ЦИФРОВАЯ КУЛЬТУРА
УНИВЕРСИТЕТ ИТМО

Лекция **«Элементы теории чисел. Алгоритмы RSA и Эль-Гамаля»**

Бойцев Антон Александрович
Романов Алексей Андреевич
Волчек Дмитрий Геннадьевич

Санкт-Петербург
2019

Содержание

1 Элементы теории чисел

1.1 Основные определения

Приведем несколько базовых определений и обозначений, чтобы в дальнейшем общаться на одном языке. Скорее всего, все эти понятия хорошо известны из школы. Чтобы укоротить некоторые формулировки, множество натуральных чисел будем обозначать $\mathbb{N}$. В это множество входят числа $1, 2, 3, 4, ..., 100, ...$ Множество целых чисел будем обозначать $\mathbb{Z}$. Это множество состоит из чисел $..., -100, ..., -2, -1, 0, 1, 2, ..., 100, ...$

Определение 1.1 *Говорят, что число $a \in \mathbb{Z}$ делится на число b, если существует такое число $k \in \mathbb{Z}$, что*

$$a = kb.$$

Обозначают это

$$a \vdots b.$$

При этом число b называется делителем числа a, а число a называется кратным числу b.

Полезно заметить, что число k, возникшее в определении, тоже является делителем a, и, в свою очередь, число a является числом, кратным k.

Пример 1.2 *Так как $24 = 6 \cdot 4$, то числа 6 и 4 являются делителями числа 24.*

Особую роль играют числа p, имеющие в качестве делителей только числа ± 1 и $\pm p$.

Определение 1.3 *Целые числа p, имеющие в качестве делителей только числа ± 1 и $\pm p$ (так называемые несобственные делители), называются простыми. Остальные целые числа называются составными.*

Замечание 1.4 *Обычно, но не всегда, простыми числами называют те простые, которые > 1. Мы тоже будем придерживаться этого определения.*

Замечание 1.5 *Число 1 в этом случае не является ни простым, ни составным.*

Итак, несколько простых чисел: $2, 3, 5, 7, 11, ...$

Фундаментальную роль в арифметике играет так называемая основная теорема арифметики.

1.2 Основная теорема арифметики

Теорема 1.6 (Основная теорема арифметики) *Любое $a \in \mathbb{N}$, $a \neq 1$ может быть быть записано в виде произведения простых чисел*

$$a = p_1 \cdot p_2 \cdot ... \cdot p_k,$$

причем эта запись единственна с точностью до порядка сомножителей.

Казалось бы, для нас эта теорема настолько естественна, что не требует никаких обоснований. Однако, как и любая теорема, она должна иметь доказательство. Попробуйте его привести. Кроме того, используя этот результат, довольно легко доказать, что множество простых чисел бесконечно (так называемая теорема Евклида). Попробуйте это сделать.

Замечание 1.7 *Обратите внимание, что если собрать повторяющиеся простые сомножители в представлении*

$$a = p_1 \cdot p_2 \cdot ... \cdot p_k,$$

то мы получим представление

$$a = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_t^{r_t},$$

где все $r_1, ..., r_t > 0$.

Пример 1.8 *Ясно, что*

$$240 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5.$$

Кроме того, можно записать

$$240 = 2^4 \cdot 3 \cdot 5.$$

Из основной теоремы арифметики следует, что любое целое число, не равное 1, имеет представление

$$a = \pm p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_t^{r_t},$$

где все $r_1, ..., r_t > 0$. Допуская, что некоторые показатели простых чисел могут быть нулевыми, заключаем, что любые два целых числа могут быть записаны в виде произведения степеней одних и тех же простых чисел (ну, и соответствующего знака), а именно

$$a = \pm p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_k^{r_k}, \quad b = \pm p_1^{s_1} \cdot p_2^{s_2} \cdot ... \cdot p_k^{s_k}$$

Пример 1.9 *Пусть* $a = 240$, $b = -700$. *Тогда*

$$a = 2^4 \cdot 3 \cdot 5, \quad b = -2^2 \cdot 5^2 \cdot 7$$

и можно записать

$$a = 2^4 \cdot 3 \cdot 5 \cdot 7^0, \quad b = -2^2 \cdot 3^0 \cdot 5^2 \cdot 7.$$

Определение 1.10 (НОД) *Пусть даны* 2 *целых числа* a *и* b, *имеющие представления*

$$a = \pm p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_k^{r_k}, \quad b = \pm p_1^{s_1} \cdot p_2^{s_2} \cdot ... \cdot p_k^{s_k},$$

где $r_1, ..., r_k, s_1, ..., s_k \geq 0$. *Наибольших общим делителем* a *и* b *называется число*

$$p_1^{m_1} \cdot p_2^{m_2} \cdot ... \cdot p_k^{m_k},$$

где $m_k = \min(r_k, s_k)$ *и обозначается* (a, b).

Можно легко показать, что наибольший общий делитель оправдывает свое название – это и правда наибольшее натуральное число, на которое делятся как a, так и b.

Пример 1.11 *Возвращаясь к примеру,*

$$a = 2^4 \cdot 3 \cdot 5 \cdot 7^0, \quad b = -2^2 \cdot 3^0 \cdot 5^2 \cdot 7.$$

Тогда

$$(a, b) = 2^2 \cdot 3^0 \cdot 5 \cdot 7^0 = 20.$$

Определение 1.12 *Числа, наибольший общий делитель которых равен* 1, *называются взаимно простыми.*

Пример 1.13 *Любые два простых числа являются взаимно простыми. Взаимно простыми могут быть и составные числа. Например,*

$$10 = 2 \cdot 3^0 \cdot 5 \cdot 7^0, \quad 21 = 2^0 \cdot 3 \cdot 5^0 \cdot 7.$$

Тогда

$$(10, 21) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 = 1.$$

1.3 Кольца вычетов

Все мы со школы отлично знаем (и, может быть, даже умеем доказывать) следующую важную теорему о делении с остатком, касающуюся целых чисел $\mathbb{Z}$.

Теорема 1.14 *Пусть $a, b \in \mathbb{Z}$. Тогда существуют единственные $p, r \in \mathbb{Z}$, что*

$$a = pb + r,$$

причем $0 \leq r < |b|$

Определение 1.15 *Число p часто называют целой частью при делении a на b, а число r – остатком от деления числа a на число b.*

Замечание 1.16 *Если остаток равен нулю, то это означает, что число a делится на b.*

Если говорить в терминах обыкновенных дробей, то теорему в вольной форме можно озвучить так: для любой дроби справедливо представление

$$\frac{a}{b} = p + \frac{r}{b},$$

где последняя дробь правильная (то есть модуль числителя меньше модуля знаменателя).
Оказывается, в некоторых задачах бывает удобно отождествлять те числа, которые имеют одинаковый остаток от деления на данное фиксированное число $n \in \mathbb{N}$. Дадим этой фразе более корректную формулировку.

Определение 1.17 *Пусть $n \in \mathbb{N}$. Будем говорить, что $a \in \mathbb{Z}$ сравнимо с $b \in \mathbb{Z}$ по модулю n, если $(a - b) \vdots n$. Обозначать мы это будем записью*

$$a \equiv b \pmod{n}.$$

Последнюю запись часто называют сравнением по модулю n.

Конечно, такое определение затуманивает суть происходящего (математики так делать очень любят). По сути, написанное означает, что остатки от деления a и b при делении на число n равны, то есть справедливо следующее наблюдение

Лемма 1.18 *$a \equiv b \pmod{n}$ тогда и только тогда, когда остатки от деления чисел a и b на число n равны.*

Пример 1.19 *Пусть* $n = 5$, $a = 32$. *Ясно, что*

$$32 = 6 \cdot 5 + 2.$$

Значит, любое число, дающее остаток 2 *при делении на* 5 *будет сравнимо с числом* 32. *Ясно, что общий вид такого числа выписывается явно*

$$b = 5k + 2,\ k \in \mathbb{Z}.$$

Введенное нами определение позволяет отождествлять те числа, которые дают одинаковый остаток от деления на n. Иными словами, все множество целых чисел $\mathbb{Z}$ оказалось разбито на объединение непересекающихся n множеств: $[0]_n, [1]_n, ..., [n-1]_n$, где

$[i]_n$– множество тех целых чисел. что дают остаток i при делении на n.

Обоснование этого следует из следующих важных свойств сравнений, а именно

Лемма 1.20 *1.* $a \equiv a \pmod{n}$;

2. $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$;

3. $a \equiv b \pmod{n},\ b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Итак, рассматривая число $n \in \mathbb{N}$, у нас естественным образом возникает n множеств. Дадим формальное определение

Определение 1.21 *Множество* $[i]_n$ *(то есть множество чисел, которые при делении на* n *дают в остатке* i*), в которое входит число* $a \in \mathbb{Z}$, *называется вычетом числа* a *по модулю* n.

Определение 1.22 *Набор множеств* $[0]_n, [1]_n, ..., [n-1]_n$ *называют полной системой вычетов по модулю* n

Последнее определение обусловлено тем, что по модулю n у целого числа нет других остатков, кроме как $0, 1, 2, ..., (n-1)$. Оказывается, что сравнения обладают следующими важными свойствами, а именно

Лемма 1.23 *1. Если* $a \equiv b \pmod{n}$ *и* $c \equiv d \pmod{n}$, *то* $(a+c) \equiv (b+d) \pmod{n}$;

2. Если $a \equiv b \pmod{n}$ *и* $c \equiv d \pmod{n}$, *то* $ac \equiv bd \pmod{n}$;

3. Если $ka \equiv kb \pmod{n}$ *и* $(k, n) = d$, *то* $a \equiv b \pmod{\frac{n}{d}}$;

4. *Если* $a \equiv b \pmod{n}$, *то* $ka \equiv kb \pmod{n}$ *или даже* $ka \equiv kb \pmod{(kn)}$.

Доказательство. Чтобы не быть совсем голословными, давайте докажем, например, свойство 2, которым будем активно пользоваться в дальнейшем. $a \equiv b \pmod{n}$, означает, что $(a-b) \vdots n$, то есть существует число $t \in \mathbb{Z}$, что $a - b = nt$. Аналогично, существует $k \in \mathbb{Z}$, что $c - d = nk$. Тогда

$$ac = (b + nt)(d + nk) = bd + n(bk + td + nkt),$$

где $(bk + td + nkt)$ – целое, что и доказывает утверждение. □

Приведенные свойства позволяют легко вычислять остатки от деления, например, степеней некоторого числа.

Пример 1.24 *Пусть требуется найти остаток от деления числа* 13^{11} *на* 35, *то есть найти* $0 \leq x < 35$, *что*

$$x \equiv 13^{11} \pmod{35}.$$

Ясно, что $13 \equiv 13 \pmod{35}$. *Далее,*

$$13^2 = 169 = 140 + 29 = 35 \cdot 4 + 29 \equiv 29 \equiv -6 \pmod{35},$$

$$13^3 = 13^2 \cdot 13 \equiv -6 \cdot 13 \pmod{35},$$

а $-78 \equiv -8 \pmod{35}$, *откуда* $13^3 \equiv 27 \pmod{35}$. *Так как*

$$13^4 = 13^2 \cdot 13^2 \equiv 36 \pmod{35},\ 36 \equiv 1 \pmod{35} \Rightarrow 13^4 \equiv 1 \pmod{35},$$

то

$$13^{11} = 13^8 \cdot 13^3 \equiv 1 \cdot 27 \pmod{35}$$

и

$$13^{11} \equiv 27 \pmod{35}.$$

Пример 1.25 *Найти остаток от деления* 2^{100} *на* 125. *Для этого нужно найти такое число* $0 \leq x < 125$, *что* $x \equiv 2^{100} \pmod{125}$.
Так как $2^7 = 128 \equiv 3 \pmod{125}$, *то* $2^{35} = (2^7)^5 \equiv 3^5 \equiv 243 \equiv -7 \pmod{125}$, $2^{50} = 2^{35} \cdot 2 \cdot (2^7)^2 \equiv -126 \equiv -1 \pmod{125}$, *откуда*

$$2^{100} \equiv 1 \pmod{125}$$

1.4 Функция Эйлера и некоторые ее свойства

В теории чисел и приложениях богатое применение имеет так называемая функция Эйлера.

Определение 1.26 (Функция Эйлера) *Функция $\varphi : \mathbb{N} \to \mathbb{N}$, возвращающая по числу n количество взаимно простых чисел с ним, не превосходящих n, называется функцией Эйлера. При этом полагают $\varphi(1) = 1$.*

Пример 1.27 *Вычислим $\varphi(15)$. Так как $15 = 3 \cdot 5$, то из ряда $1, 2, 3, ..., 15$ нужно исключить все числа, делящиеся либо на 3, либо на 5. Тогда останутся числа*

$$1, 2, 4, 6, 7, 8, 11, 13,$$

то есть $\varphi(15) = 8$.

Из только что данного определения сразу следует, что если p – простое число, то

$$\varphi(p) = p - 1.$$

Действительно, до числа p находится ровно $(p-1)$ натуральное число. Так как p простое, то оно взаимно просто с каждым из них.
Для вычисления функции Эйлера от составного числа можно воспользоваться ее важным свойством, свойством мультипликативности, а именно

Лемма 1.28 (О мультипликативности функции Эйлера) *Если $m = nk$, где $m, n, k \in \mathbb{N}$ и $(n, k) = 1$, то*

$$\varphi(m) = \varphi(nk) = \varphi(n)\varphi(k).$$

Если p – простое, $n \in \mathbb{N}$, то

$$\varphi(p^n) = p^n - p^{n-1}.$$

Пример 1.29 *Вычислить $\varphi(117)$. Так как $117 = 13 \cdot 3^2$, а $\varphi(13) = 12$, $\varphi(3^2) = 3^2 - 3 = 6$, то*

$$\varphi(117) = \varphi(13)\varphi(3^2) = 12 \cdot 6 = 72.$$

С функцией Эйлера связано еще одно важное утверждение теории чисел, так называемая теорема Эйлера.

Теорема 1.30 (Теорема Эйлера) *Пусть $(a, n) = 1$, тогда*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Вернемся к уже ранее разобранному примеру

Пример 1.31 *Найти остаток от деления числа 2^{100} на 125. Так как $125 = 5^3$, то $\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100$, откуда*

$$2^{100} \equiv 1 \pmod{125}.$$

1.5 Решение линейных сравнений

Рассмотрим общую задачу о нахождении такого множества X, что для каждого $x \in X$

$$ax \equiv b \pmod{n}.$$

Возможны следующие варианты.
1. $(a, n) = 1$. Мы знаем, что согласно теореме Эйлера,

$$1 \equiv a^{\varphi(n)} \pmod{n}.$$

Тогда

$$ax \equiv ba^{\varphi(n)} \pmod{n}$$

и

$$x \equiv ba^{\varphi(n)-1} \pmod{n}.$$

Если x пробегает полную систему вычетов по модулю n, то ax тоже пробегает полную систему вычетов, а значит только при одном значении x, взятом из полной системы, решение возможно. Тем самым, решение единственно.
2. Если $(a, n) = d > 1$ и $b \vdots d$, то поделим наше сравнение на d и перейдем к сравнению

$$a_1 x \equiv b_1 \pmod{n_1},$$

причем $(a_1, d_1) = 1$. По предыдущему пункту, такое сравнение имеет решение $x \equiv b_1 a_1^{\varphi(n_1)-1} \pmod{n_1}$. Ясно, что исходное сравнение имеет d решений, причем все они могут быть выписаны, как

$$x \equiv b_1 a_1^{\varphi(n_1)-1} + n_1 k \pmod{n}, \quad k = 0, ..., (d-1).$$

3. Если же $(a, n) = d > 1$, но b не делится на d, то сравнение, очевидно, решений не имеет.

Пример 1.32 *Решить сравнение*

$$3x \equiv 7 \pmod{5}.$$

Так как $(3, 5) = 1$, *то сравнение имеет единственное решение. Так как* $\varphi(5) = 4$, *то*

$$x \equiv 7 \cdot 3^3 \pmod{5} \text{ } \textit{или} \text{ } x \equiv 189 \pmod{5}.$$

Упростив, можно записать

$$x \equiv 4 \pmod{5}.$$

Замечание 1.33 *Часто число* $b \cdot a^{\varphi(n)-1}$ *оказывается очень большим, особенно, если* n *большое. Чтобы уменьшить это число можно поступить либо так, как мы делали в первой части, либо сразу использовать несколько другой подход. Так как*

$$3x \equiv 7 \pmod 5,$$

то

$$3x \equiv 7 + 5 \pmod 5, \text{ откуда } 3x \equiv 12 \pmod 5.$$

Так как $(3, 5) = 1$*, то получим эквивалентное сравнение*

$$x \equiv 4 \pmod 5.$$

Пример 1.34 *Решить сравнение*

$$6x \equiv 15 \pmod 9.$$

Так как $(6, 9) = 3$*, то, поделив на* 3*, получим сравнение*

$$2x \equiv 5 \pmod 3.$$

Так как в то же время $2x \equiv 5 + 3 \pmod 3$*, то есть* $2x \equiv 8 \pmod 3$*, получим*

$$x \equiv 4 \pmod 3.$$

Тогда для исходного сравнения получим три решения

$$x \equiv 4 \pmod 9, \quad x \equiv 7 \pmod 9, \quad x \equiv 10 \pmod 9.$$

Последнее можно так же переписать, $x \equiv 1 \pmod 9$.

Пример 1.35 *Решить сравнение*

$$2x \equiv 5 \pmod 8.$$

Так как $(2, 8) = 2$*, но* 5 *не делится на* 2*, то решений сравнение не имеет.*

2 Шифрование информации

2.1 Алгоритм шифрования RSA

Рассмотрим подробно алгоритм шифрования RSA – криптографический алгоритм с открытым ключом, который основан на вычислительной сложности разложения на множители больших чисел. Алгоритм генерации ключей может быть записан по шагам следующим образом:

1. Выбирается два различных простых числа p, q.
2. Вычисляется их произведение $N = p \cdot q$, называемое модулем.
3. Вычисляется $\varphi(N) = (p-1) \cdot (q-1)$.
4. Выбирается целое число $1 < c < \varphi(N)$ такое, что НОД$(c, \varphi(N)) = 1$. При этом число c называют открытой экспонентой (public exponent).
5. Вычисляется число d, решая сравнения $cd \equiv 1 \pmod{\varphi(N)}$. При этом число d называется секретной экспонентой.
6. Пара $\{c, N\}$ является открытым ключом, а пара $\{d, N\}$ – закрытым, его держат в секрете.

Предположим, что мы хотим передать сообщение от Боба Алисе. Тогда Боб должен знать открытый ключ Алисы, чтобы зашифровать сообщение, а Алиса должна использовать свой секретный ключ, чтобы его расшифровать. Пусть Боб хочет послать Алисе сообщение m. Сообщением выступают целые числа в диапазоне $0, ..., (N-1)$. Тогда Боб выполняет следующие действия:

1. По открытому ключу $\{c, N\}$ Алисы вычисляет $e = m^c \pmod{N}$.
2. Передает зашифрованное число e.

Чтобы Алиса могла расшифровать сообщение, она поступает по следующему алгоритму:

1. Принимает зашифрованное сообщение e.
2. С помощью своего секретного ключа $\{d, N\}$ вычисляет $x \equiv e^d \pmod{N}$. Число $x = m$ и есть то сообщение m, что зашифровал Боб.

2.1.1 Пример шифрования чисел

Рассмотрим простой пример, демонстрирующий все этапы вычислений. Для начала, сформируем открытый и закрытый ключи, для этого:

1. Выберем, например, простые числа $p = 3$, $q = 7$.
2. Вычислим модуль $N = 3 \cdot 7 = 21$.
3. Найдем функцию Эйлера от модуля: $\varphi(N) = (3-1) \cdot (7-1) = 12$.
4. Выберем число c, меньшее 21 такое, что НОД$(c, 12) = 1$. Например, пусть $c = 5$.
5. Тогда d найдем из сравнения

$$5d \equiv 1 \pmod{12},$$

откуда $5d \equiv 1 + 24 \pmod{12}$ и $d \equiv 5 \pmod{12}$. Ясно, что в качестве d подойдет значение 5, однако, чтобы не путать величины d и c, выберем $d = 17$.

6. Тем самым, пара $\{5, 21\}$ – открытый ключ, а пара $\{17, 21\}$ – секретный.

Пусть Боб хочет передать Алисе сообщение $m = 19$. Тогда он, по открытому ключу $\{5, 21\}$, вычисляет

$$e \equiv 19^5 \pmod{21}.$$

Так как $19^2 = 361 \equiv 4 \pmod{21}$, то

$$19^5 = 19^2 \cdot 19^2 \cdot 19 \equiv 4 \cdot 4 \cdot 19 \pmod{21}.$$

Но $304 \equiv 10 \pmod{21}$, а значит $e = 10$.

Алиса, получив сообщение e, использует свой секретный ключ. Для этого она вычисляет

$$x \equiv 10^{17} \pmod{21}.$$

Так как $10^2 = 100 \equiv 16 \pmod{21}$, $10^4 \equiv 256 \equiv 4 \pmod{21}$, то

$$10^{17} \equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 10 = 2560 \equiv 19 \pmod{21}.$$

Тем самым, Алиса получает сообщение 19.

2.1.2 Пример шифрования текстовой информации

Что делать в ситуации, когда нам требуется зашифровать и передать некоторый текст, а не число? Например, наша цель – закодировать фразу

`Сизифов труд`

Каким образом можно поступить? Давайте каждой букве, каждому символу, присвоим некоторое число. В прочем, это давно придумано и называется кодом ASCII. В нем 255 символов, а значит, для успешного кодирования любого символа, модуль N должен быть больше, чем 255. Выберем, для примера, $p = 17$, $q = 23$. Тогда $N = 17 \cdot 23 = 391$. Ясно, что $\varphi(N) = 16 \cdot 22 = 352$. Пусть $c = 301$, тогда d находится из сравнения

$$301d \equiv 1 \pmod{352}$$

и $d = 69$. Тем самым, пара $\{301, 391\}$ – открытый ключ, а пара $\{69, 391\}$ – секретный ключ.

Приступим к кодированию.
Буква `С` в ASCII таблице имеет код 209, тогда ее закодированное значение получим из сравнения

$$e \equiv 209^{301} \pmod{391},$$

откуда $e = 292$.
Следующий символ – буква `и` имеет в ASCII код 232. Закодировав, получим

$$e \equiv 232^{301} \pmod{391},$$

откуда $e = 177$.
Итого, вместо первых двух наших символов мы будем передавать 292177.
Отметим один важный момент. Для того, чтобы процесс раскодирования не вызывал больших трудностей, мы будем кодировать каждый символ тремя цифрами. Например, если закодированное сообщение имеет вид $e = 3$, то мы будем передавать 003, а если сообщение имеет вид $e = 32$, то будем передавать 032. Продолжая процесс, получим полное закодированное сообщение:

$$292177300177316255020121174304156329.$$

Опишем теперь процесс раскодирования.
Делим полученное сообщение на блоки по три цифры

$$292\ 177\ 300\ 177\ 316\ 255\ 020\ 121\ 174\ 304\ 156\ 329,$$

и для раскодирования первой буквы вычисляем, используя секретный ключ $\{69, 391\}$,

$$x \equiv 292^{69} \pmod{391},$$

откуда $x = 209$. Используя таблицу ASCII, числу 209 соответствует буква С. Действуя аналогично, раскодируем фразу обратно.

Отметим несколько отрицательных моментов такого кодирования. Легко видеть, что указанный метод довольно слаб, так как шифрует по буквам, в результате чего одна и та же буква или символ шифруется одним и тем же числом. Таким образом пробелы (если это текст) сразу выдадут свои позиции. Далее можно подобрать коды символов на основе частоты использования букв, например «а» «о», а значит злоумышленник, перехватив зашифрованное сообщение, может расшифровать его и без секретного ключа, и даже не пытаясь его подобрать. Метод можно интуитивно усложнить, если при шифровании каждой буквы на нее будет влиять результат, полученный от предыдущей, например, так:

$$b \equiv (b + a) \pmod{n},$$

где b – текущее значение, а a – предыдущее. Первая буква остается исходной, однако и это легко решается добавлением в начале сообщения произвольной последовательности букв (которые получатель после расшифровки просто проигнорирует). Эти действия заметно усложняют процесс угадывания, и в таком виде алгоритм уже часто применяется в реальной практике.

2.2 Алгоритм шифрования Эль-Гамаля

Алгоритм Эль-Гамаля в чем-то схож с рассмотренным ранее RSA, но, в отличие от последнего, не был запатентован, и потому стал более дешевой альтернативой: не требовалась оплата взносов за лицензию. Алгоритм генерации ключей может быть записан по шагам следующим образом:

1. Выбирается простое число p.

2. Выбирается произвольное целое число q, являющееся так называемым примитивным (чаще – первообразным) корнем по модулю p:

$$q^{\varphi(p)} \equiv 1 \pmod{p},$$

$$q^l \not\equiv 1 \pmod{p} \text{ при } 1 \leq l < \varphi(p).$$

3. Выбирается случайное целое число c такое, что $1 < c < p - 1$.

4. Вычисляется число b из следующего сравнения

$$b \equiv q^c \pmod{p}$$

5. Открытым ключом является тройка $\{p, q, b\}$, закрытым (секретным) ключом — число c.

Нахождение первообразного корня по модулю p сопряжено с некоторыми трудностями, так как проверка условий

$$q^l \not\equiv 1 \pmod{p} \text{ при } 1 \leq l < \varphi(p).$$

требует временных затрат. Для упрощения вычислений часто бывает полезна следующая теорема.

Теорема 2.1 *Пусть $\varphi(p)$ раскладывается на простые множители, как*

$$\varphi(p) = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_n^{k_n},$$

причем НОД$(g, p) = 1$. Тогда g – первообразный корень по модулю p тогда и только тогда, когда сравнения

$$g^{\frac{\varphi(p)}{p_1}} \equiv 1 \pmod{p},\ g^{\frac{\varphi(p)}{p_2}} \equiv 1 \pmod{p},\ ...\ ,\ g^{\frac{\varphi(p)}{p_n}} \equiv 1 \pmod{p}$$

не имеют решений.

Перейдем непосредственно к шифрованию. Предположим, что мы хотим передать сообщение от Боба Алисе. Тогда Боб должен знать открытый ключ Алисы, чтобы зашифровать сообщение, а Алиса должна использовать свой секретный ключ, чтобы его расшифровать.

Пусть Боб хочет послать Алисе сообщение m не превосходящее числа $N - 1$, где $N = p$. Тогда Боб выполняет следующие действия:

1. Выбирает случайное целое число r такое, что $1 < r < p - 1$.

2. Вычисляются два числа

$$e \equiv m \cdot b^r \pmod{p},$$

$$f \equiv q^r \pmod{p}.$$

3. Пара чисел $\{f, e\}$ является шифротекстом.

Зная закрытый ключ c, Алиса может расшифровать исходное сообщение, получив шифротекст $\{f, e\}$, по следующей готовой формуле:

$$m = f \cdot e^{-c} \pmod{p}.$$

2.2.1 Пример шифрования

Рассмотрим простой пример, демонстрирующий все этапы вычислений. Для начала сформируем ключи, для этого:

1. Выбираем число $p = 17$.

2. Вычисляем первообразный корень q по модулю 17. Можно проверить, что любое из чисел $3, 5, 6, 7, 10, 11, 12, 14$ является первообразным корнем по модулю 17. Мы выберем, например, число $q = 11$.

3. Выбираем случайное число $c = 14 < p - 1$.

4. Находим число b из сравнения

$$b \equiv 11^{14} \pmod{17} \Rightarrow b = 9$$

5. Открытым ключом является тройка $\{17, 11, 9\}$, а закрытым ключом число 14.

Пусть Боб хочет передать Алисе сообщение $m = 13$. Тогда он выбирает случайное число $r = 7 < p - 1$ и вычисляет числа:

$$e \equiv 13 \cdot 9^7 \pmod{17} \Rightarrow e = 9,$$

$$f \equiv 11^7 \pmod{17} \Rightarrow f = 3.$$

Полученный шифротекст $\{3, 9\}$ передается Алисе, которая использует ключ $c = 14$ и дешифрует полученное сообщение.

$$m = 9 \cdot 3^{-14} \pmod{17} \Rightarrow p = 13$$

Тем самым, Алиса получает зашифрованное Бобом сообщение 13.

3 Электронные подписи

3.1 Электронная подпись RSA

Рассмотрим применение алгоритма шифрования RSA для электронной подписи документов. Цифровая подпись необходима в тех ситуациях, когда важно установить изменение данных и подлинность подписавшей стороны. Получатель подписанного документа может использовать цифровую подпись для доказательства третьей стороне того, что подпись действительно сделана отправляющей стороной, а в документ не было внесено изменений.

В ходе подписания документа подсчитывается хеш-функция, которая сократит любой его объем до определенного количества байтов. Хеш-функции бывают различных типов и также влияют на уровень надежности электронной подписи. Таблица ASCII символов в определенном смысле также является хэшем, но на практике текст сначала кодируется, а потом хешируется.

Электронная подпись, в отличие от ассиметричного шифрования, основана на закрытом ключе. Проверить же подпись может любой желающий, используя открытый ключ. Генерация ключей происходит точно так же, как и для шифрования.

Алгоритм подписи может быть записан по шагам следующим образом:

1. Генерация ключей $\{c, N\}$ и $\{d, N\}$ происходит так же, как и в алгоритме RSA, только теперь $\{c, N\}$ – секретный ключ, а $\{d, N\}$ – открытый ключ.

2. Вычисляется хеш-значение h документа или сообщения m.

3. Вычисляется подпись s сообщения m из сравнения

$$s \equiv h^c \pmod{N}.$$

4. Пара $\{m, s\}$ из сообщения и подписи передается адресату.

Принимающая сторона должна иметь возможность проверить, получила ли она истинный документ без изменений, или его подделку. Алгоритм проверки электронной подписи может быть представлен следующими шагами:

1. Проверяющая сторона получает пару из сообщения и подписи $\{m, s\}$.

2. Вычисляется хеш-значение h сообщения m.

3. Вычисляется значение h', используя открытый ключ $\{d, N\}$, из следующего сравнения

$$h' \equiv s^d \pmod{N}$$

4. Если равенство $h = h'$ выполняется, значит подпись верна.

3.1.1 Пример получения электронной подписи

Рассмотрим простой пример, демонстрирующий все этапы вычисления электронной подписи и ее проверки.

Для начала, сформируем открытый и секретный ключи, для этого обратимся к примеру шифрования алгоритмом RSA и возьмем ранее найденные значения. Для $p = 3$, $q = 7$ были найдены: $\{5, 21\}$ – открытый ключ и $\{17, 21\}$ – закрытый. В алгоритме электронной подписи все наоборот: $\{5, 21\}$ – секретный ключ, а $\{17, 21\}$ – открытый.

Пусть Боб хочет передать Алисе сообщение $m = 19$, подписанное секретным ключом $\{5, 21\}$. Тогда он хеширует свое сообщение неким алгоритмом и получает, например, значение $h = 19$, а затем по ключу вычисляет подпись s из сравнения

$$s \equiv 19^5 \pmod{21}.$$

Таким образом $s = 10$.

Алиса получает сообщение m, подпись s, и использует открытый ключ для проверки электронной подписи. Она хеширует полученное сообщение таким же алгоритмом и получает $h = 19$ и вычисляет h' из сравнения

$$h' \equiv 10^{17} \pmod{21}.$$

Таким образом $h' = 19$ и совпадает с исходным хешем h. Это означает что сообщению стоит доверять, и оно действительно отправлено Бобом, а Алиса получила его без каких-либо повреждений, или оно не было подменено во время передачи.

3.2 Электронная подпись Эль-Гамаля

Алгоритм подписи Эль-Гамаля может быть записан по шагам следующим образом:

1. Генерируются открытый ключ $\{p, q, b\}$ и секретный ключ c, согласно алгоритму генерации ключей Эль-Гамаля.

2. Вычисляется хеш-значение h документа или сообщения m.

3. Выбирается случайное целое число r такое, что $1 < r < p - 1$.

4. Вычисляется значение $f = q^r \pmod{p}$.

5. Вычисляется подпись s из сравнения

$$h \equiv f \cdot c + r \cdot s \pmod{p - 1},$$

или

$$s \equiv (h - f \cdot c)r^{-1} \pmod{p - 1}$$

6. Пара $\{s, f\}$ является подписью сообщения или документа.

Зная открытый ключ $\{p, q, b\}$, подпись $\{s, f\}$ сообщения m проверяется следующим образом:

1. Проверяются условия $0 < s < p$ и $0 < f < p - 1$.

2. Вычисляется хеш-значение h сообщения m.

3. Подпись считается верной, если выполняется следующее сравнение:

$$b^f \cdot f^s \equiv q^h \pmod{p}$$

3.2.1 Пример получения электронной подписи

Рассмотрим пример. Возьмем уже найденный открытый ключ $\{17, 9, 4\}$ и закрытый ключ 14 из примера на шифрование.

Пусть Боб хочет передать Алисе сообщение $m = 19$, тогда он хеширует свое сообщение неким алгоритмом и получает, например, значение $h = 19$. Далее Боб выбирает случайное число $r = 7 < p - 1$ и вычисляет $f = 9^7 \pmod{17} = 2$. Тогда подпись вычисляется из сравнения

$$s \equiv (19 - 2 \cdot 14) \cdot 7^{-1} \pmod{16} \Rightarrow s = 1.$$

Алиса, получает сообщение m, подпись $\{s, f\}$, и открытый ключ $\{p, q, b\}$, а затем выполняет проверку электронной подписи. Она хеширует полученное сообщение таким же алгоритмом и получает $h = 19$, а затем проверяет сравнение

$$4^2 \cdot 2^1 \equiv 9^{19} \pmod{17} \Rightarrow 32 \equiv 9^{19} \pmod{17},$$

которое оказывается верным, а значит сообщению стоит доверять.