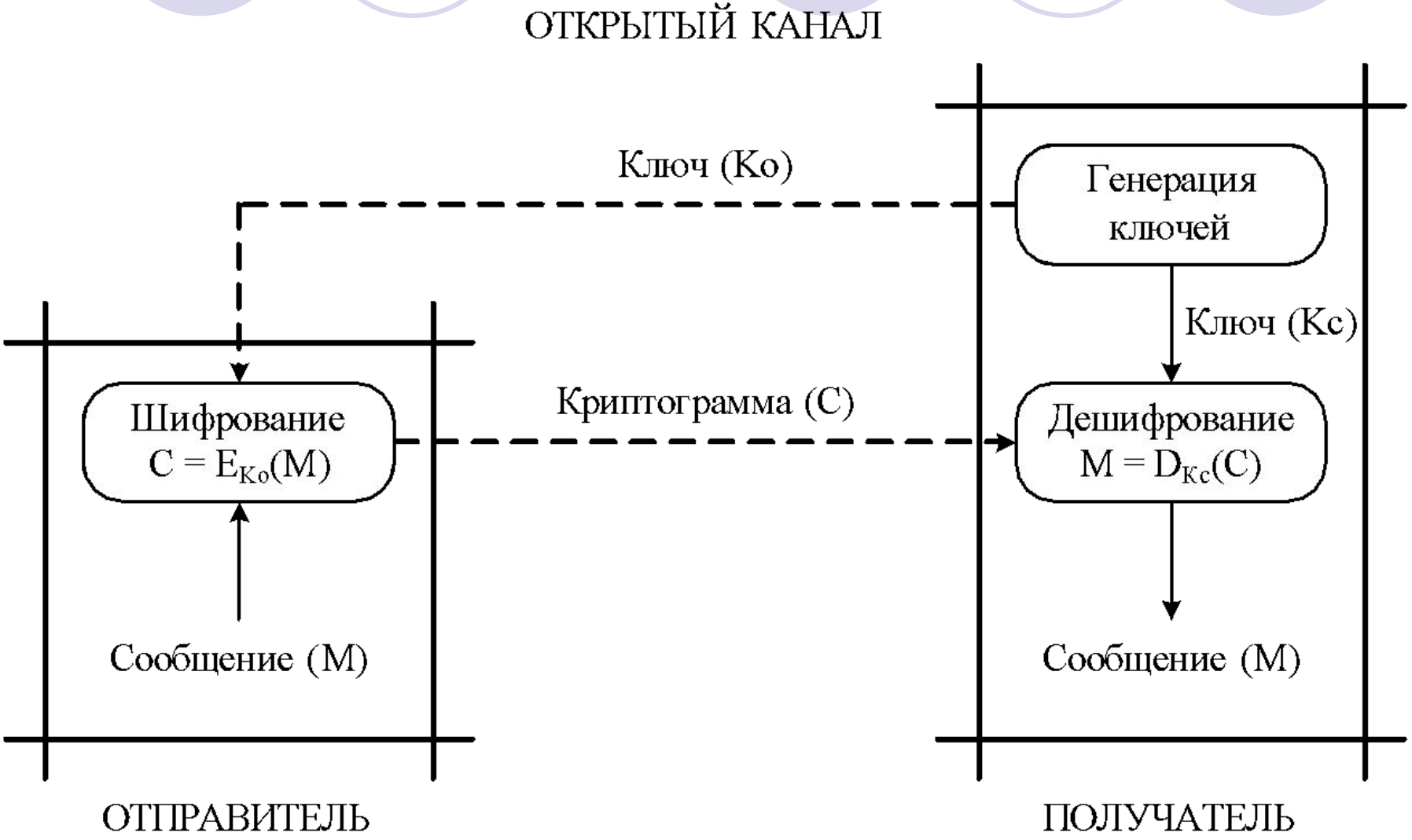
Лекция 5.
Системы с открытым ключом

1. Асимметричные алгоритмы шифрования
2. Односторонние функции
3. Примеры криптосистем

Асимметричные алгоритмы шифрования

- В асимметричных системах для шифрования данных используется один ключ, а для дешифрования – другой (поэтому их и называют асимметричными). Ключ, используемый для шифрования, является открытым, поэтому может быть опубликован для использования всеми пользователями системы, которые шифруют данные. Для дешифрования данных получатель пользуется вторым ключом, являющимся секретным, и он не может быть определен из ключа шифрования.

Схема асимметричной криптосистемы



Особенности асимметричных криптосистем

- открытый ключ Ko и криптограмма C могут быть отправлены по незащищенным каналам, т.е. противнику известны открытый ключ и криптограмма;
- открытыми являются алгоритмы шифрования (E: M → C) и дешифрования (D: C → M).
- Защита информации в асимметричной криптосистеме основана на секретности ключа Kc.

Требования к асимметричным криптосистемам

- вычисление пары ключей (Ko, Kc) должно быть простым;
- отправитель может легко вычислить криптограмму, зная открытый ключ Ko и сообщение M:C = EKo(M);
- получатель может легко восстановить исходное сообщение, используя секретный ключ Kc и криптограмму C: M = DKc(C);
- при попытке вычислить секретный ключ Kc противник наталкивается на непреодолимую вычислительную проблему, даже зная открытый ключ Ko;
- при попытке вычислить исходное сообщение M противник также наталкивается на непреодолимую вычислительную проблему, даже зная пару (Ko, C).

Преимущества

- Не нужно предварительно передавать секретный ключ по надёжному каналу.
- Пару ключей можно не менять значительное время (при симметричном шифровании необходимо обновлять ключ после каждого факта передачи).
- В больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Недостатки

- В алгоритм сложнее внести изменения.
- Более длинные ключи.
- Шифрование-расшифрование с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом.
- Требуются существенно бóльшие вычислительные ресурсы,

Длина симметр. ключа, бит	Длина асимметр. ключа , бит
56	384
64	512
80	768
112	1792
128	2304

- Причина работоспособности таких систем: существует односторонняя математическая связь между открытым и секретным ключами так, что:
- Информация об открытом ключе не помогает восстановить секретный
- Владение секретным ключом позволяет расшифровывать сообщения, зашифрованные открытым ключом

Односторонние функции

Криптографические системы с открытым ключом используют так называемые необратимые или односторонние функции,

Односторонней называется функция $F: X \rightarrow Y$, обладающая двумя свойствами:

а) существует полиномиальный алгоритм вычисления значений $y=F(x)$;

б) не существует полиномиального алгоритма *инвертирования* функции F, т.е. решения уравнения $F(x)=y$ относительно x.

Множество классов необратимых функций порождает все разнообразие систем с открытым ключом.

- Функции могут считаться односторонними, даже если для них свойство б) пока строго не доказано, но известно, что задача инвертирования эквивалентна некоторой давно изучаемой трудной математической задаче.
- *Односторонней функцией с секретом К* называется функция $F_K(x)$ $X \rightarrow Y$, зависящая от параметра K и обладающая тремя свойствами:

а) при любом K существует полиномиальный алгоритм вычисления значений $y=F_K(x)$;

б) при неизвестном K не существует полиномиального алгоритма инвертирования F_K (вычисления x по известному y);

в) при известном K существует

- Криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

1. *Разложение больших чисел на простые множители*

Прямая задача - вычисление произведения двух очень больших целых чисел P и Q: N = P * Q, является относительно несложной задачей.

Обратная задача - разложение на множители большого целого числа, т.е. нахождение делителей P и Q большого целого числа N=P * Q является практически неразрешимой задачей при достаточно больших значениях N. По современным оценкам теории чисел при целом $N \approx 2^{664}$ и $P \approx Q$ для разложения числа N потребуется около 10^{23} операций, т.е. задача практически неразрешима на современных ЭВМ.

2. Дискретное логарифмирование

Пусть A и N - целые числа, такие, что 1≤ A< N. Определим множество Z_N: Z_N = {0,1,2,:,N-1} . Тогда модульная экспонента с основанием A по модулю N представляет собой функцию

$$f_{A,N}(x) = A^x \pmod N$$

где x - целое число, 1≤ x≤ N-1.

Существуют эффективные алгоритмы, позволяющие достаточно быстро вычислить значения функции .

Если $y=A^x$, то $x = \log_A x$. Задача дискретного логарифмирования формулируется следующим образом. Для известных целых A, N, y найти целое число x, такое, что $A^x \bmod N = y$

Алгоритм вычисления дискретного логарифма за приемлемое время пока не найден. Поэтому модульная экспонента считается однонаправленной функцией.

- По современным оценкам теории чисел при целых числах A ≈ 2^{664} и N ≈ 2^{664} решение задачи дискретного логарифмирования (нахождение показателя степени x для известного y) потребует около 10^{26}операций, т.е. эта задача имеет в 10^3 раз большую вычислительную сложность, чем задача разложения на множители. При увеличении длины чисел разница в оценках сложности задач возрастает.
- Пока не удалось доказать, что не существует эффективного алгоритма вычисления дискретного логарифма за приемлемое время. Исходя из этого, модульная экспонента отнесена к однонаправленным функциям условно, что, однако, не мешает с успехом применять ее на практике

3. *Вычисление квадратных корней по модулю составного числа*

4. *Особенные математические объекты, называемых эллиптическими кривыми над конечными полями.*

Положения теории чисел, используемые в криптографии с открытым ключом

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

В математике рассматривается так называемая **основная теорема арифметики**, которая утверждает, что

любое *натуральное число* (n>1) либо само является простым, либо может быть разложено *произведение* простых делителей, причем единственным способом.

Разложение на множители называется **каноническим**, если все множители являются простыми и записаны в порядке возрастания. Например, *каноническое разложение* числа 150 на множители: $150 = 2 * 3 * 5^2$

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

Например, числа 11 и 12 взаимно просты.

Исследованием закономерностей, связанных с целыми числами, 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?

Если

где p_1, p_2, ..., p_n – разные простые множители, то n можно представить в виде

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

Число натуральных чисел, не превосходящих n и, взаимно простых с n, называется **функцией Эйлера** и обозначается φ(n)

- $$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \cdots \times \left(1 - \frac{1}{p_n}\right)$$ 1
- **Следствие 2**. Пусть p и q — два различных простых (p<>q). Тогда φ(p*q)= (p-1)(q-1)

- Определить, какие из пар чисел (25,12), (25,15), (13,39), (40,27) взаимно просты.
- Найти значение функции Эйлера:

а) $\varphi(10)$;

б) $\varphi(14)$,

в) $\varphi(20)$.

Модульная арифметика

Каждое целое число a можно разделить с остатком на натуральное число m: $a = km + r \quad 0 \le r < m$.

Остаток от деления числа на m называется вычетом (в данном случае - вычетом числа a по модулю m). Операция, сопоставляющая числу a его вычет по модулю m, называется приведением a по модулю m.

Вычет суммы по модулю m равен сумме вычетов, приведенной при необходимости еще раз по модулю m. Аналогичным свойством обладает вычет произведения. Таким образом, нахождение вычетов больших чисел можно свести к работе с числами, по абсолютной величине не превосходящими квадрата модуля.

- (a+b) mod n =((a mod n) + (b mod n)) mod n
- (ab) mod n =((a mod n) * (b mod n)) mod n

- **Малая теорема Ферма**
- В основе алгоритма шифрования по системе *RSA* лежит теорема, сформулированная в начале семнадцатого столетия без доказательства французским математиком Пьером Ферма (Pierre Fermat). Её часто называют "Малой *теоремой Ферма*«

Малая теорема Ферма формулируется следующим образом. Если p - *простое число*, а m - любое число, которое не делится на p, то $m^{p-1} \equiv 1(mod\ p),$

то есть число m^{p-1} при делении на p дает *остаток* 1

Используя теорему Ферма вычислить: а) 2^{12} mod13 ;

б) 3^{13} mod13 , в) 5^{22} mod11

Теорема Эйлера утверждает, что для любых взаимно простых чисел m и n (m < n) $m^{\varphi(n)}$mod*n* = 1 или $m^{k\varphi(n)+1}$ mod*n* = 1

Теорема Ферма-Эйлера . Если p и q - два различных простых числа. а m - любое число. которое не делится на p и q, то $m^{(p-1)(q-1)} \equiv 1(mod\ pq).$

Используя теорему Эйлера вычислить: а) 5^4 mod12 ,

б) 3^9 mod20 , в) 2^{14} mod21

- **Наибольший общий делитель**

Пусть a и b — два целых положительных числа. Наибольший общий делитель чисел a и b наибольшее число c, которое делит и a, и b: c = НОД(a, b).

Для нахождения наибольшего общего делителя можно использовать следующий *алгоритм* **Евклида**.

- Алгоритм NOD (целые a, b, c);

Начало

1. Пока a<>b выполнять:

   1.1.Если a>b то a:=a-b, иначе b:= b-a;

2. c:=a;

Конец.

- **Обобщенный алгоритм Евклида**

Теорема. Пусть a и b — два целых положительных числа. Тогда существуют целые (не обязательно положительные) числа x и y, такие, что ax + by = НОД(a,b).

- **Инверсия по модулю m**

Во многих задачах криптографии для заданных чисел c, m требуется находить такое число d < m, что cd mod m = 1

- Такое d существует тогда и только тогда, когда числа c и m взаимно простые. Число d, удовлетворяющее равенству cd mod m = 1, называется **инверсией** c **по модулю** m и часто обозначается c^{-1} mod m. Данное обозначение для инверсии связано с тем, что *равенство* cd mod m = 1 можно переписать в виде cc^{-1} mod m = 1.
- Таким образом, *умножение* на c^{-1} соответствует делению на c при вычислениях по модулю m.
- Инверсию по модулю m также можно вычислять с помощью обобщенного алгоритма Евклида.

Алгоритм рюкзака

Разработан Мерклом и Хеллманом в 1976 году.

Рюкзачная последовательность A = (a1,…an) – это упорядоченный набор из n, n ≥ 3, различных натуральных чисел a_i. Входом задачи о рюкзаке называется пара (A, α), где A – рюкзачная последовательность, а α – натуральное число. Решением для входа (A, α) будет такое подмножество из A, сумма элементов которого равняется α.

- В варианте, используемом в криптографии, нужно для данного входа (A, α) построить решение, зная, что такое решение существует.
- Последовательность A используется для шифрования блока C из n двоичных символов путем суммирования тех компонент A, для которых в соответствующих позициях C стоит единица. Если эту сумму обозначить через α, то тогда дешифрование равносильно нахождению C по A и α
- Например, пусть задана последовательность
- A = (3, 41, 5, 1, 21, 10). Тогда двоичные блоки (1, 1, 0, 0, 1, 0) и (1, 0, 1, 1, 0, 1) шифруются как 65 и 19 соответственно.

- Существуют две различные проблемы рюкзака. Одна решается за линейное время, а другая, как считается, – нет.
- Если рюкзачная последовательность является сверхвозрастающей $a_j > \sum_{i=1}^{j-1} a_i$

(т.е. , для j = 2,…,n), то полученную проблему можно легко решить.

- Последовательность просматривается справа налево. Значение α сравнивается с самым большим элементом. Если α меньше, то число не участвует в формировании в шифротекста, иначе – участвует. Далее α уменьшается на это число. Аналогичные действия производятся со следующим по величине элементом последовательности. до тех пор, пока α не уменьшится до нуля.
- Например, пусть полный вес рюкзака - 70, а последовательность весов {2,3,6, 13,27,52}.Открытый текст, полученный из значения шифротекста 70, был бы равен 110101

Нормальные рюкзаки представляют собой трудную проблему. Единственным способом определить, какие элементы входят в сумму, является методическая проверка возможных решений. Самый быстрый алгоритм имеет экспоненциальную зависимость от числа элементов.

- В алгоритме Меркла-Хеллмана закрытый ключ является последовательностью весов сверхвозрастающего рюкзака. Открытый ключ - это последовательность весов нормального рюкзака с тем же решением.
- чтобы получить нормальную последовательность рюкзака, сверхвозрастающую последовательность рюкзака, например, {2,3,6,13,27,52}, умножим по модулю n все значения на число m. Значение модуля должно быть больше суммы всех чисел последовательности, например, n=105. Множитель должен быть взаимно простым числом с модулем, например, m=31. Нормальной последовательностью рюкзака будет

2*31 mod 105 = 62

3*31 mod 105 = 93

6*31 mod 105 = 81

13*31 mod 105 = 88

27*31 mod 105 = 102

52*31 mod 105 = 37

Итого- {62,93,81,88,102,37}.

Шифрование
сообщение = 011000 110101 101110
011000 соответствует 93 + 81 = 174
110101 соответствует 62 + 93 + 88 + 37 = 280
101110 соответствует 62 + 81 + 88 + 102 = 333
Шифротекстом будет последовательность 174,280,333

Дешифрирование
Определяется m^{-1}, такое что $m(m^{-1})=1(\text{mod } n)$. Каждое значение щифротекста умножается на m^{-1} mod n, а затем разделяется с помощью закрытого ключа, чтобы получить значения открытого текста.

В примере сверхвозрастающая последовательность - {2,3,6,13,27,52}, n равно 105, а m - 31. Шифротекстом служит 174,280,333. В этом случае $п^{-1}$ равно 61, поэтому значения шифротекста должны быть умножены на 61 mod 105.

174*61 mod 105 = 9 = 3 + 6, что соответствует 011000
280*61 mod 105 = 70 = 2 + 3 + 13 + 52, что соответствует 110101
333*61 mod 105 = 48 = 2 + 6 + 13 + 27, что соответствует 101110
Расшифрованным открытым текстом является 011000 110101 101110.

- Реальные рюкзаки должны содержать не менее 250 элементов. Длина каждого члена сверхвозрастающей последовательности должна быть где-то между 200 и 400 битами, а длина модуля должна быть от 100 до 200 битов. Для получения этих значений практические реализации используют генераторы случайной последовательности.

Алгоритм RSA

В 1977 году в журнале Scientific American трое ученых Рональд Ривест, Ади Шамир и Леонард Адлеман из Массачусетского технологического института опубликовали методом криптографической защиты информации RSA, названный так по начальным буквам фамилий ее изобретателей.

В основу криптографической системы с открытым ключом RSA положена сложность задачи факторизации произведения двух больших простых чисел. Для шифрования используется операция возведения в степень по модулю большого числа. Для дешифрования за разумное время (обратной операции) необходимо уметь вычислять функцию Эйлера от данного большого числа, для чего необходимо знать разложения числа на простые множители.

– выбираются 2 различных простых числа ***p*** и ***q***;

– вычисляется ***n = pq*** и функция Эйлера

m = (p–1)(q–1); Функция Эйлера указывает количество положительных целых чисел в интервале от 1 до n, которые взаимно просты с n.

– Выбирается целое число ***e***, взаимно простое с ***m***.

– Вычисляется число ***d***, удовлетворяющее условию: ***ed = 1 (mod m)***.

– Секретным ключом абонента является тройка чисел ***(p, q, d)***, открытым ключом — пара чисел ***(n, e)***.

– Открытые ключи всех абонентов помещаются в общедоступный справочник.

Закодированный с помощью RSA текст защищён от несанкционированного прочтения настолько, насколько затруднено разложение на множители числа n.

Шифрование:

1. Отправитель разбивает свое сообщение на блоки, равные $k=[\log_2(n)]$ бит, блок, может быть интерпретирован как число из диапазона $(0;2^k-1)$.
2. Для каждого такого числа (назовем его m_i) вычисляется выражение $c_i=((m_i)^e) \bmod n$.

Дешифрование

$((c_i)^d) \bmod n = ((m_i)^{e*d}) \bmod n = m_i$.

Частный случай теоремы Эйлера утверждает, что если число $n = p * q$, то для любого x имеет место равенство $(x^{(p-1)(q-1)}) \bmod n = 1$.

$((m_i)^{e*d}) \bmod n = ((m_i)^{k(p-1)(q-1)+1}) \bmod n =$

$((m_i)^{(p-1)(q-1)})^k * (m_i) \bmod n = m_i$.

пример использования метода RSA для шифрования сообщения "CAB". 1. Выберем p=3 и q=11.

2. Определим n=3*11=33.

3. Найдем (p-1)*(q-1)=20. Следовательно, в качестве d выберем любое число, которое является взаимно простым с 20, например d=3.

4. Выберем число e. В качестве такого числа может быть взято любое число, для которого удовлетворяется соотношение (e*3) mod 20 = 1, например 7.

5. Представим шифруемое сообщение как последовательность целых чисел в диапазоне 0...32. Пусть буква A изображается числом 1, буква B - числом 2, а буква C - числом 3. Тогда сообщение можно представить в виде последовательности чисел 3 1 2.

Зашифруем сообщение, используя ключ {7,33}:

$C1=(3^7) \bmod 33 = 2187 \bmod 33 = 9$,

$C2=(1^7) \bmod 33 = 1 \bmod 33 = 1$,

$C3=(2^7) \bmod 33 = 128 \bmod 33 = 29$.

Расшифруем сообщение {9,1,29}, полученное в результате зашифрования по известному ключу на основе секретного ключа {3,33}:

$M1=(9^3) \bmod 33 = 729 \bmod 33 = 3$,

$M2=(1^3) \bmod 33 = 1 \bmod 33 = 1$,

$M3=(29^3) \bmod 33 = 24389 \bmod 33 = 2$.

Таким образом, в результате расшифрования сообщения получено исходное сообщение "CAB".

Алгоритм быстрого возведения в степень по модулю

Предположим, что требуется вычислить $z = a^b \bmod n$. Рассмотрим следующий алгоритм:

1. Представим b в двоичный системе исчисления: $b = (b_0\, b_1 \ldots b_k)_2$, $b_i \in \{0, 1\}$. Например, $199 = 11000111_2$,

2. Заполним следующую таблицу

b	b_0	b_1	...	b_k
a	a_0	a_1	...	a_k

где $a_0 = a$, $a_{i+1} = \begin{cases} a_i^2 \bmod n, & \text{если } b_{i+1} = 0, \\ a_i^2 \cdot a \bmod n, & \text{если } b_{i+1} = 1 \end{cases}$ для $i \geq 0$.

Результат появится в последней ячейке второй строки.

Пример. Вычислить $2^{199} \bmod 1003$:

b	1	1	0	0	0	1	1	1
c	2	8	64	84	35	444	93	247

Ответ: $2^{199} \bmod 1003 = 247$.

Алгоритм ElGamal

1. Генерация ключей
- Генерируется случайное простое число p длины n битов. (p=11)
- Выбирается случайное число g<p . (g=2)
- Выбирается случайное целое число x такое, что 1<x<p-1. (x=8)
- Вычисляется $y=g^x \bmod p$. $y=2^8 \bmod 11=3$
- Открытым ключом является тройка (p, g, y) – (11, 2, 3), закрытым ключом — число x (8).

2. Шифрование
- Сообщение M шифруется следующим образом: (M=5)
- Выбирается сессионный ключ k — случайное целое число такое, что 1<k<p-1. k=9
- Вычисляются числа $a=g^k \bmod p$ и $b=M\ y^k \bmod p$. $a=2^9 \bmod 11=6$: $b=5\ 3^9 \bmod 11=9$
- Пара чисел (a,b) является шифротекстом. (6,9)

3. Дешифрование

$$b(a^x)^{-1} \equiv (y^k M)g^{-xk} \equiv (g^{xk} M)g^{-xk} \equiv M \pmod p$$

$$M = b(a^x)^{-1} \bmod p = b \cdot a^{(p-1-x)} \bmod p$$

Асимметричные криптосистемы на базе эллиптических кривых

Эллиптической кривой **E** называется множество точек (**x**, **y**), удовлетворяющих однородному уравнению Вейерштрасса:

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5,$$

где a_i - коэффициенты уравнения

$$y^2 = x^3 + ax + b \pmod p,$$

при этом a и b должны удовлетворять неравенству

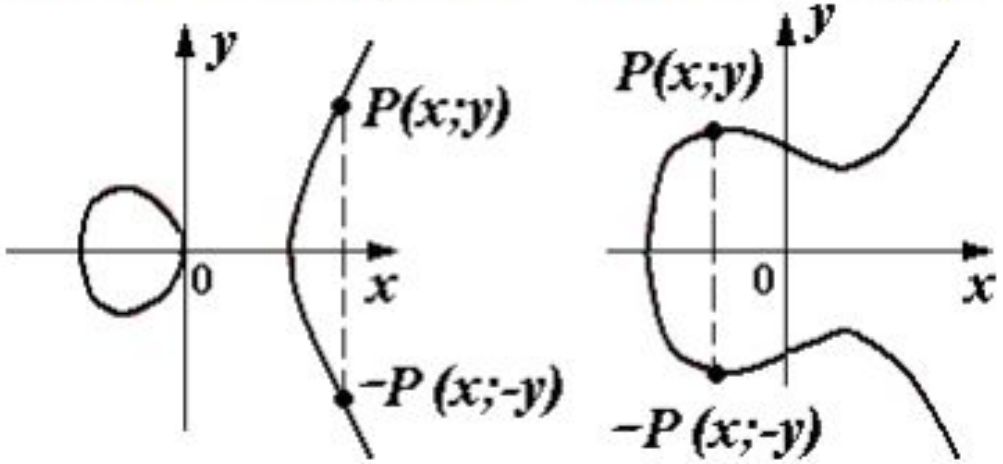
$$4a^3 + 27b^2 \pmod p \neq 0 \text{ и } p > 3.$$

- Введем две операции, которые можно выполнять над точками кривой.
- **Сложение точек** $P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2 2, y_2)$
- **Умножение точки** на число $P_k(x_k, y_k) = k * P(x, y)$.

стойкость шифрования с помощью эллиптических кривых базируется на сложности нахождения множителя **k** точки **P** по их произведению. Т.е. если **Q = k P**, то зная **P** и **k** довольно легко вычислить **Q**. Эффективное решение обратной задачи (найти **k** при известных **P** и **Q**) на текущий момент пока не опубликовано.

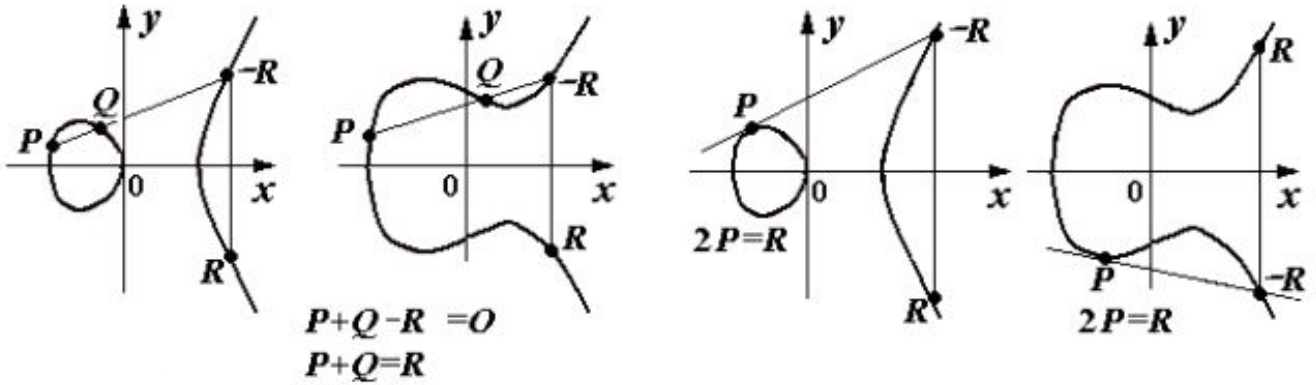
Законы сложения точек кривой и построение группы точек кривой. Симметрия кривой относительно оси Ox дает наглядное определение обратной точки. А именно: ***обратной точкой*** для точки $P(x;y)$ на эллиптической кривой называют точку $-P(x;-y)$.

Замечательным свойством несингулярных кривых является то, что любая прямая, проходящая через две различные точки кривой пересекает кривую в единственной точке. Кроме того, касательная к эллиптической кривой в любой точке (кроме точек перегиба) пересекает ее еще в одной точке.



Такие особенности позволяют задать групповую операцию, называемую ***сложением точек эллиптической кривой***.

Суммой двух точек P и Q называется точка $R = P + Q$, обратная третьей точке пересечения эллиптической кривой и прямой, проходящей через точки P и Q.



Суммирование точек

Удвоение точки

Если суммируемые точки P и Q совпадают, то $P+Q=P+P=R$, что равносильно ***удвоению точки*** $2P=R$. При $P=Q$ секущая PQ превращается в касательную к кривой и геометрически удвоенная точка $2P$ – это точка, обратная к точке пересечения этой касательной и эллиптической кривой.

Найдем координаты точки $R=P+Q=(x_3;y_3)$, выразив их через координаты точек $P(x_1;y_1)$ и $Q(x_2;y_2)$. При этом точки P и Q могут быть различными или совпадающими. В соответствии с этим имеем два случая:

1). $P\neq\pm Q$. Запишем уравнение прямой PQ. Угловой коэффициент прямой PQ равен:

$$\lambda=\frac{y_2-y_1}{x_2-x_1}.$$

Уравнение PQ: $y=y_1+\lambda(x-x_1)$. Ищем третью точку пересечения кривой и прямой PQ:

$$\begin{cases}y^2=x^3+ax+b,\\ y=y_1+\lambda(x-x_1)\end{cases}\Rightarrow\quad (y_1+\lambda(x-x_1))^2=x^3+ax+b$$

Возводя в квадрат и группируя подобные члены, получим кубическое уравнение $x^3 - \lambda^2 x^2 + \ldots = 0$. По теореме Виета для кубических уравнений сумма корней кубического уравнения равна коэффициенту при x^2, взятому с противоположным знаком, т.е.

$$x_1 + x_2 + x_3 = \lambda^2 .$$

$$x_3 = \lambda^2 - x_1 - x_2 .$$

Подставив x_3 в уравнение прямой PQ, находим ординату точки $-R$:

$$y_3' = y_1 - \lambda(x_3 - x_1).$$

Точка $R(x_3; y_3)$ – симметрична точке $-R$ относительно оси Ox, поэтому

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

2). При $P = Q$, $R = 2P$. Дифференцируем обе части равенства $y^2 = x^3 + ax + b$:

$$2ydy = 3x^2 + a .$$

В точке $P(x_1; y_1)$ производная равна угловому коэффициенту касательной к кривой:

$$\lambda = \left.\frac{dy}{dx}\right|_{(x_1;y_1)} = \frac{3{x_1}^2 + a}{2y_1}.$$

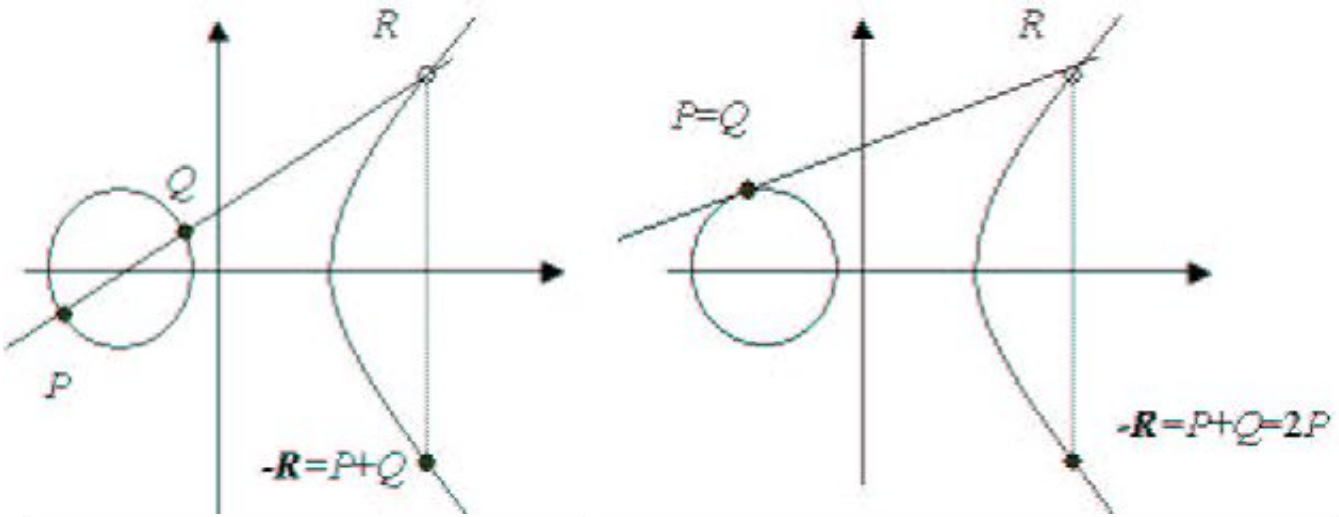
Координаты удвоенной точки $R(x_3; y_3) = 2P$:

$$x_3 = \lambda^2 - 2x_1;$$
$$y_3 = \lambda(x_1 - x_3) - y_1.$$

Чтобы построить группу E точек эллиптической кривой, выберем в качестве нейтрального элемента группы точку $O(x\ ;\infty)$, для которой положим:

$$P + (-P) = O, \qquad \forall P \in E.$$

Прямая, проходящая через точки P и $-P$, перпендикулярна к оси абсцисс и поэтому можно принять, что третья точка пересечения перпендикуляра и кривой уходит в бесконечность вдоль оси ординат. Поэтому точку O называют ***точкой на бесконечности*** (***бесконечно удаленной точкой***) кривой.



Операция	Поле характеристики p, где $p \neq 2$ и $p \neq 3$
Сложение точек $P \neq \pm Q$ $P(x_1;y_1)+Q(x_2;y_2)=R(x_3;y_3)$	$\lambda = \frac{y_2 - y_1}{x_2 - x_1} (\mathrm{mod}\, p);$ $x_3 = \lambda^2 - x_1 - x_2 (\mathrm{mod}\, p);$ $y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, p)$
Удвоение точки $R(x_3;y_3)=2P(x_1;y_1)$	$\lambda = \frac{3x_1^{\,2} + a}{2y_1} (\mathrm{mod}\, p);$ $x_3 = \lambda^2 - 2x_1 (\mathrm{mod}\, p);$ $y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, p)$
$O+O=O;$ $P(x;y)+O=P(x;y);$ $P(x;y)+P(x;-y)=O$	

- Умножение точки P *эллиптической кривой* на положительное число k определяется как сумма k точек P

Алгоритм вычисления точек на *эллиптической кривой*

- *Для каждого x (0 ≤ x ≤ p) вычисляется*

$$x^3 + ax + b \pmod p$$

- Выясняется: имеет ли это значение квадратный корень
- Если корень – есть, то эти два значения (x,y) являются точками

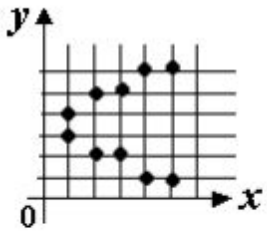
$$E_p (a,b)$$

Пример 1. Найти все точки эллиптической кривой $E_7(2,6)$.

Р е ш е н и е. $E_7(2,6)$ – это кривая $y^2 = x^3 + 2x + 6 (\mathrm{mod}\, 7)$.

Считаем значения $x^3 + 2x + 6 (\mathrm{mod}\, 7)$ и $y^2 (\mathrm{mod}\, 7)$ для $x, y, = 1,2,\ldots,6$.

x	1	2	3	4	5	6
$x^3 + 2x + 6 (\mathrm{mod}\, 7)$	2	4	4	1	1	3
y	1	2	3	4	5	6
$y^2 (\mathrm{mod}\, 7)$	1	4	2	2	4	1



Группа $E_7(2,6)$ состоит из точек $(x;y)$, при которых $y^2 (\mathrm{mod}\, 7) = x^3 + 2x + 6 (\mathrm{mod}\, 7)$. Это точки $(1,3)$, $(1,4)$, $(2,2)$, $(2,5)$, $(3,2)$, $(3,5)$, $(4,1)$, $(4,6)$, $(5,1)$, $(5,6)$ и O. На графике есть симметрия относительно прямой $y = p/2 = 3,5$.

Пример 2. Вычислить: а) $(8,3)+(3,6)$; б) $2(1,8)$ в группе $E_{11}(1,6)$.

Р е ш е н и е. Кривая $E_{11}(1,6)$ – это $y^2 = x^3 + x + 6 (\mathrm{mod}\, 11)$.

а) $(x_1, y_1) = (8,3)$; $(x_2, y_2) = (3,6)$.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{6-3}{3-8} = \frac{3}{-5} \equiv -3 \cdot 5^{-1} \equiv -3 \cdot 9 \equiv 6 (\mathrm{mod}\, 11);$$

$$x_3 = \lambda^2 - x_1 - x_2 \equiv 36 - 8 - 3 \equiv 3 (\mathrm{mod}\, 11);$$

$$y_3 = \lambda (x_1 - x_3) - y_1 = 6(8-3) - 3 \equiv 5 \Rightarrow (8,3) + (3,6) = (3,5).$$

б) $(x_1, y_1) = (1,8)$; $\lambda = \dfrac{3x_1^{\,2} + a}{2y_1} = \dfrac{3 \cdot 1 + 1}{2 \cdot 8} = \dfrac{4}{16} = 4^{-1} \equiv 3 (\mathrm{mod}\, 11)$;

$$x_3 = \lambda^2 - 2x_1 = 9 - 2 \cdot 1 \equiv 7 (\mathrm{mod}\, 11);$$

$$y_3 = \lambda (x_1 - x_3) - y_1 = 3(1-7) - 8 \equiv 7 (\mathrm{mod}\, 11); \quad \Rightarrow \quad 2(1,8) = (7,7).$$

2. Способы использования эллиптических кривых

Шифрование/дешифрование с использованием эллиптических кривых

Параметры - *эллиптическая кривая* $E_p(a,b)$ и точка G на ней. Участник B выбирает закрытый ключ n_B и вычисляет открытый ключ $P_B = n_B \times G$. Чтобы зашифровать сообщение P_m используется открытый ключ получателя B P_B. Участник A выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение C_m, являющееся точкой на *эллиптической кривой*.

$$C_m = \{k \times G, P_m + k \times P_B\}$$

Шифрование/дешифрование с использованием эллиптических кривых

Чтобы дешифровать сообщение, участник B умножает первую координату точки на свой закрытый ключ и вычитает результат из второй координаты:

$$P_m + k \times P_B - n_B \times (k \times G) =$$
$$P_m + k \times (n_B \times G) - n_B \times (k \times G) = P_m$$

Участник А зашифровал сообщение P_m добавлением к нему kxP_B. Никто не знает значения k, поэтому, хотя P_B и является открытым ключом, никто не знает $k \times P_B$. Противнику для восстановления сообщения придется вычислить k, зная G и $k \times G$. Сделать это будет нелегко.

Получатель также не знает k, но ему в качестве подсказки посылается $k \times G$. Умножив $k \times G$ на свой закрытый ключ, получатель получит значение, которое было добавлено отправителем к незашифрованному сообщению. Тем самым получатель, не зная k, но имея свой закрытый ключ, может восстановить незашифрованное сообщение

Схема алгоритма Рабина − Миллера

Пусть дано нечетное число p. Надо проверить является ли число p простым. Далее предположим, что $p - 1 = 2^s t$.

1. Выбираем случайное число a, меньшее p и определяем k = 0.
2. Вычисляем с помощью алгоритма Эвклида НОД двух чисел a и p. Если НОД (a, p) ≠ 1, то p – составное число.
3. Вычисляем $b \equiv a^t \bmod p$. Если b = 1 или b = p − 1, то число p вероятно простое.
4. Если b≠ 1 и b ≠ p − 1, то вычисляем $b \equiv b^2 \bmod p$ и k= k + 1.
5. Если число b = p − 1, то число p вероятно простое. Перейти на шаг 7.
6. Пока k < s выполнять пункт 4.
7. Завершить работу алгоритма.

Пример. Пусть $p = 181$. Имеем $p - 1 = 45 \times 2^2$. По представленному разложению определяем значение параметра $t = 45$.

1. Выбираем случайное число $a = 52 < p$, и определяем $k = 0$.
2. Используем алгоритм Эвклида для вычисления НОД двух чисел 52 и 181: получаем, что НОД двух чисел 181 и 52 равен 1.
3. Вычисляем $b \equiv 52^t \bmod 181 \equiv 52^{45} \bmod 181$: $180 \bmod 181$. получили $b = 180 = p - 1$. Откуда следует, что число $p = 181$ вероятно простое

- В тесте Рабина-Миллера вероятность получить результат "не простое число" — 1/4. Если число прошло m тестов (с m различными основаниями *a*), вероятность, что тест выдаст не простое число — $(1/4)^m$. Для практических приложений достаточно повторить тест Рабина-Миллера 5 раз.