**Симметричное** — для шифрования и расшифровки информации применяется один и тот же криптографический ключ.

**Асимметричное** — для кодирования и расшифровки используется два ключа. Открытый известен всем пользователям системы, а закрытый доступен только владельцу. Информация шифруется открытым ключом, расшифровать ее может только владелец закрытого.

Сущность **подстановочного** **шифрования** состоит в том, что исходный текст (из множества М) и зашифрованный текст (из множества С) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки.   
**Типы** подстановочных шифров:

• моноалфавитных (шифры однозначной замены или простые подстановочные); Максимальное количество ключей для любого шифра этого вида не превышает N! **Шифр Цезаря, Атбаш** (1 на последний, 2 на предпоследний и тд). Одним из существенных недостатков моноалфавитных шифров является их низкая криптостойкость. Зачастую метод криптоанализа базируется на частоте встречаемости букв исходного текста

• полиграммных; **шифр Порты, шифр Плейфера и шифр Хилла**

• омофонических (однозвучные шифры или шифры многозначной замены);

• полиалфавитных. **Диск** **Альберти, Таблица Трисемуса, Шифр Виженера**

Сущность **перестановочного шифрования** состоит в том, что исходный текст (М) и зашифрованный текст (С) основаны на использовании одного и того же алфавита, а тайной или ключевой информацией является алгоритм перестановки. Относятся к классу симметричных. Классическими примерами перестановочных шифров являются анаграммы. Делятся на два подкласса:

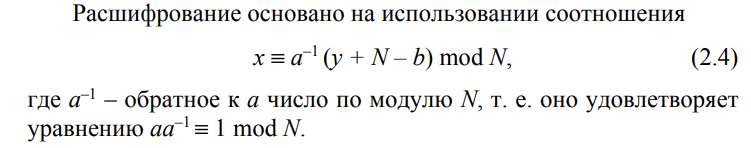
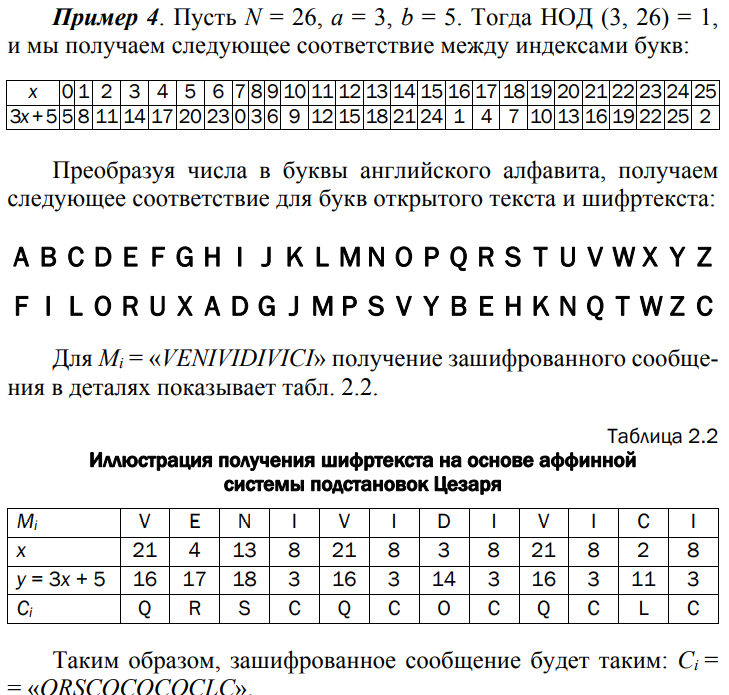
• шифры простой, или одинарной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) один раз;

• шифры сложной, или множественной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) несколько раз.

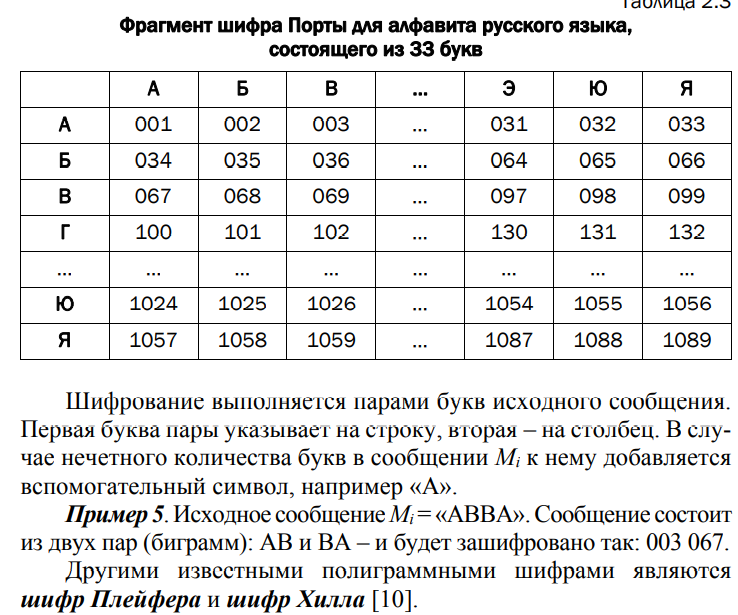
**Потоковый шифр** (иногда говорят «поточный») – симметричный шифр, преобразующий каждый символ mi открытого текста в символ шифрованного ci, зависящий от ключа и расположения символа в тексте. Делятся на 2 класса: синхронные и асинхронные. Основной задачей потоковых шифров является выработка некоторой последовательности (гаммы) для зашифрования, т. е. выходная гамма является ключевым потоком (ключом) для сообщения. Синхронные потоковые шифры (СПШ) характеризуются тем, что поток ключей генерируется независимо от открытого текста и шифртекста.

**Блочный шифр.** Все перечисленные стандарты и алгоритмы блочных шифров (БШ) строятся на основе подстановочных и перестановочных шифров, т. е. являются комбинационными. БШ относятся также к классу симметричных.

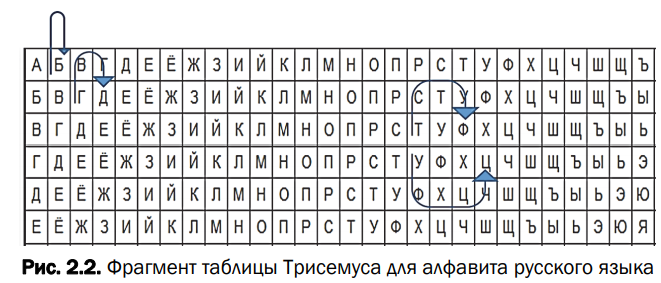
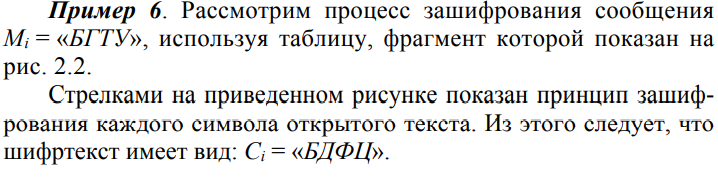
**Аффинная система подстановок Цезаря**

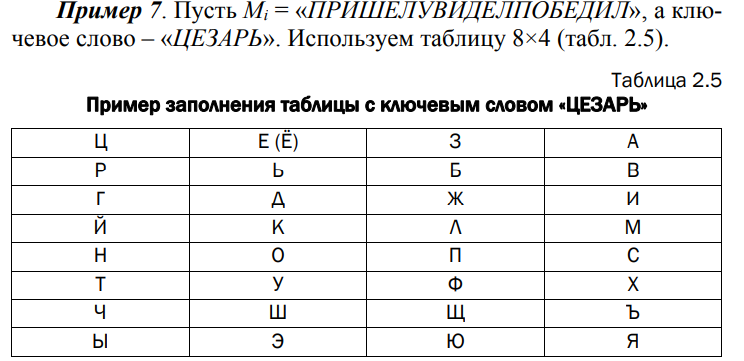


**ШИФР ПОРТЫ**

****

**Таблица Трисемуса**

****

****

Следуя вышеуказанного принципу подстановки, получим Сi = = «ФГМЭЬПШИМКЬПФУЖЬКМП»

**Шифр Виженера**

**Берем алфавит, Строка = ключ, столбец = слово. Пересечение = зашифрованное слово**

**Лабораторная 1**

**Высшая** **арифметика**, – раздел математики, изучающий натуральные числа и иные похожие величины.

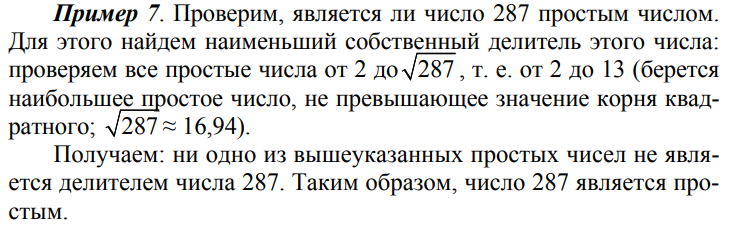
Множество всех **целых** **чисел** (обозначим буквой Z) есть набор всех действительных чисел без дробной части: {..., –3, –2, –1, 0, 1, 2, 3, ...}.

**Натуральные** **числа** являются подмножеством целых чисел и образуют множество N: {1, 2, 3, ...}.

**Делимость** – одно из основных понятий теории чисел. Если для некоторого целого числа a и натурального числа b существует целое число q, при котором bq = a, то говорят, что число a делится на b. В этом случае b называется **делителем** числа a, а a называется **кратным** числу b. При этом используются следующие обозначения: a ⋮ b – a делится на b, или b | a – b делит a.

Делитель a называется **собственным** **делителем** числа b, если 1 < |a| < |b|, и **несобственным** – в противном случае.

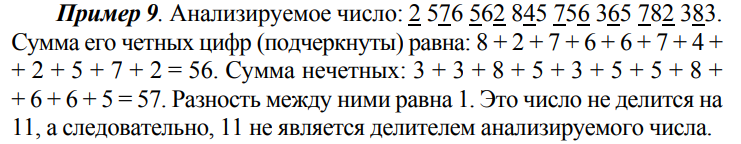
**Наименьший** **простой** **делитель** составного числа n не превышает **√n**, поэтому для проверки простоты числа доста точно проверить его делимость на 2 и на все нечетные (а еще лучше простые) числа, не превосходящие **√n**;



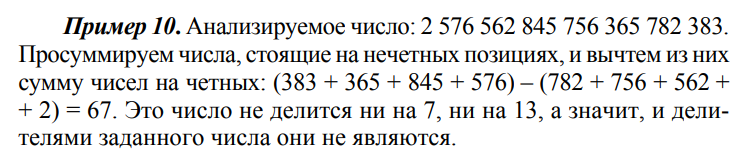
Если число не имеет делителей, кроме самого себя и единицы, то оно называется **простым**, а если у числа есть еще делители, то **составным**.

Простых чисел бесконечно много, причем существует примерно n / ln(n) простых чисел, меньших числа n.

Сложность решения задачи разложения больших чисел на простые сомножители, известной как «**проблема факторизации**», определяет криптостойкость некоторых алгоритмов асимметричной криптографии, в частности алгоритма RSA

Основано на свойство делимости на 11. Нужно из суммы всех нечетных цифр числа вычесть сумму всех четных его цифр. Четность и нечетность определяется счетом от младшего разряда. Если получившаяся разность делится на 11, то и анализируемое число тоже на него делится. 

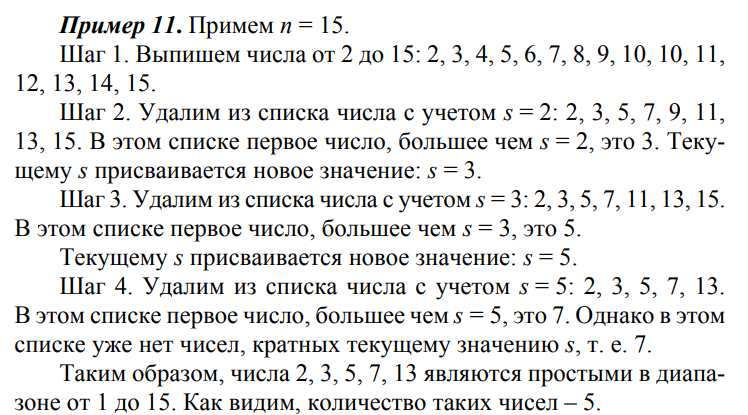
Основано на свойстве делимости на 7 и 13. Нужно разбить анализируемое число на тройки цифр, начиная с младших разрядов. Просуммировать числа, стоящие на нечетных позициях, и вычесть из них сумму чисел на четных. Проверить делимость результата на числа 7 и 13.

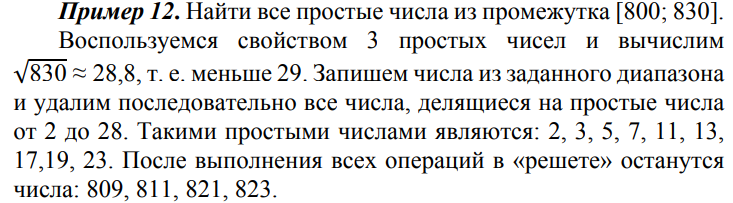


Если два простых числа отличаются на 2, то их называют **числа-близнецы**.

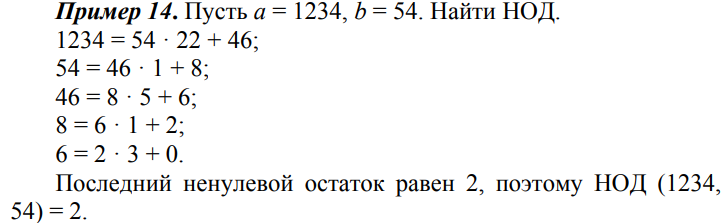
**РЕШЕТО ЭРАСТОФЕНА**

1) выписать подряд все целые числа от двух (либо от m) до n (2, 3, 4, …, n). Пусть некоторая переменная (напрмер, s) изначально равна 2 – первому простому числу;   
2) удалить из списка числа от 2s до n, считая шагами по s (это будут числа, кратные s: 2s, 3s, 4s, …);   
3) найти первое из оставшихся чисел в списке, большее чем s, и присвоить значению переменной s это число;   
4) повторять шаги 2 и 3, пока возможно.





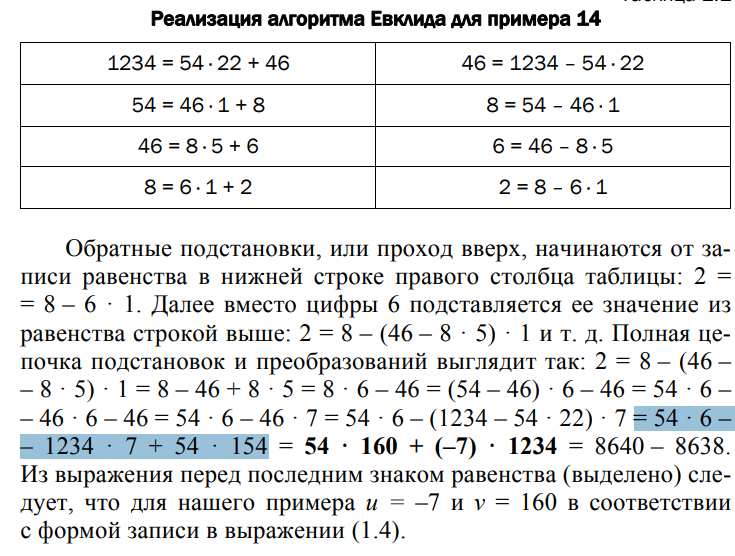
НОД Алгоритм Евклида



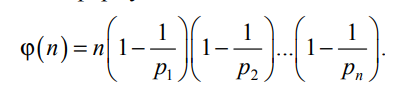
**Взаимно** **простыми** являются целые числа, наибольший общий делитель которых равен 1.

**Соотношение Безу. Расширенный алгоритм Евклида.**

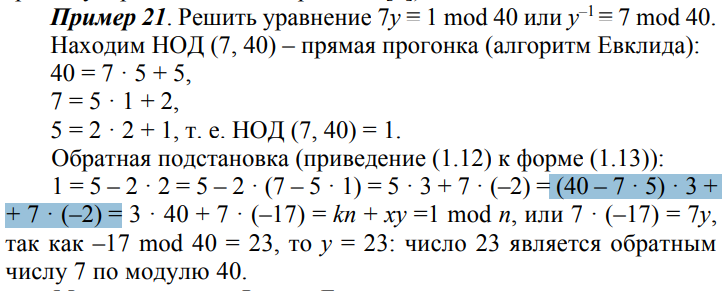
аu + bv = d



Количество натуральных чисел, непревосходящих nивзаимно простых с n, называется **функция Эйлера** и обозначается φ(n).



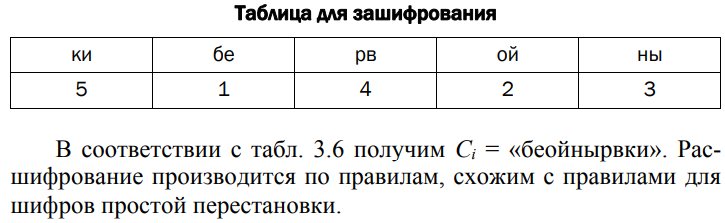
Обратное по модулю число



**ЛАБОРАТОРНАЯ РАБОТА 3**

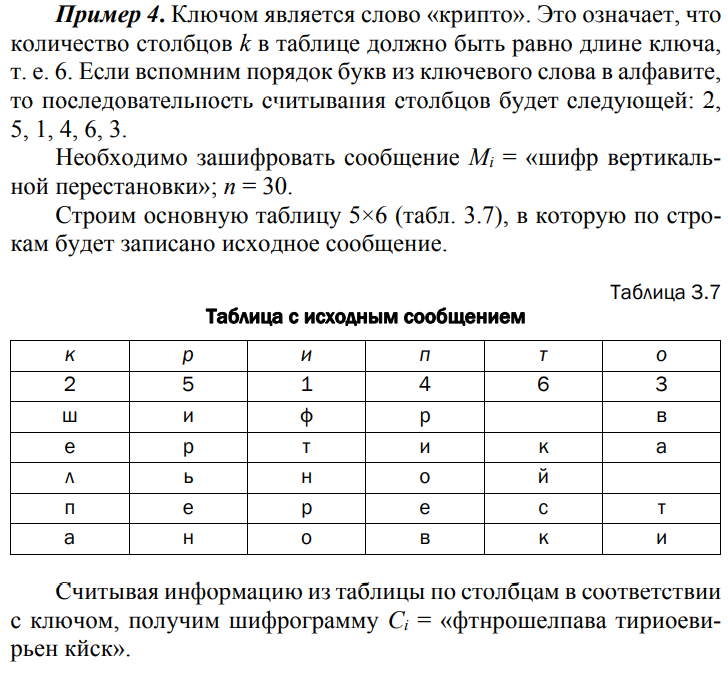
Шифры простой перестановки: если Мi = «шифр перестановки», то Сi = «иквонатсереп рфиш»

Шифры простой блочной перестановки:



Шифры маршрутной перестановки: Шифр Скитала , змейкой, спиралью

Шифр вертикальной перестановки



Шифры множественной перестановки

**ЛАБОРАТОРНАЯ РАБОТА 4 ЭНИГМА**

«Энигма» строится на основе подстановочных шифров, подобных шифру Цезаря, в котором ключ сообщения, который должен знать получатель, – это просто смещение между двумя алфавитами. Принято считать, что в основе шифра «Энигмы» лежит динамический шифр Цезаря.

Букву не может зашифровать саму в себя.

Содержит из клавиатуру, роторы, рефлектор, коммутационную и индикационную модель.

Конкретный механизм мог быть разным, но общий принцип был таков: при каждом нажатии на клавишу самый правый ротор сдвигался на одну позицию, а при определенных условиях сдвигались и другие роторы.

1. Установить начальную стартовую позицию роторов (предположим, их 3) согласно текущей кодовой таблице (коду дня), например WZA.

2. Выбрать случайный ключ сообщения, например SXT. Затем оператор устанавливал роторы в стартовую позицию WZA.

3. Зашифровать ключ сообщения SXT. Предположим, что в результате зашифрования ключа получится UHL.

4. Далее оператор ставил ключ сообщения (SXT) как начальную позицию роторов и зашифровывал собственно сообщение. После этого он отправлял стартовую позицию (WZA) и зашифрованный ключ (UHL) вместе с сообщением.

Расшифрование сообщения.

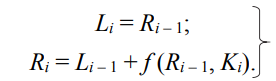
1. Установить стартовые позиции роторов в соответствии с первой трехграммой (WZA).

2. Расшифровать вторую треграмму (UHL) и извлечь исходный ключ (SXT).

3. Далее получатель использовал этот ключ как стартовую позицию для расшифрования шифртекста. Обычно срок действия ключей составлял одни сутки.

**ЛАБОРАТОРНАЯ 5 БЛОЧНЫЕ DES, ГОСТ, Blowfish, AES, ГОСТ 28147–89**

Все перечисленные стандарты и алгоритмы блочных шифров (БШ) строятся на основе подстановочных и перестановочных шифров, т. е. являются комбинационными. БШ относятся также к классу симметричных.

****

****

**AES** (Advanced Encryption Standard) – алгоритм шифрования, действующий в качестве государственного стандарта в США с 2001 г. В основу стандарта положен шифр Rijndael. Шифр Rijndael/AES (т. е. рекомендуемый стандартом) характеризуется размером блока 128 битов, длиной ключа 128, 192 или 256 битов и количеством раундов 10, 12 или 14 в зависимости от длины ключа.

**ГОСТ 28147–89**. ГОСТ предусматривает три режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки. Первый из режимов шифрования предназначен для шифрования ключевой информации и не может использоваться для шифрования других данных, для этого предусмотрены два других режима. По сравнению с DES первый более удобен для программной реализации. В ГОСТ 28147–89 применяется более длинный ключ – 256 битов, здесь используются 32 раунда шифрования.

**Blowfish.** Основой алгоритма является сеть Фейстеля с 16 раундами. Длина блока равна 64 битам, ключ может иметь любую длину в пределах 448 битов. Blowfish использует большое количество подключей. Эти ключи должны быть вычислены заранее, до начала любого зашифрования/расшифрования данных.

**Лавинный эффект** -  означает, что изменение значения малого количества битов во входном тексте или в ключе ведет к «лавинному» изменению значений выходных битов шифротекста. Другими словами, это зависимость всех выходных битов от каждого входного бита. Если криптографический алгоритм не обладает лавинным эффектом в достаточной степени, [криптоаналитик](http://cryptowiki.net/index.php?title=%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7" \o "Криптоанализ) может сделать предположение о входной информации, основываясь на выходной информации.

**ЛАБОРАТОРНАЯ РАБОТА 7**

**Односторонняя функция** (one-way function) называется математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, т. е. зная х, легко вычислить f(x), но по известному f(x) трудно найти подходящее значение x.

**Сверхвозрастающей** называется **последовательность**, в которой каждый последующий член больше суммы всех предыдущих.

**ЛАБОРАТОРНАЯ РАБОТА 8**

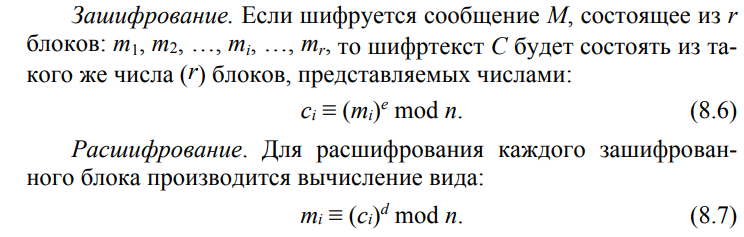
Практически все системы асимметричного зашифрования/расшифрования основаны либо на проблеме факторизации (среди них – RSA), либо на проблеме дискретного логарифмирования (среди них – Эль-Гамаля).

**RSA.** Стал первым полноценный алгоритмом с открытым ключом, который впоследствии стал одним из основных для шифрования и для электронных цифровых подписей.

Для генерации двух ключей: тайного и открытого используются два больших случайных простых числа p и q равной длины. n = pq. Это есть один из трех компонент ключа, состоящего из чисел n, e, d.

Затем случайным образом выбирается второй компонент ключа (открытый ключ или ключ зашифрования, e, такой что e и (p – 1)(q – 1) являются взаимно простыми числами; вспомним, что (p – 1)(q – 1) = φ(n) – функция Эйлера). Б. Шнайер [5] рекомендует число е выбирать из ряда: 3, 17, 216 + 1.

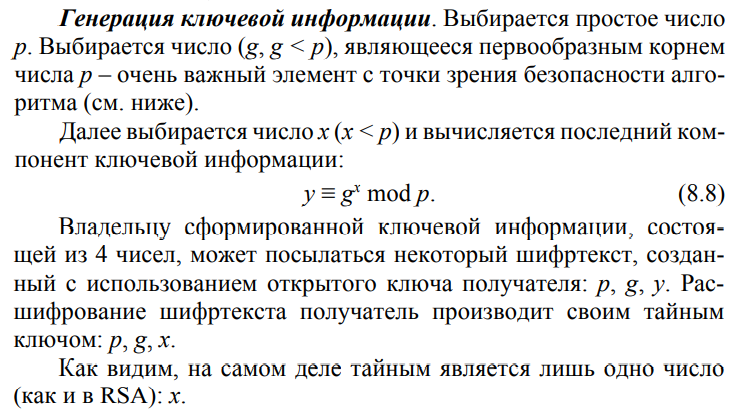
Расширенный алгоритм Евклида используется для вычисления третьего компонента ключа: ключа расшифрования d такого, что выполняется условие

. 

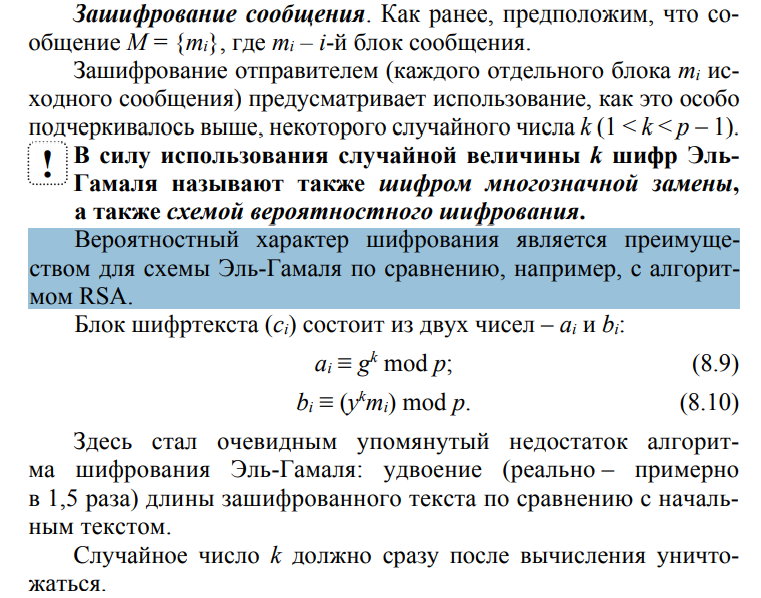
**Алгоритм Эль-Гамаля**

Он может быть использован для решения трех основных криптографических задач: для зашифрования/расшифрования данных, для формирования цифровой подписи и для согласования общего ключа. Как подчеркивалось выше, безопасность алгоритма Эль-Гамаля, как и безопасность алгоритма Диффи – Хеллмана, основана на трудности вычисления дискретных логарифмов.

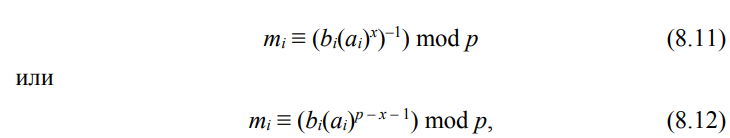
И в случае шифрования, и в случае формирования цифровой подписи каждому пользователю необходимо сгенерировать пару ключей. Рассматриваемый алгоритм отличается от алгоритма RSA несколькими параметрами и особенностями: 1) генерацией ключевой информации и числом компонент, составляющих ключ; 2) каждому блоку (символу) открытого сообщения в шифртексте на основе алгоритма Эль-Гамаля соответствуют 2 блока (в RSA – один-один); 3) в алгоритме Эль-Гамаля при зашифровании используется число (обозначим его k), которое практически никак не связано с ключевой информацией получателя и которое принимает (по определению) различные значения при зашифровании различных блоков сообщения.



**Вероятностный характер шифрования является преимуществом для схемы Эль-Гамаля по сравнению, например, с алгоритмом RSA.**



Расшифрование.



**При примерно одинаковой размерности ключей рассмотренные алгоритмы обеспечивают примерно одинаковый уровень криптостойкости.**