Методы асимметричного шифрования

Шифр Эль-Гамаля

Историческая справка

- Схема была предложена в 1985 году Тахером Эль-Гамалем (Taher Elgamal), египетским криптографом
- В отличие от RSA алгоритм Эль-Гамаля не был запатентован и, поэтому, стал более дешевой альтернативой
- Схема Эль-Гамаля лежала в основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).

Шифр Elgamal

- Шифр является усовершенствованием системы Диффи-Хеллмана
- Шифр основан на вычислении дискретных логарифмов в конечном поле :
  - Пусть $y = g^x mod\ p$
  - Вычислительно трудно найти *x* при известных *y, g, p*
- Проблема вычисления дискретного логарифма имеет такую же сложность, как проблема разложения на множители

Elgamal генерация ключей

- Генерируется случайное простое число p
- Выбирается целое число g такое, что $1< g< p$, и g-порождающий элемент циклической группы (генератор) порядка p, для которого справедливо: $g \bmod p, g^2 \bmod p, g^3 \bmod p \ldots g^{p-1} \bmod p$ являются различными целыми из $[1,p-1]$
- Выбирается случайное целое число x такое, что $1 < x < p$
- Вычисляется $y = g^x \bmod p$
- Открытым ключом объявляется тройка (p, g, y)
- Закрытым ключом назначается число x

Elgamal зашифрование

- Открытый текст разбивается на блоки m_i размером $\mathrm{k} = [\log_2 \mathrm{p}]$ бит. Блоки интерпретируются, как числа из диапазона *(0; 2^k -1)*
- Ключ шифрации (открытый ключ) – тройка *(p, g, y)*
- Выбирается сессионный ключ-случайное целое число *k, 1<k<p-1*
- Каждый блок открытого текста преобразуется в пару чисел *(a,b)*:

$$a = \left(g^k\right) mod\ p \qquad b = (y^k * m_i)mod\ p$$

- Эта пара чисел *(a,b)* является блоком шифротекста c_i
- Длина шифротекста вдвое больше длины исходного сообщения

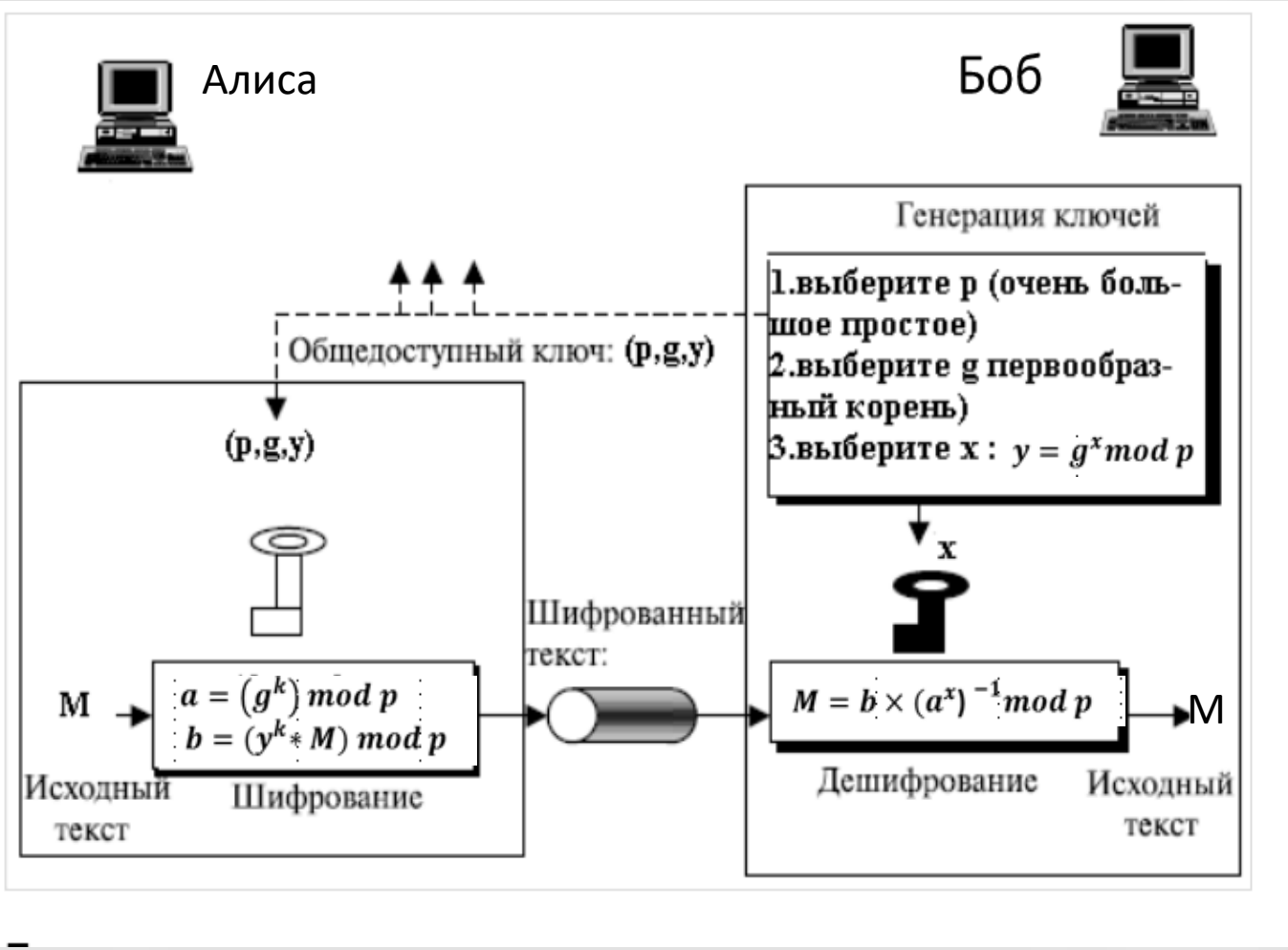
Elgamal расшифрование

- Ключ расшифрования – число *x* (закрытый ключ)
- Блок шифротекста преобразуется в открытый текст по формуле:
  - $m_i = b \times (a^x)^{-1} mod\ p$
  - Поскольку $(a^x)^{-1} \equiv g^{-kx} mod\ p$ (подстановка ранее определенного *a*), имеем (подстановка ранее определенного *y*):

    $b \times (a^x)^{-1} \equiv (y^k * m_i) \times g^{-kx} \equiv (g^{kx} * m_i) \times g^{-kx} \equiv m_i\ mod\ p$
- Для практических вычислений используется выражение:

  $m_i = b \times (a^x)^{-1} mod\ p = b \times a^{(p-1-x)} mod\ p$ (т. к. $a^{(p-1)} \equiv 1 mod\ p$ согласно малой теоремы Ферма)

Протокол конфиденциальной передачи сообщения на основе шифра Elgamal



- Отправитель создает маску $y^k = g^{xk}$, которая скрывает значение открытого текста M.
- Получатель создает точную копию маски $a^x = g^{kx}$ и инвертирует ее (мультипликативная инверсия), чтобы снять маску с шифротекста
- Отправителю остается неизвестным число *x*, а получателю остается неизвестным число *к*

Пример

- Ключ: p=11, g=2($2^{10} \equiv 1 \bmod 11$), $x = 3, y = g^x \bmod p = 2^3 \bmod 11 = 8$.
  - Открытый ключ (p,g,x)=(11,2,8)
  - Закрытый ключ x=3
- Зашифрование открытого текста m_i=7
  - k=4, $a = (g^k) \, mod \, p$=2^4mod11=5; $b = (y^k * m_i) mod \, p = (4096 \times 7) mod 11 = 6$
  - Зашифрованный текст (a,b)=(5,6)
- Расшифрование:
  - $b \times a^{(p-1-x)} mod \, p$=6× 5^7mod11=6× $3 mod \, 11 = 7 = m_i$

Безопасность шифра

- Чтобы шифр Эль-Гамаля был безопасен, модуль p должен содержать по крайней мере 300 десятичных цифр
- Модуль p или случайное число k, которое отправитель использует для зашифровки, должны обновляться для каждой передачи сообщения, чтобы предотвратить атаку знания исходного текста:
  - $b = (y^k * M) mod\ p \quad b' = (y^k * M') mod\ p$ и пусть M стало известно
  - Тогда $y^k = b \times M^{-1} mod\ p$ и $M' = b' \times (y^k)^{-1} mod\ p$
- Шифр Эль-Гамаля может использоваться всякий раз, когда может использоваться RSA, т.е. шифрования и дешифрования маленьких сообщений

Эллиптическая криптография

Эллиптическая криптография

- Безопасность RSA и Elgamal обеспечивается ценой использования больших ключей
- Требуется альтернативный метод, который дает тот же самый уровень безопасности, но с меньшими размерами ключей
- Одним из этих перспективных вариантов является криптосистема на основе метода эллиптических кривых (*Elliptic Curve Cryptosystem — ECC*)

Эллиптические кривые в вещественных числах

- Эллиптические кривые обычно применяются для вычисления длины кривой в окружности эллипса:

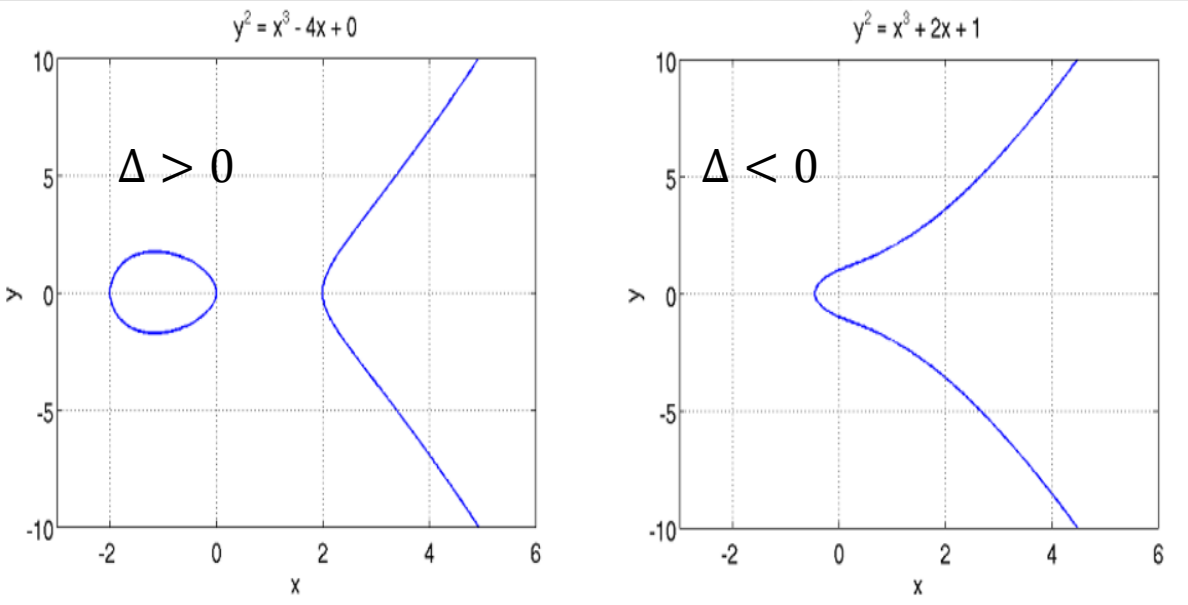
$$y^2 + \text{axy} + by = x^3 + cx^2 + \text{dx} + e$$

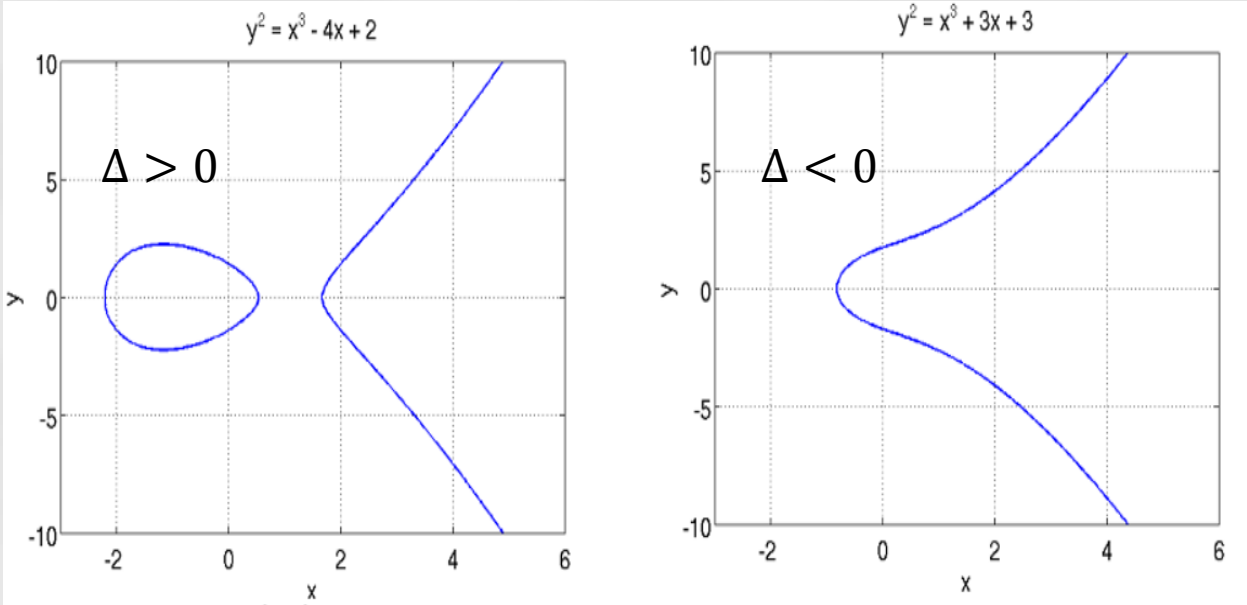
- В криптографии распространение получил частный вид эллиптических кривых:

$$y^2 = x^3 + \text{ax} + b$$

- Если дискриминат $\Delta = -16(4a^3 + 27b^2) \neq 0$, уравнение представляет несингулярную (гладкую) эллиптическую кривую, иначе сингулярную (с особыми точками)

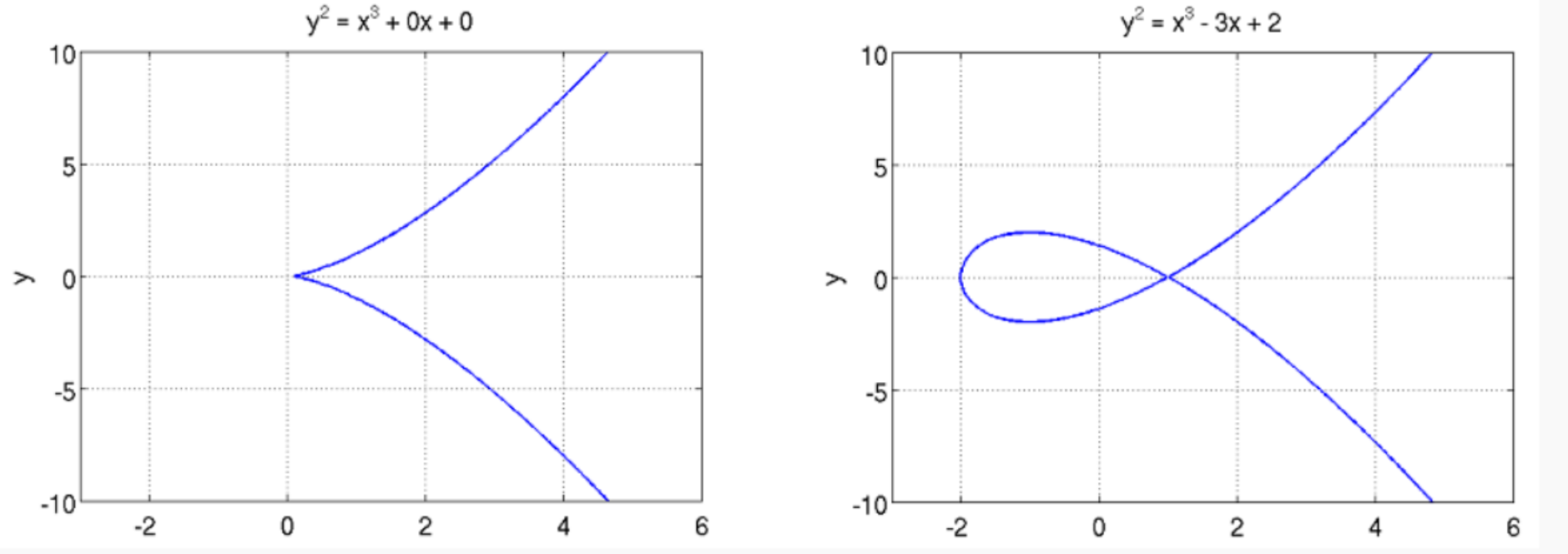
Примеры несингулярных эллиптических кривых





- График не имеет особых точек (возврата и самопересечений)
- График имеет две части, если дискриминат Δ положителен и одну часть, если значение дискриминанта Δ отрицательно
- *Замечательным свойством несингулярных кривых является то, что любая прямая, проходящая через две различные точки кривой ещё раз пересекает кривую и эта третья точка пересечения является единственной !*

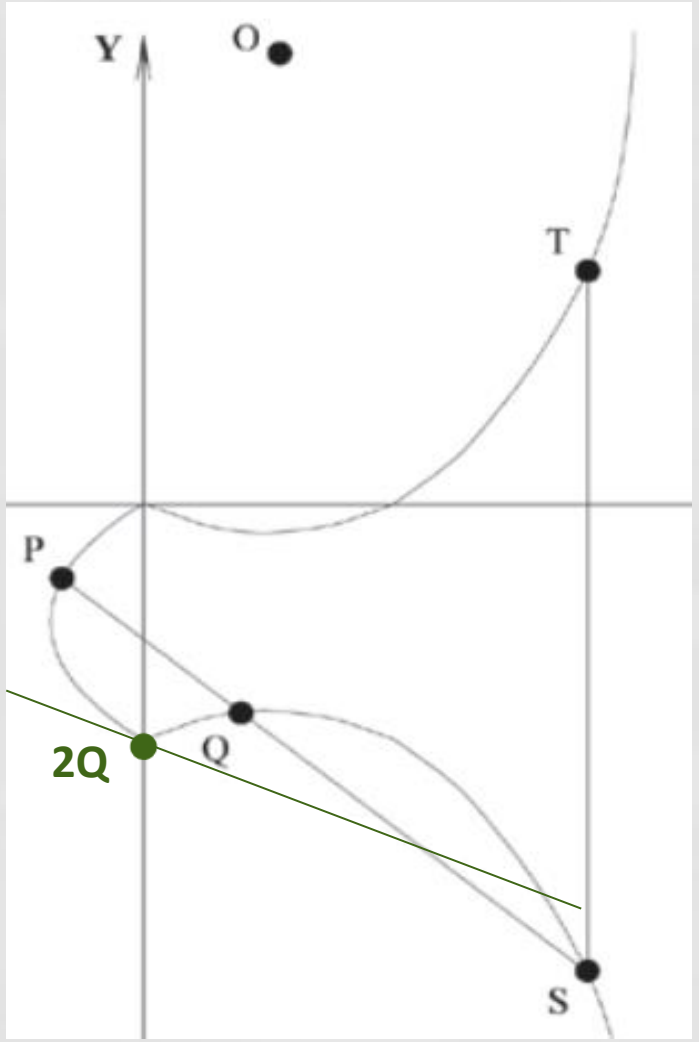
Примеры сингулярных эллиптических кривых



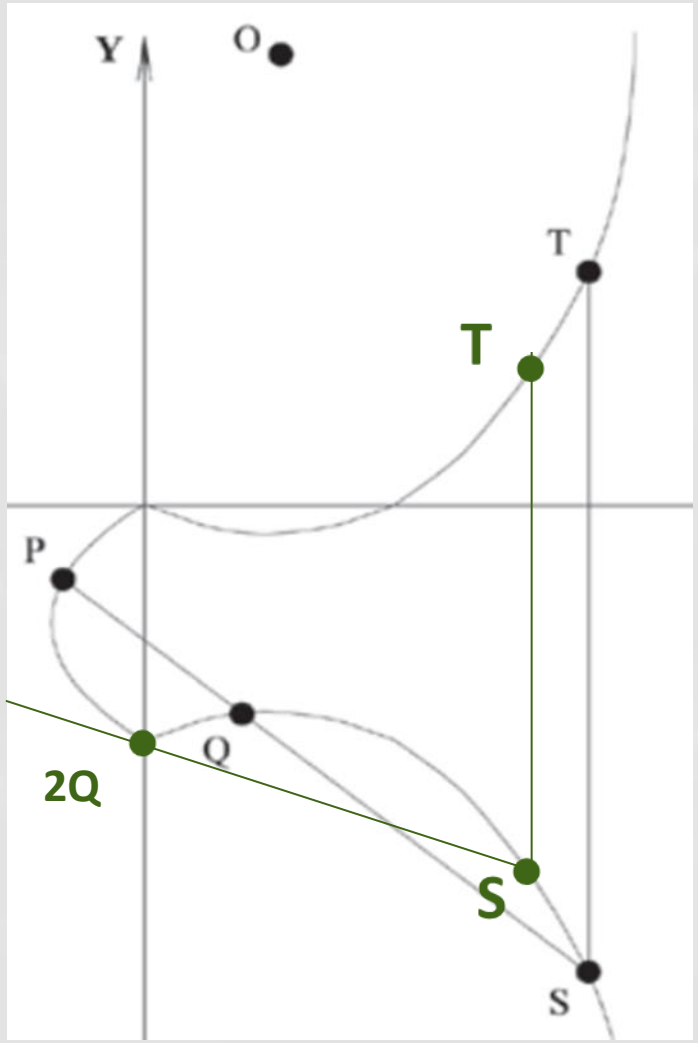
- При использовании сингулярных кривых стойкость эллиптической криптосистемы значительно снижается

Свойства точек эллиптической кривой

- Предполагаем:
  - На плоскости существует бесконечно удаленная точка **O**, принадлежащая кривой, в которой сходятся все вертикальные прямые линии
  - Если три точки эллиптической кривой лежат на прямой линии, то их сумма есть **O**
  - Касательная к кривой пересекает точку касания два раза



Сложение точек эллиптической кривой



- Точка **O** выступает в роли нулевого элемента: **O**=-**O** и для любой точки P на кривой справедливо P + **0** = P
- Вертикальная линия пересекает кривую в двух точках с одной и той же абсциссой (координатой x), например, S = (x, y), T = (x, -y), и в бесконечно удаленной точке: S + T + **O** = **O** и T = -S
- Чтобы сложить две точки P и Q с разными координатами x, следует провести через эти точки прямую и найти точку пересечения ее с эллиптической кривой: P + Q + S = **O**
- Чтобы удвоить точку Q, следует провести касательную в точке Q и найти другую точку пересечения S с эллиптической кривой. Тогда Q + Q +S= 2 x Q +S=**O**
- Умножение точки P эллиптической кривой на положительное число k определяется как сумма k точек P

Эллиптические кривые в криптографии

- Эллиптические кривые над вещественными числами приводит нас к проблеме округления (тексты должны представляться целыми числами)

- В криптографии используются только кривые над конечными полями, т.е. координаты точек кривой принадлежат конечному полю

Эллиптические кривые в GF(p)

- Элементами данной эллиптической кривой являются пары неотрицательных целых чисел, которые меньше p $(p>3)$ и удовлетворяют частному виду эллиптической кривой

$$y^2 = (x^3 + ax + b) mod\ p$$

- Такую кривую будем обозначать $E_p(a, b)$. При этом числа a и b должны быть меньше p и должны удовлетворять условию $(4a^3 + 27b^2) mod\ p \neq 0$
- Любая точка на $E_p(a, b)$ вычисляется следующим образом:
  - Для значения x, $0 <= x <= p$, вычисляется $(x^3 + ax + b)\ mod\ p$
  - Для каждого из полученных на предыдущем шаге значений выясняется имеет ли это значение квадратом целого числа. Если является, то определяется y

Пример

- Задана кривая $E_{13}(1,1)$. Проверить принадлежность кривой точек *P(4, 2), R(3,5)* и *Q(7,0)*
  - $E_{13}(1,1)$ обозначает $y^2 = (x^3 + x + 1) mod\ 13$
  - Вычисляем $(4^3 + 4 + 1)\ mod\ 13 = (12 + 4 + 1)\ mod\ 13 = 4 = 2^2$
  - Вычисляем $(3^3 + 3 + 1)\ mod\ 13 = (27 + 3 + 1)\ mod\ 13 = 5$
  - Вычисляем $(7^3 + 7 + 1)\ mod\ 13 = (5 + 7 + 1)\ mod\ 13 = 0 = 0^2$

Свойства точек $E_p(a,b)$

- *P + **0** = P; P+Q=Q+P (коммут.); (P+Q)+R=P+(Q+R) (ассоциат.)*
- Если *P = (x,y),* то *P + (x,-y) = 0*. Точка *(x,-y)* является отрицательным значением точки *P* и обозначается -P. Точка -P лежит на эллиптической кривой, т.е. принадлежит $E_p\ (a,b)$.
- Если $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, то $P + Q = (x_3, y_3)$ определяется по следующим формулам:
- $x_3 = (\lambda^2 - x_1 - x_2)\ mod\ p \quad y_3 = (\lambda(x_1 - x_3) - y_1) mod\ p$

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) mod p, & P \neq Q \\ ((3x_1^2 + a))/2y_1\ mod p, & P = Q \end{cases}$$

- λ- угловой коэффициент секущей, проведенный через точки *P* и *Q*

Свойства точек $E_p(a,b)$

- *P + **0** = P; P+Q=Q+P (коммут.); (P+Q)+R=P+(Q+R) (ассоциат.)*
- Если *P = (x,y),* то *P + (x,-y) = 0*. Точка *(x,-y)* является отрицательным значением точки *P* и обозначается -P. Точка -P лежит на эллиптической кривой, т.е. принадлежит $E_p\ (a,b)$.
- Если $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, то $P + Q = (x_3, y_3)$ определяется по следующим формулам:
- $x_3 = (\lambda^2 - x_1 - x_2)\ mod\ p \quad y_3 = (\lambda(x_1 - x_3) - y_1) mod\ p$

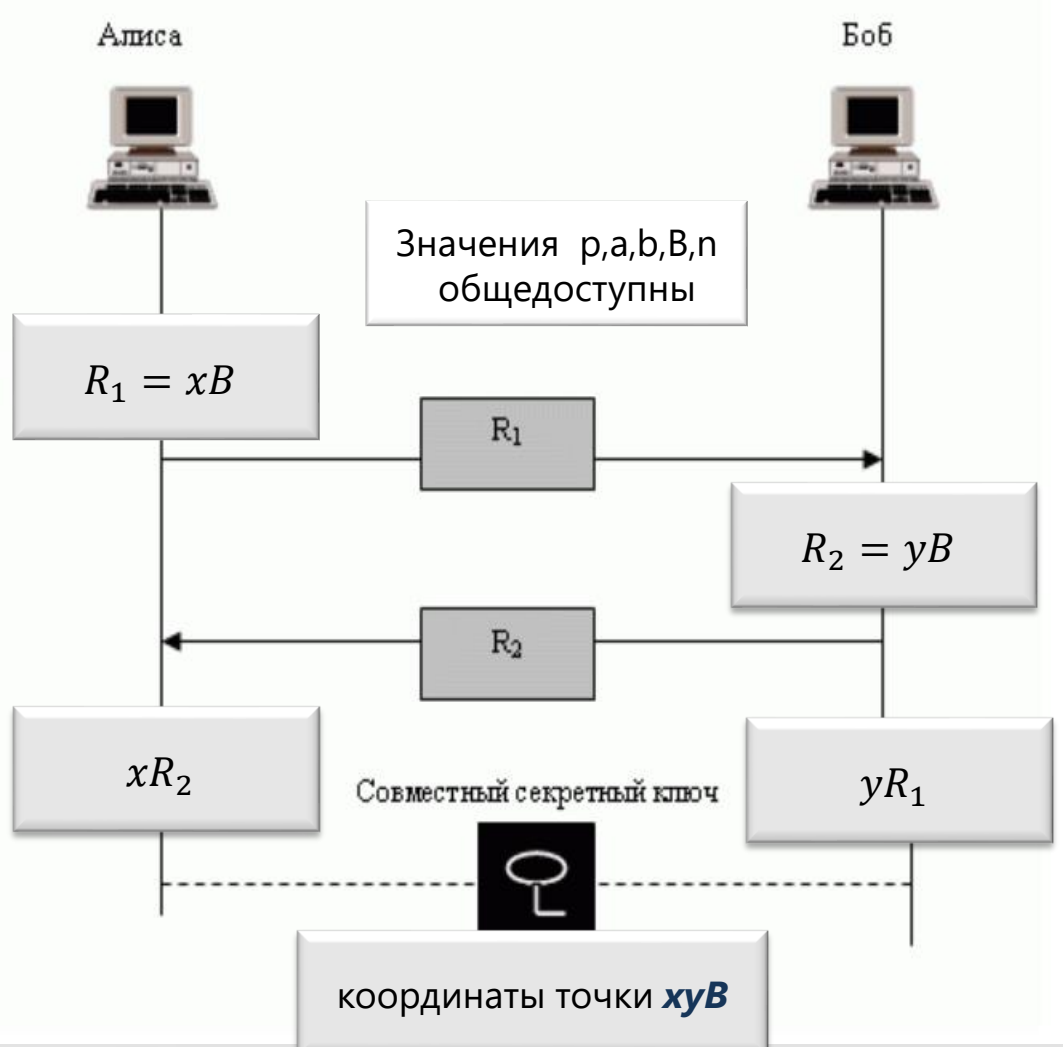
$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) mod p, & P \neq Q \\ ((3x_1^2 + a))/2y_1\ mod p, & P = Q \end{cases}$$

- λ- угловой коэффициент секущей, проведенный через точки *P* и *Q*

Задача дискретного логарифмирования на эллиптической кривой

- Даны точки P и Q на эллиптической кривой $E_p(a,b)$. Необходимо найти коэффициент $k < p$ такой, что $P = k \times Q$
- Относительно легко вычислить P по данным k и Q, но вычислительно трудно вычислить k, зная P и Q

Протокол Диффи-Хеллмана для эллиптических кривых (ECDH)

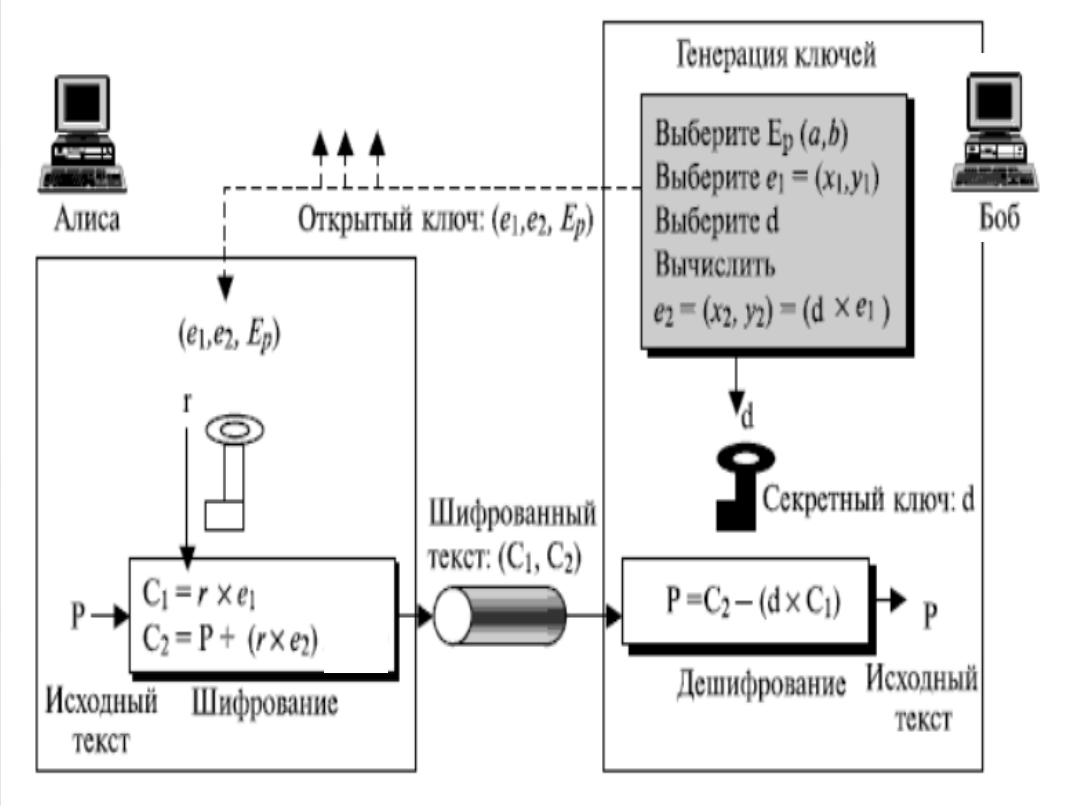


- Группа точек эллиптической кривой $E_p(a, b)$
- *B* – базовая точка (порождающий элемент) циклической подгруппы точек {kB, k=1,n} порядка n: *nB=0*
- *x, y* - большие случайные числа такие, что *0 < x < n , 0 < y < n*
- Поскольку:

$$xR_2 = x(yB) = xyB$$
$$yR_1 = y(xB) = xyB$$

- Стороны фактически создают симметричный ключ сеанса (координаты точки xyB)
- Самостоятельно «освежить» основы: https://habr.com/ru/post/335906/

Шифр Эль-Гамаля на эллиптических кривых



- Получатель выбирает кривую $E_p(a,b)$, точку e_1 на кривой, выбирает секретной число d и вычисляет еще одну точку $e_2 = d \times e_1$
- Открытый ключ $E_p(a,b), e_1, e_2$
- Отправитель сопоставляет открытому тексту точку P на кривой и создает шифровку C_1, C_2, выбрав случайное r

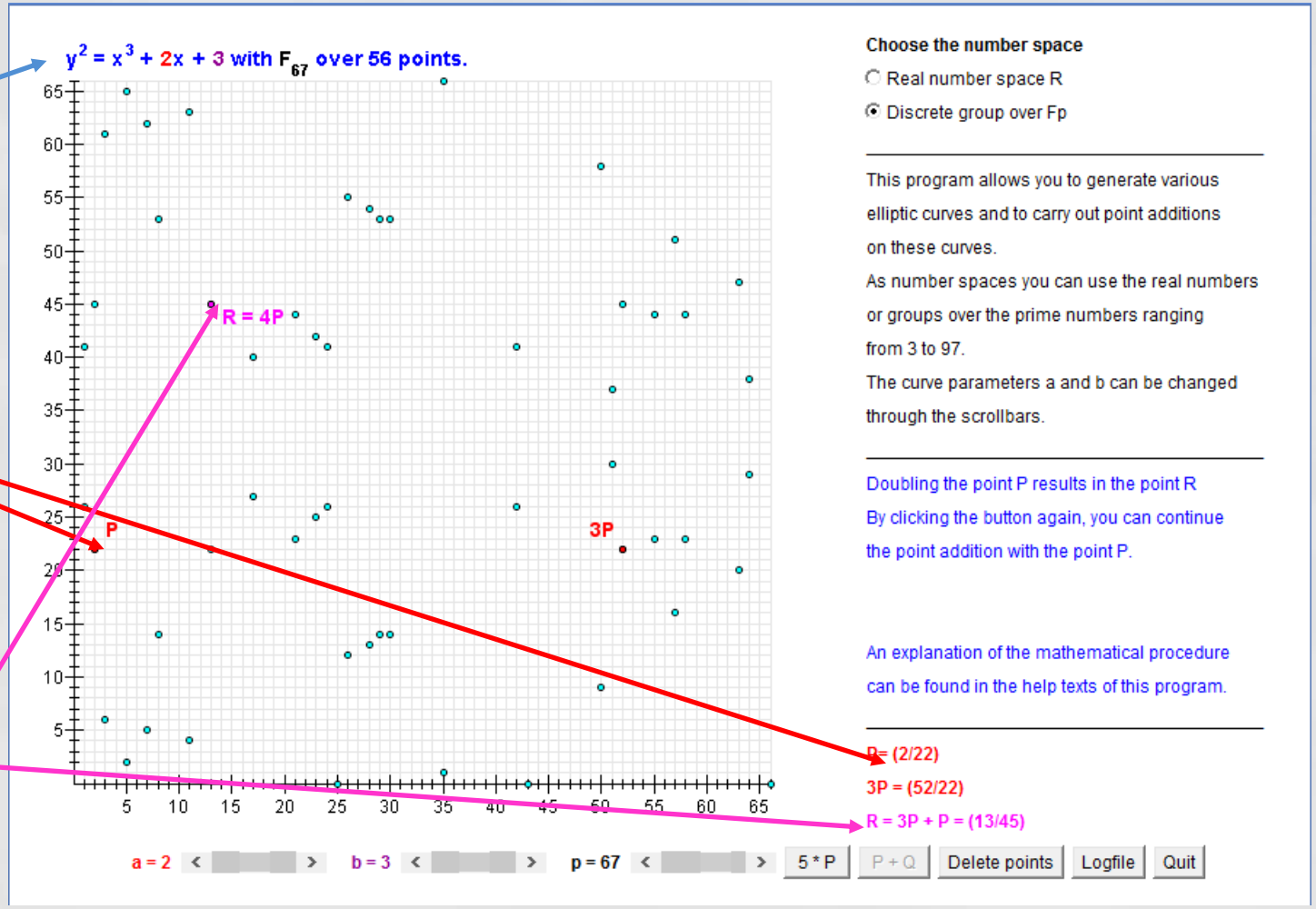
$$C_1 = r \times e_1 \quad C_2 = P + r \times e_2$$

- Получатель выполняет расшифровку:

$$C_2 - (d \times C_1) = P + r \times d \times e_1 - d \times r \times e_1 = P$$

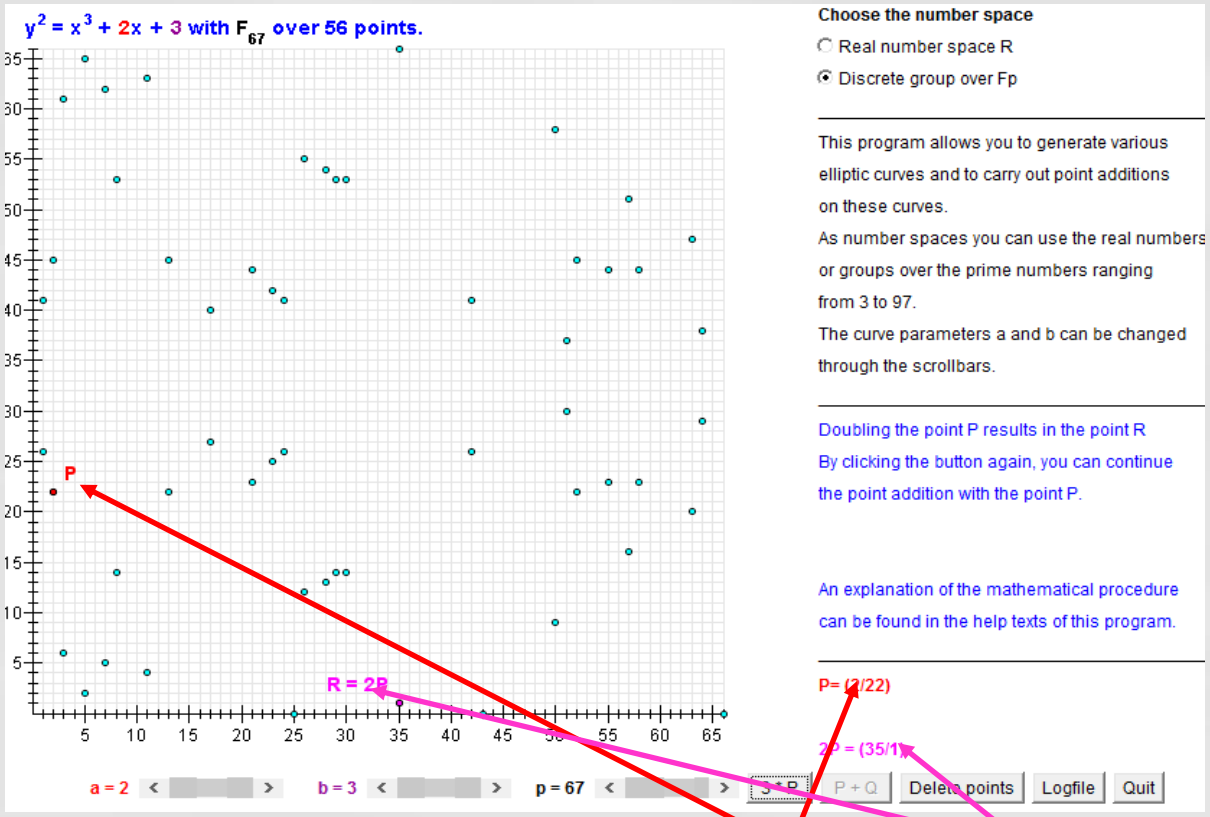
Пример генерации ключа

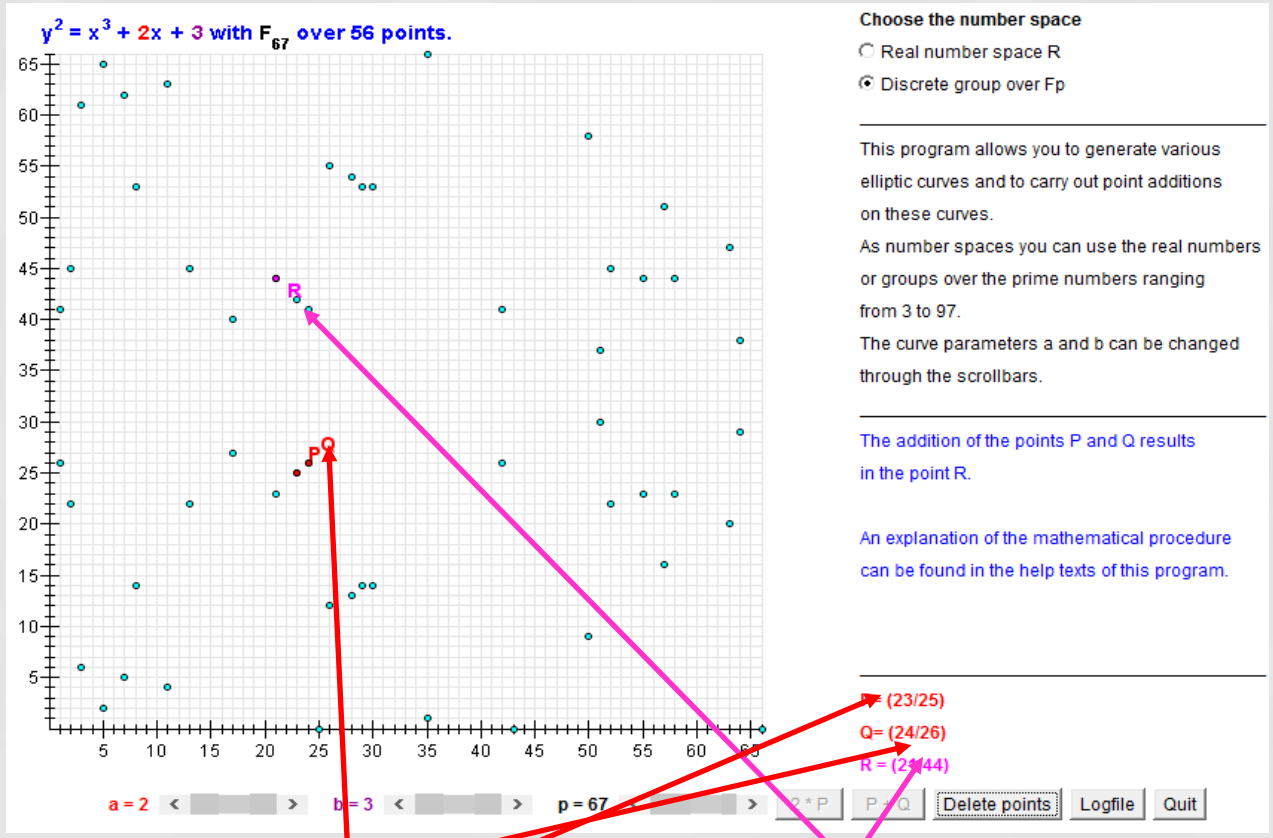
- Выбираем кривую $E_{67}(2,3)$
- Выбираем точку $e_1=(2,22)$
- Выбираем закрытый ключ d=4
- Вычисляем $e_2 = d \times e_1=4 \times (2,22)=(13,45)$



Пример зашифрования

- Текст представляется точкой P=(24,26) и выбираем случайное r=2

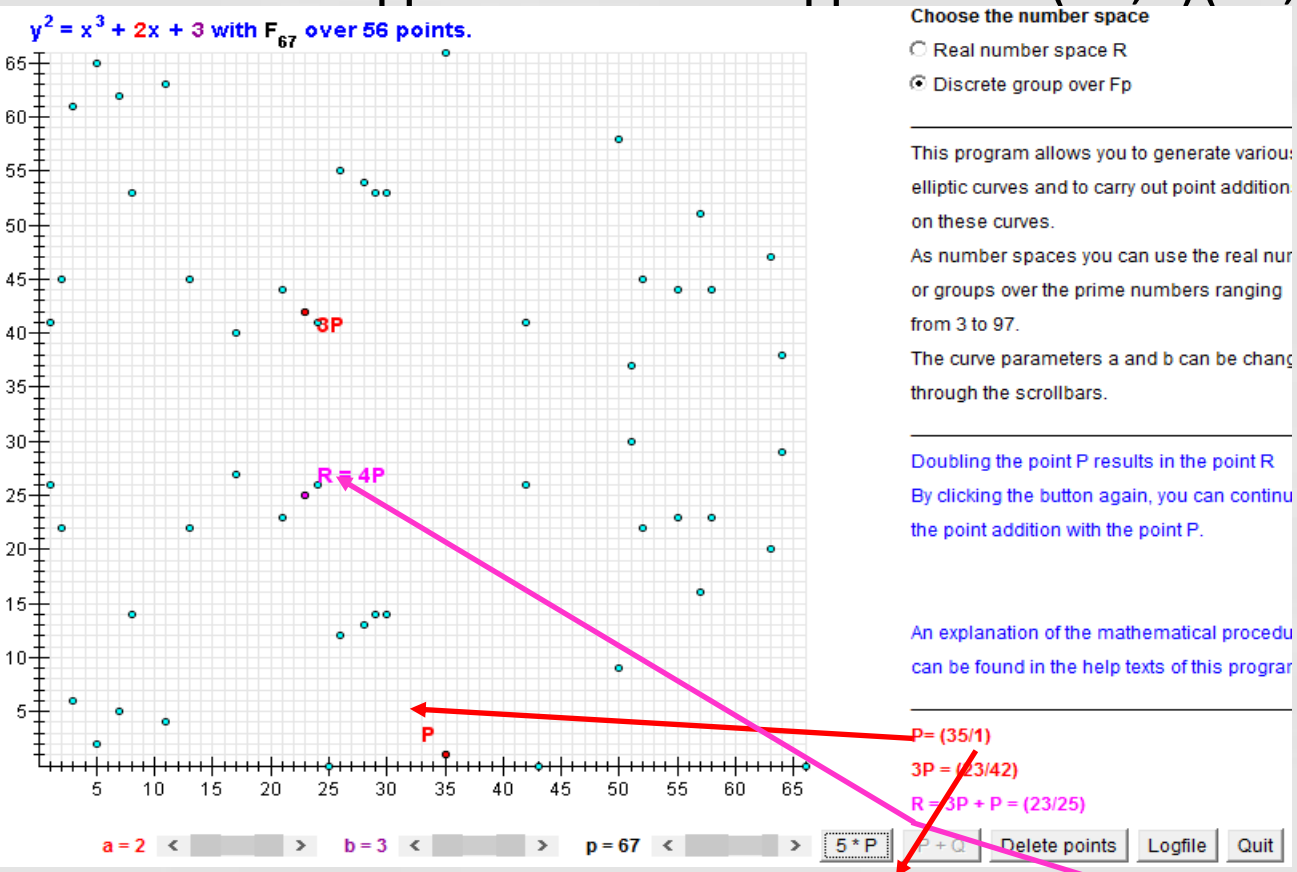


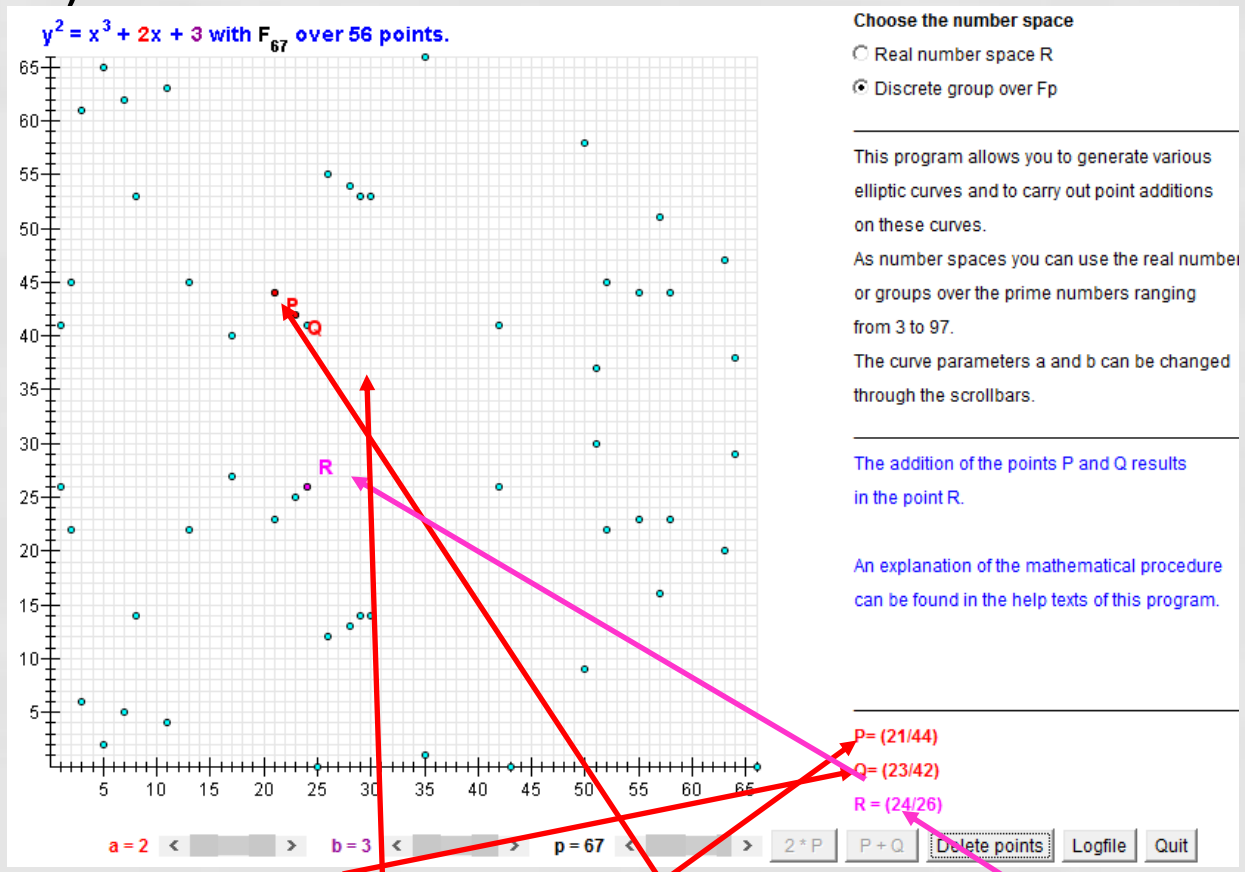


- Находим $C_1 = r \times e_1$=2 × (2,22) =(35,1) и C_2=P+r × e_2 =(24,26)+2× (13,45) = (21,44)

Пример расшифрования

- Расшифровываем шифротекст (35,1)(21,44)





- Вычисляем d × C_1 =4× (31,1) =(23,25), −(23,25)=(23, 42), $P = C_2 - d \times C_1$=(24,26)

Свойства метода с использованием эллиптической кривой

- Возведение в степень в алгоритме Эль-Гамаля заменено умножением точки на константу в модели
- Умножение в алгоритме Эль-Гамаля заменено сложением точек в модели
- Инверсия в алгоритме Эль-Гамаля — мультипликативная инверсия заменяется аддитивной инверсией точки на кривой
- Вычислительные затраты, поэтому, меньше в модели
- Для того же самого уровня безопасности (вычислительные затраты на атаки) модуль p, может быть меньшим в эллиптической системе (ECC), чем в RSA. Например, ECC с модулем, состоящим из 160 битов, может обеспечить тот же уровень безопасности, как RSA с модулем 1024 битов

Таблица сравнения размеров ключей RSA и ECC (от NIST) для получения одинакового уровня защиты

Размер ключа RSA (биты)	*Размер ключа ECC (биты)*
1024	160
2048	224
3072	256
7680	384
15360	521