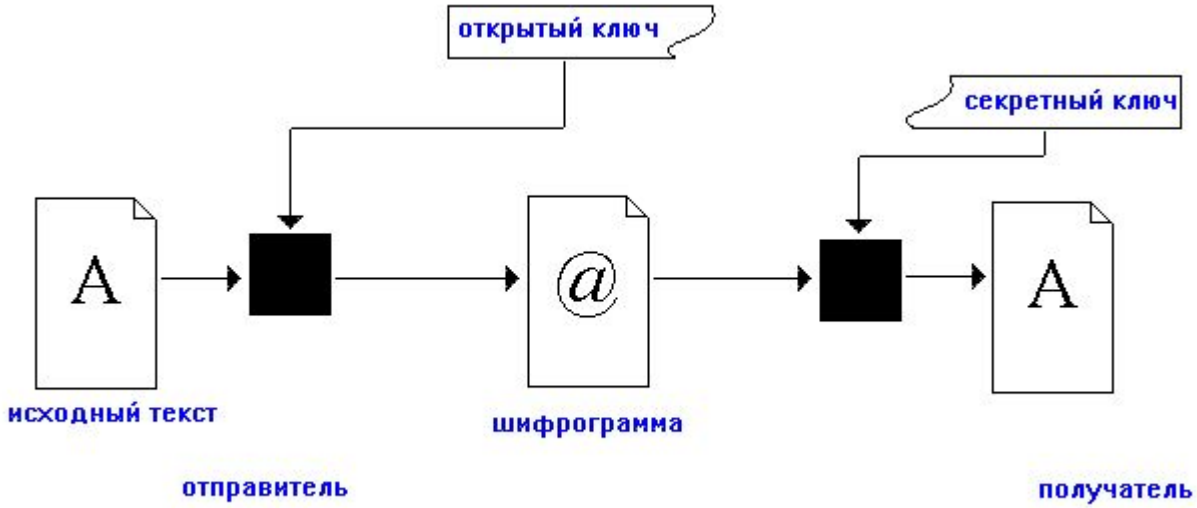
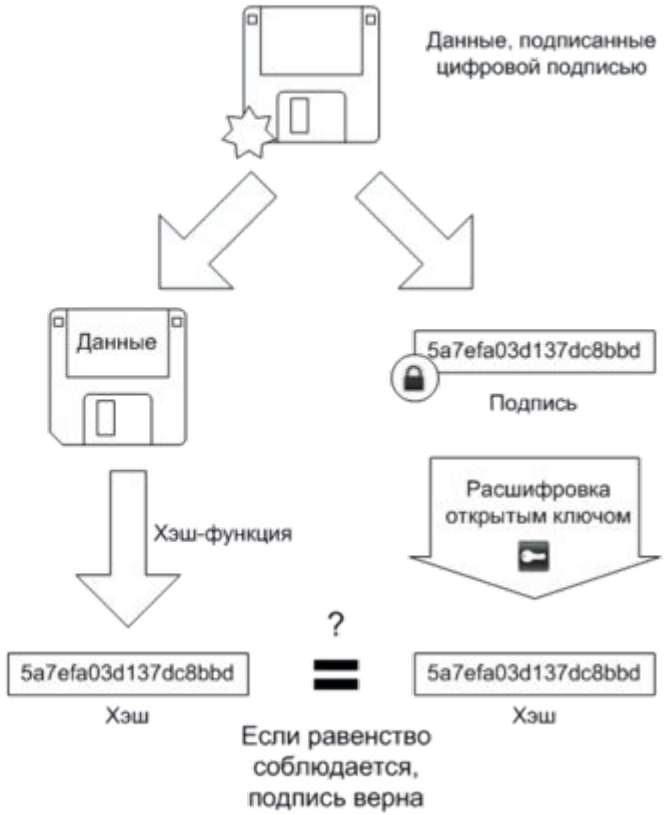
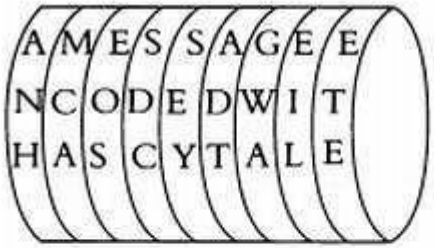

открытый ключ
секретный ключ
A
@
A
исходный текст
шифрограмма
отправитель
получатель

Подписывание

Проверка

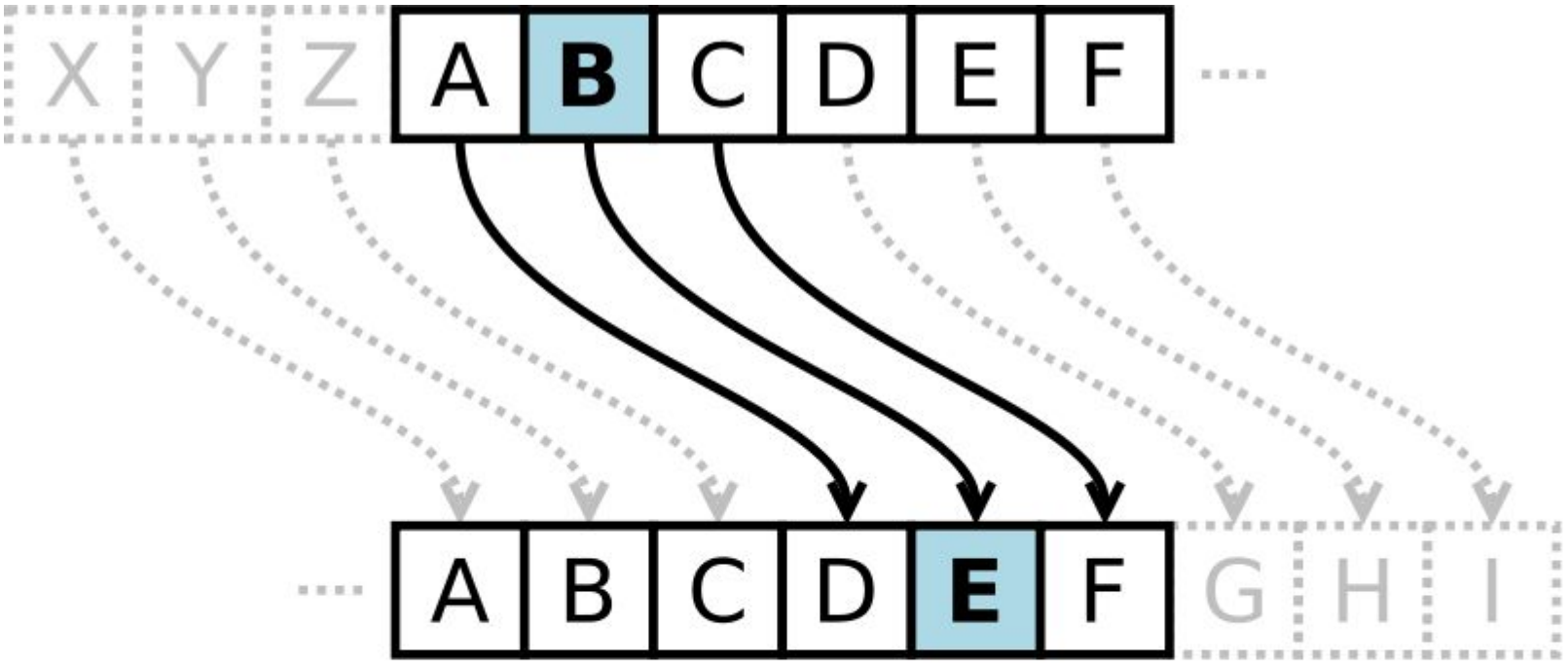


Асимметричное шифрование



M = A MESSAGE ENCODED WITH A SCYTALE

C = ANH MCA EOS SDC SEY ADT GWA EIL ETE



Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется буквой находящейся на некоторое постоянное число позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3 A была бы заменена на D, B станет E, и так далее.

Модульная арифметика

Символически сравнимость записывается в виде формулы (**сравнения**):

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

Число *n* называется **модулем** сравнения.
Например, 32 и −10 сравнимы по модулю 7, так как оба числа при делении на 7 дают остаток 4:

$$32 = 7 \cdot 4 + 4, \quad -10 = 7 \cdot (-2) + 4$$

Эквивалентные формулировки: числа *a*, *b* **сравнимы по модулю** *n*, если:

1. их разность $a - b$ делится на *n* без остатка;
2. *a* может быть представлено в виде $a = b + kn$, где *k* — некоторое целое число.

Для вышеприведенного примера: 32 и −10 сравнимы по модулю 7, так как их разность 42 делится на 7, и к тому же имеет место представление:

$$32 = -10 + 6 \cdot 7$$

Для фиксированного натурального числа n отношение сравнимости по модулю n обладает следующими свойствами:

- рефлексивности: для любого целого a справедливо $a \equiv a \pmod{n}$.
- симметричности: если $a \equiv b \pmod{n}$, то $b \equiv a \pmod{n}$.
- транзитивности: если $a \equiv b \pmod{n}$ и $b \equiv c \pmod{n}$, то $a \equiv c \pmod{n}$.

Таким образом, отношение сравнимости по модулю n является отношением эквивалентности на множестве целых чисел.

Любые два целых числа сравнимы по модулю 1.

Если числа a и b сравнимы по модулю n, и n делится на m, то a и b сравнимы по модулю m.

Для того, чтобы числа a и b были сравнимы по модулю n, каноническое разложение на простые сомножители которого имеет вид

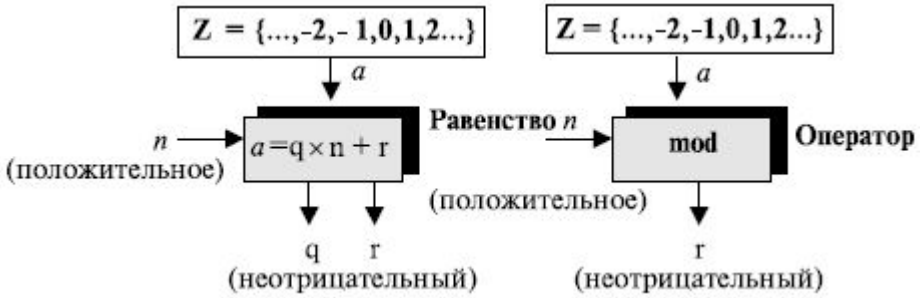
$$n = \prod_{i=1}^{d} p_i^{\alpha_i},$$

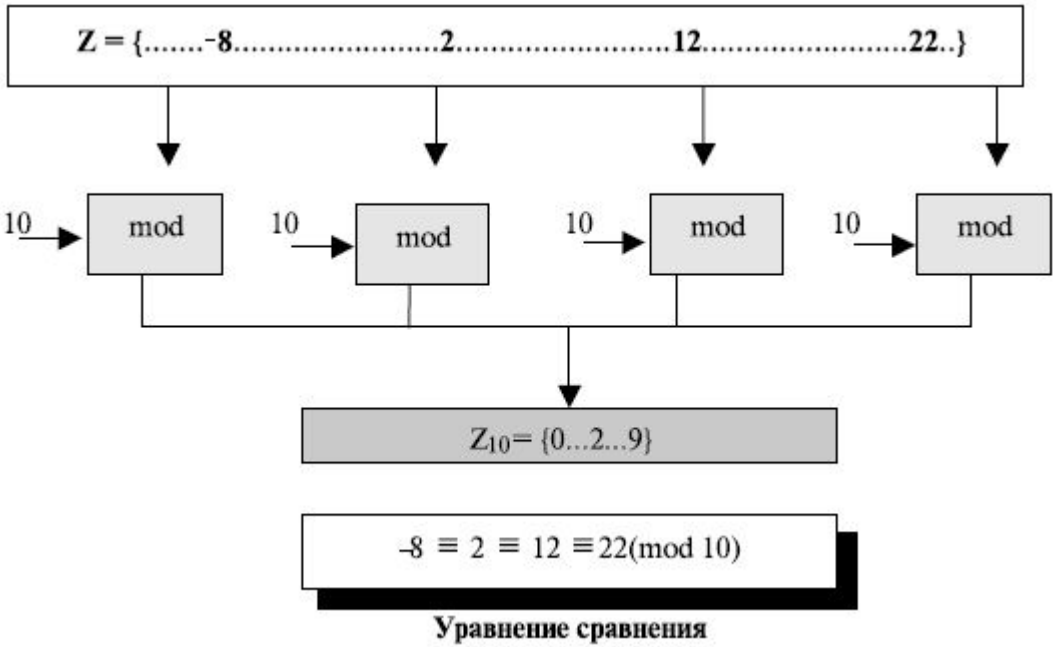
необходимо и достаточно, чтобы

$$a \equiv b \pmod{p_i^{\alpha_i}}, \quad i = 1, 2, \ldots, d.$$

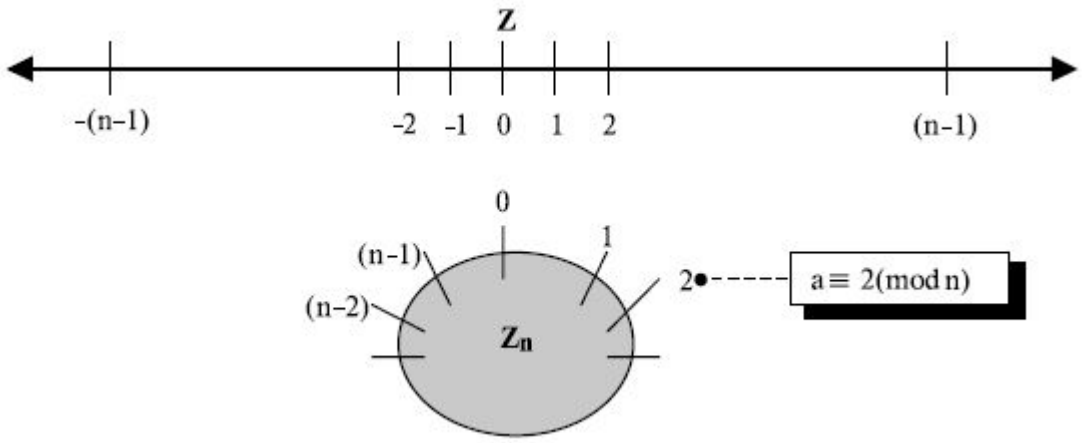
Если $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod{m}$, где $m = [m_1, m_2]$.

Уравнение деления (a=q*x+r), рассмотренное в предыдущей секции, имеет два входа (a и n) и два выхода (q и r). В модульной арифметике мы интересуемся только одним из выходов — остатком r. Мы не заботимся о частном q. Другими словами, когда мы делим a на n, мы интересуемся только тем, что *значение остатка равно* r. Это подразумевает, что мы можем представить изображение вышеупомянутого уравнения как *бинарный оператор* с двумя входами a и n и одним выходом r.



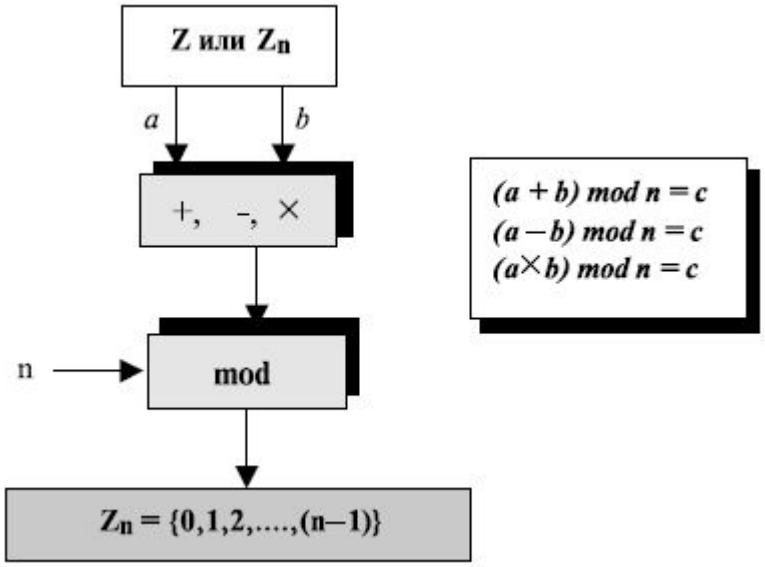


Уравнение сравнения



Круговая система обозначений

Понятие "сравнение" может быть лучше раскрыто при использовании круга в качестве модели. Так же, как мы применяем линию, чтобы показать распределение целых чисел в Z, мы можем использовать круг, чтобы показать распределение целых чисел в Z_n.



Три *бинарных операции* (*сложение, вычитание* и *умножение*), которые мы обсуждали для Z, могут также быть определены для набора Z_n. Результат, возможно, должен быть отображен в Z_n с использованием операции по модулю.

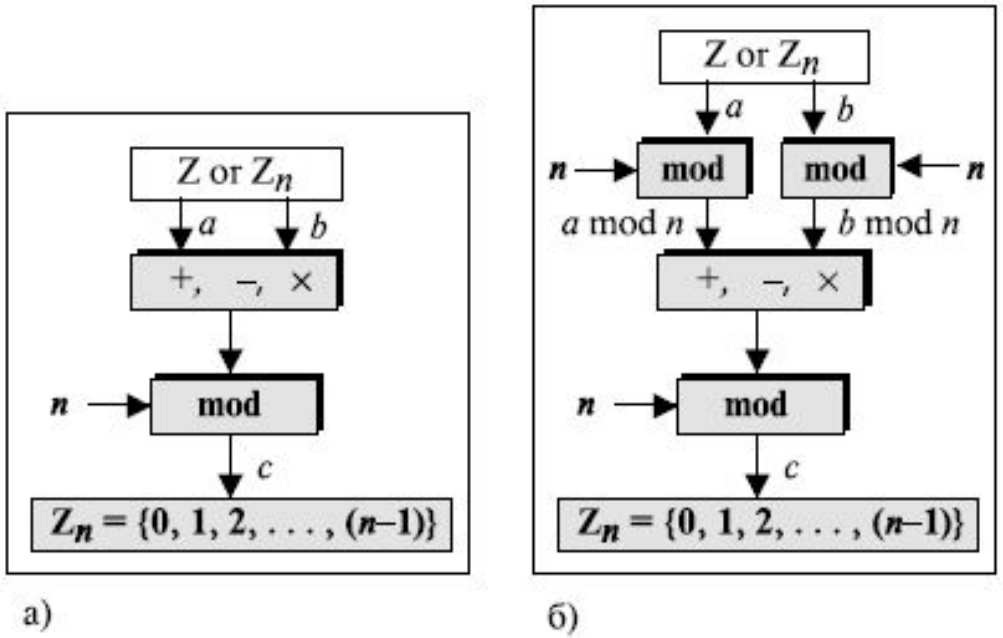
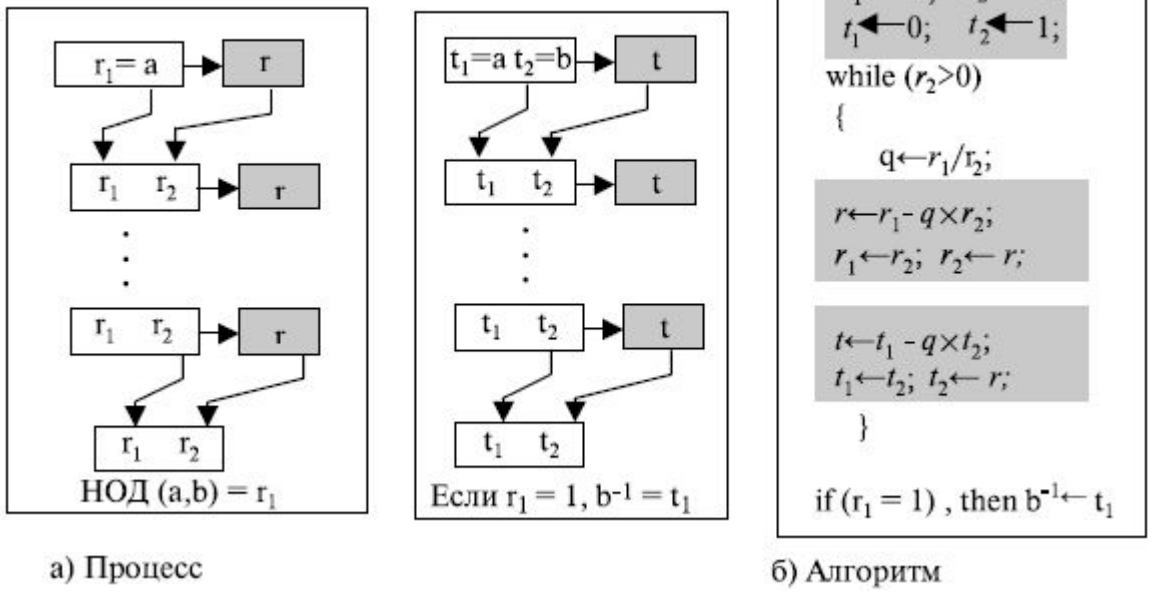


Рисунок показывает процесс до и после применения указанных выше свойств. Хотя по рисунку видно, что процесс с применением этих свойств более длинен, мы должны помнить, что в криптографии мы имеем дело с очень большими целыми числами. Например, если мы умножаем очень большое целое число на другое очень большое целое число, которое настолько большое, что не может быть записано в компьютере, то применение вышеупомянутых свойств позволяет уменьшить первые два операнда прежде, чем начать умножение. Другими словами, перечисленные свойства позволяют нам работать с меньшими числами. Этот факт станет понятнее при обсуждении экспоненциальных операций в последующих лекциях.

Когда мы работаем в модульной арифметике, нам часто нужно найти операцию, которая позволяет вычислить величину, обратную заданному числу. Мы обычно ищем **аддитивную инверсию** (оператор, обратный сложению) или **мультипликативную инверсию** (оператор, обратный умножению).



а) Процесс

б) Алгоритм

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

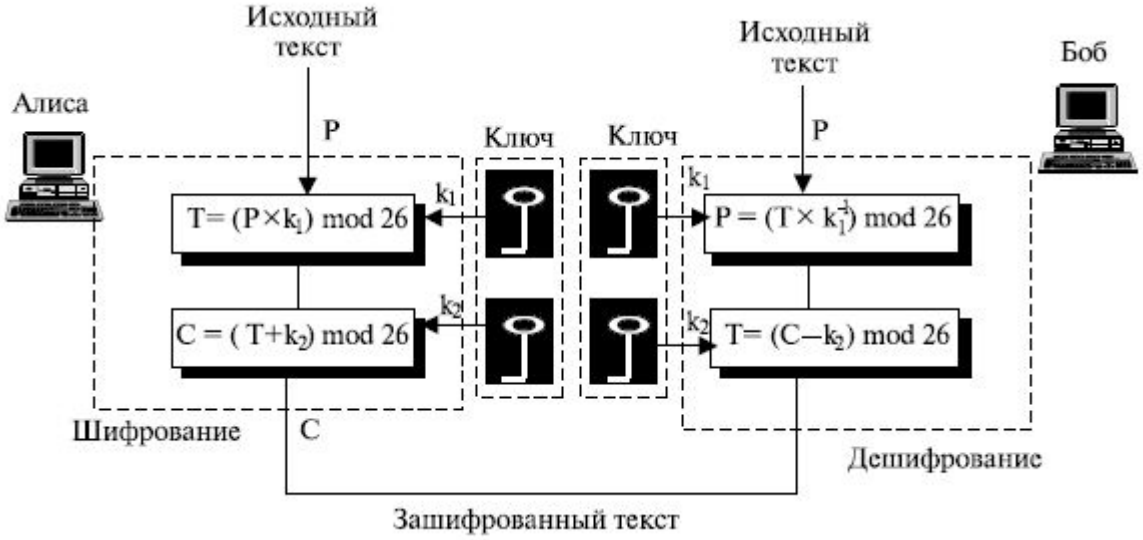
Таблица сложения в Z_{10}

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Таблица умножения в Z_{10}

Рисунок показывает две таблицы для сложения и умножения. При сложении таблиц каждое целое число имеет аддитивную инверсию. Обратные пары могут быть найдены, если результат их сложения — ноль. Мы имеем (0, 0), (1, 9), (2, 8), (3, 7), (4, 6) и (5, 5). При умножении таблиц мы получаем только три мультипликативных пары (1, 1), (3, 7) и (9, 9). Пары могут быть найдены, когда результат умножения равен 1. Обе таблицы симметричны по диагонали, от левой вершины к нижней вершине справа. При этом можно обнаружить свойства коммутативности для сложения и умножения (a+b = b+a). Таблица сложения также показывает, что каждый ряд или колонка может поменяться с другим рядом или колонкой. Для таблицы умножения это неверно.

N - число символов в алфавите



Аффинный шифр - тип моноалфавитного шифра замены, в чем каждое письмо в алфавите нанесено на карту к его числовому эквиваленту, зашифровало использование простой математической функции и преобразовало назад в письмо. Формула использовала средства, которые каждое письмо шифрует к одному другому письму, и назад снова, означая, что шифр - по существу стандартный шифр замены с управлением правила, какое письмо идет в который. Также, у этого есть слабые места всех шифров замены. Каждое письмо зашифровано с функцией, где величина изменения.

В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря.

Аналитическая машина Бэббиджа