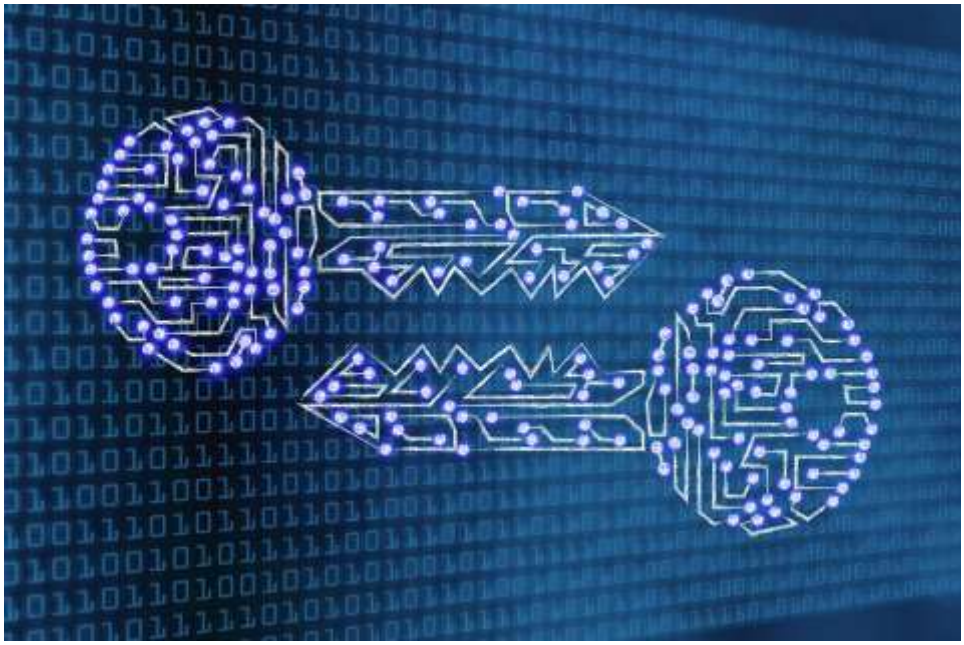
Al-Farabi Kazakh National University

Физико-технический факультет

Специальность – Радиотехника, электроника и телекоммуникации

МЕТОДИЧЕСКАЯ РЕКОМЕНДАЦИЯ

К ЛАБОРАТОРНЫМ РАБОТАМ ПО КРИТОГРАФИЧЕСКИМ АЛГОРИТМАМ



@A.K. Imanbayeva

Как криптография обеспечивает секретность и безопасность связи

Криптографический процесс преобразования текста из читаемой формы в неразборчивую - известную как шифрованный текст - называется шифрованием. Отправка секретных или частных сообщений в виде шифрованного текста является типичным применением криптографии. После получения зашифрованного текста он дешифруется уполномоченным получателем в читаемую форму. Дешифровка (или расшифровка) выполняется с использованием ключа шифрования, который служит для того, чтобы третьи лица не смогли прочитать пересылаемые сообщения.

Методы шифрования использовались многими цивилизациями на протяжении всей истории человечества для предотвращения понимания сообщений неуполномоченными лицами. Юлию Цезарю приписывают одну из самых ранних форм шифрования — так называемый "шифр Цезаря" — для передачи сообщений своим генералам. С развитием цивилизации и усложнением передаваемой информации, к нашему дню криптография стала играть жизненно важную роль в обеспечении приватности, конфиденциальности данных, их целостности и аутентификации в компьютерных системах и сетях. В современном мире, где большинство наших личных и профессиональных коммуникаций и транзакций осуществляется в режиме онлайн, криптография важна как никогда.

Прежде чем приступать к изучению алгоритмов криптографической защиты, необходимо повторить (изучить) основы теории чисел

ОСНОВНЫЕ ТЕМЫ ТЕОРИИ ЧИСЕЛ, ИСПОЛЬЗУЕМЫХ В КРИПТОГРАФИИ, КОТОРЫЕ СЛЕДУЕТ ИЗУЧИТЬ:

Простые и составные числа

Основная теорема арифметики

Взаимно простые числа и функция Эйлера

Арифметика остатков и теория сравнений

Простые и составные числа

Каждое *натуральное число*, большее единицы, делится по крайней мере на два числа: на 1 и на само себя. Если число не имеет делителей, кроме самого себя и единицы, то оно называется **простым**, а если у числа есть еще делители, то **составным**. *Единица* же не считается ни простым числом, ни составным. Например, числа 7, 29 — простые; числа 9, 15 — составные (9 делится на 3, 15 делится на 3 и на 5).

Интересный факт: если два простых числа отличаются на 2, то их называют числами-"близнецами". Чисел-"близнецов" не очень много. Например, "близнецами" являются 5 и 7, 29 и 31, 149 и 151, а также $242\ 206\ 083*2^{38\ 880}\pm1$ (наибольшая найденная на момент написания учебного пособия пара "близнецов").

Не о всяком числе можно сразу сказать, простое оно или составное. Если число меньше ста, то, скорее всего мы сразу сможем ответить на этот вопрос. Однако с большими числами дело сложнее. Возьмем, например, число 2009. Простое оно или составное? Попробуем найти возможные делители этого числа среди первых простых чисел. 2009 определенно не делится на 2 (так как оно нечетное), на 3 (так как сумма его цифр 2+9=11 не делится на 3), на 5. А вот, попробовав разделить 2009 на 7, мы увидим, что в результате получается *целый* результат – 287. Таким образом, получен ответ: число 2009 – составное. В данном случае ответ получен достаточно быстро. Бывает, что проверка на простоту производится гораздо дольше, а для работы с большими целыми числами требуются даже специальные компьютерные программы.

Поиск больших простых чисел имеет важное *значение* для математики и не только. Например, в криптографии большие простые числа используются в алгоритмах шифрования с открытым ключом. Для обеспечения надежности шифрования там используются простые числа длиной до 1024 *бит*.

Перемножить два числа сравнительно нетрудно, особенно если у нас есть калькулятор, а числа не слишком велики. Существует и обратная задача – *задача факторизации* – нахождение двух или более чисел, дающих при перемножении заданное число. Эта задача гораздо труднее, чем перемножение чисел, и любому, кто пытался ее решить, об этом известно. Например, если от нас требуется умножить 67 на 113, то результат, 7571, будет получен, наверно, меньше чем за минуту. Если же от нас требуется найти два числа, *произведение* которых равно 7571, то, скорее всего, это займет у нас гораздо больше времени.

Поиск сомножителей числа n может вестись, например, перебором всех простых чисел до $\sqrt{n},$ как в рассмотренном выше примере с числом 2009. Однако, если множители – большие простые числа, то на их *поиск* уйдет достаточно много времени.

Таким образом, факторизация большого числа требует значительных затрат времени даже в том случае, когда известно, что оно является произведением двух больших простых чисел.

Сложность задачи факторизации используется в некоторых криптографических алгоритмах, например, в системе шифрования *RSA*.

Основная теорема арифметики

Любое составное число можно составить из некоторого количества простых с помощью умножения. Например, составное число 2009 можно получить так:

2009 = 7 * 7 * 41

В математике рассматривается так называемая **основная теорема арифметики**, которая утверждает, что любое *натуральное число* (n>1) либо само является простым, либо может быть разложено на *произведение* простых делителей, причем единственным способом (если не обращать внимания на порядок следования сомножителей).

Воспользовавшись обозначением степени, разложение числа 2009 на простые множители можно записать так:

$2009 = 7^2 * 41$

Разложение на множители называется **каноническим**, если все множители являются простыми и записаны в порядке возрастания.

Например, запишем *каноническое разложение* числа 150 на множители:

$150 = 2 * 3 * 5^2$

Взаимно простые числа и функция Эйлера

Два числа называются взаимно простыми, если они не имеют ни одного общего делителя кроме единицы.

Например, числа 11 и 12 взаимно просты (у них нет общих делителей кроме единицы), числа 30 и 35 — нет (у них есть общий делитель 5).

Исследованием закономерностей, связанных с целыми числами, долго занимался швейцарский математик Леонард Эйлер (Leonard Euler). Одним из вопросов, которым он интересовался, был следующий: сколько существует натуральных чисел, не превосходящих n и взаимно простых с n? Ответ на этот вопрос был получен Эйлером в 1763 году и этот ответ связан с каноническим разложением числа n на простые множители. Так, если

$$n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_n^{a_n}$$

где p_1, p_2, ..., p_n – разные простые множители, то число ϕ натуральных чисел, не превосходящих n и взаимно простых с n можно точно определить по формуле

$$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \cdots \times \left(1 - \frac{1}{p_n}\right)$$

Число натуральных чисел, не превосходящих n и, взаимно простых с n, называется **функцией Эйлера** и обозначается $\phi(n)$.

Например, найдем количество натуральных чисел, не превосходящих 12 и взаимно простых с 12. Из ряда натуральных чисел

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

взаимно простыми (не имеющими общих делителей) с 12 будут только числа 1, 5, 7, 11. Их количество равно четырем. Таким образом $\phi(12) = 4.$

Теперь попробуем подсчитать

$\phi(12)$

по формуле, предложенной Эйлером. Для этого вначале запишем *каноническое разложение* числа 12:

$12 = 2^2 * 3.$

Теперь подсчитаем функцию Эйлера $\phi(12)$:

$$\varphi(12) = 12 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 4 \times 3 \times \frac{12}{23} = 4$$

Значения, вычисленные путем простого перебора взаимно простых чисел и по формуле Эйлера, совпали. Это неудивительно, так как формула для вычисления функции Эйлера может быть доказана строго математически.

Формулу Эйлера удобно использовать для больших n, если известно разложение числа n на простые множители. Для криптографии формула Эйлера важна тем, что она позволяет легко получить число

$\phi(n)$

для простых и некоторых других чисел. В криптографии используются два следующих следствия формулы Эйлера.