помощью открытого ключа зашифрованный текст C, используя формулу $C = M^e \pmod n$, затем посылает его Бобу. Чтобы расшифровать полученное сообщение, Боб вычисляет $C^d \pmod n$, что эквивалентно исходному сообщению M. Зависимость между e и d гарантирует, что Боб вычислит M верно. Так как только Боб знает d, то только он имеет возможность расшифровать полученное сообщение.

Криптосистема RSA обладает высокой степенью надежности. Однако существует ряд способов взлома шифра. Основным из них является факторизация модуля n. Эффективного способа сделать это в наше время не существует. Но следующий ряд методов может облегчить факторизацию. В случае, когда p и q не сильно отличаются друг от друга, то они могут быть найдены довольно быстро методом факторизации Ферма. Тест Полладра-По хорошо факторизует числа только определенного вида. В настоящее время особую популярность приобретают метод факторизации с помощью эллиптических кривых и метод квадратичного решета. Самые эффективные программы используют именно эти методы. Стоит также отметить, что для RSA представляет опасность развитие технологии квантовых компьютеров, так как на квантовых компьютерах разработан алгоритм Шора, факторизующий число за $O(\lg n)$, что фактически означает крах всей криптографии.

Другой способ взлома RSA состоит в том, чтобы найти метод вычисления корня степени e по модулю n. Поскольку $C = M^e \pmod n$, то корнем степени e в кольце вычетов по модулю n является сообщение M. Вычислив корень, можно вскрывать зашифрованные сообщения, даже не зная закрытого ключа. Такая атака не эквивалентна факторингу, но в настоящее время подобные методы неизвестны. В особых случаях, когда на основе одного и того же

показателя относительно небольшой величины шифруется достаточно много связанных сообщений, есть возможность их вскрыть.

Существуют и другие типы атак, позволяющие, однако, вскрыть только одно сообщение и не позволяющие нападающему вскрыть другие, зашифрованные тем же ключом. Самое простое нападение на единственное сообщение – атака по предполагаемому открытому тексту. Нападающий, имея зашифрованный текст, предполагает, что сообщение содержит какой-то определенный текст, затем шифрует предполагаемый текст открытым ключом получателя и сравнивает полученный текст с имеющимся зашифрованным текстом. Такую атаку можно предотвратить, добавив в конец сообщения несколько случайных битов. Другая атака единственного сообщения применяется в том случае, когда кто-то посылает одно и то же сообщение M трем корреспондентам, каждый из которых использует общий показатель. Зная это, нападающий может перехватить сообщения и расшифровать сообщение M. Такую атаку можно предотвратить, вводя в сообщение перед каждым шифрованием несколько случайных битов.

Из-за того, что скорость шифрования данных с помощью RSA крайне мала по сравнению с алгоритмами блочного шифрования (порядка
50-200 кбайт/с, в то время как у DES, например, – порядка гигабайт в секунду), для больших объемов данных используют блочные алгоритмы шифрования, а с помощью RSA шифруют только ключ блочного алгоритма. Это плата за высокую надёжность алгоритма и исключительную криптостойкость.

На настоящий момент нет никаких математических выкладок, показывающих, что факторизация чисел осуществима за разумное время. А это означает, что перспективным направлением атаки является атака не на сам алгоритм, а на сопутствующие информационные системы. И ждать развития квантовых компьютеров.

ЛИТЕРАТУРА

1 Герман О., Нестеренко Ю. Теоретико-числовые методы в криптографии. М: Академия, 2012. 272с.

2 RSA – алгоритм шифрования с открытым ключом [Электронный ресурс] / http://www.paveldvlip.ru/algorithms/rsa.html.