# **ЛР №12 Криптография. Исследование криптографических алгоритмов на основе эллиптических кривых**

**Определение 1. Эллиптические кривые** – математический объект, который может быть определен над любым полем.

Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением

у2 = х3 + aх + b, (11.1)

при этом константы (а и b – вещественные числа) должны удовлетворять условию

4a3 + 27b2 ≠ 0. (11.2)

Формула (11.1) называется *уравнением Вейерштрасса*, а условие (11.2) исключает из рассмотрения *кривые с особыми точками* или *особые кривые.*

**Определение 3**. Частью ЭК является *бесконечно удаленная точка* (также известная как *идеальная точка*), которую мы обозначим символом *О*.

**Определение 4**. **Группа**– непустое множество с определенной на нем бинарной операцией, называемой сложением и удовлетворяющей нескольким аксиомам.

**Определение 5. Группа для ЭК** есть непустое множество, элементы которого являются точками ЭК, обладающими **следующими свойствами**:

* единичный элемент – это бесконечно удаленная точка О;
* обратная величина точки R – это точка, симметричная относительно оси Х;148 Лабораторная работа № 11
* сложение задается следующим правилом: сумма трех ненулевых точек P, Q и –R, лежащих на одной прямой, будет равна

P + Q + (–R) = О.

В соответствии с этим можем сформулировать **законы сложения точек эллиптической кривой**:

* прямая, проходящая через точки R и –R, является вертикальной прямой, которая не пересекает ЭК ни в какой третьей точке; если R = (х, –у), то R + (х, у) = О. Точка (х, у) является отрицательным значением точки R и обозначается –R. Таким образом, по определению R + (–R) = О;
* P + Q = R: пусть P и Q – две различные точки ЭК (рис. 11.1), и Р не равно Q; если проведем через P и Q прямую, то она пересечет ЭК еще только в одной точке, называемой –R; точка –R отображается относительно оси Х в точку R, равную сумме точек P и Q: P + Q = R.

Геометрическая интерпретация операции сложения двух точек показана на рис. 11.1.

Числа х и у являются рациональными, а точки P, Q, R и –R (как и любые точки ЭК) – рациональными точками.

Если Р = (х1, у1) и Q = (х2, у2), то Р + Q = (х3, у3) определяется в соответствии с правилами:

x3= λ2 – х1 – х2; (11.3)

у3= λ(х1 – х3) – у1, (11.4)

где λ = (у2 – у1)/(х2 – х1) при Р ≠ Q и λ = (3(х1)2+а)/2у1 при Р = Q. (11.5)

Из этого следует, что число λ – угловой коэффициент секущей, проведенной через точки Р = (х1, у1) и Q = (х2, у2). При Р = Q секущая превращается в касательную, чем и объясняется наличие двух формул для вычисления λ.

# **ЭК над конечными полями**

**Определение 6**. *Конечное поле* – это множество конечного числа элементов. Примером конечного поля является множество целых чисел по модулю *p*, где *p* – простое число. Поле обозначается как *GF*(*p*) или *Fp*. Здесь операции сложения и умножения работают как в модулярной арифметике.

**Определение 7**. *Эллиптическая кривая над полем Fp* задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю *р* (mod *p*):

*у*2 ≡ *х*3 + *aх* + *b* (mod *p*), (11.6)

далее для упрощения используем знак простого неравенства:

4*a*3 *+* 27*b*2 ≠ 0 (mod *p*) (11.7)

**Определение 8*.*** Если мы складываем два значения, кратных *Р*, то получаем значение, кратное *Р* (т. е. значения, кратные *Р*, замкнуты относительно операции сложения). Это означает, что *множество кратных Р значений – это* ***циклическая подгруппа***группы, образованной эллиптической кривой.

**Определение 9.** Наименьшее значение числа *q*, для которого выполняется равенство qР= *О*, называется ***порядком точки*** *Р*.

**Определение 10.** Порядок группы точек эллиптической кривой равен числу различных точек ЭК, включая точку *О*.

**Определение 11*.*** Точка *Р* называется ***генератором*** или ***базовой точкой***циклической подгруппы (такую точку во многих документах обозначают символом *G*).

***Порядок подгруппы*** *– это делитель порядка исходной группы*. Иными словами, если ЭК содержит *m* точек, а одна из подгрупп содержит *q*, то *q* является делителем *m.*

Как и в случае с непрерывными ЭК, теперь важным является вычисление некоторого числа *d*, если мы знаем *P* и *Q* для *Q = dP*. Это и есть ***задача дискретного логарифмирования* для эллиптических кривых**.

В криптографии на основе **ЭК тайный ключ** – это **случайное целое** d, выбранное из множества {1, 2, ..., q – 1}, где **q – порядок подгруппы**; **открытый ключ – это точка Q**, такая, что Q = dG, где **G – базовая точка подгруппы**.

# **Основные этапы генерации ключевой информации на основе ЭК**

***Первый этап****: выбор (генерация) ЭК*. Обычно он основан на выполнении следующих условий и операций.

* 1. Входными параметрами являются: число *l*, число *р*, удовлетворяющее условию 22*l –* 1 < *р* < 22*l*, *р* = 3 mod 4, 0 < *a* < *p*. Можно использовать некоторое простое число *р* = 22*l* – *с*, где *с* – небольшое натуральное число.
  2. Выбирается число *b* такое, что 0 < *b* < *p*. Таким образом, задана ЭК: *Ер*(*а*, *b*).
  3. Выбираются порядок *q* (простое число) и генерирующая  
     точка *G*, которая задается двумя координатами, например  
     *G =* (0, *уG*).

Второй этап: генерация ключевой информации.

* 1. Входными параметрами являются: р, а, b, q и G.
  2. Генерируется тайный ключ – число d, выбранное из множества {1, 2, …, q – 1}.
  3. Вычисляется открытый ключ – точка Q: Q = dG, (11.8). К открытому ключу также относятся р, а, b, q.

# **Использование ЭК в криптографии**

ЭК в криптографических приложениях обычно используется на этапе генерации либо согласования ключевой информации. Таким образом, можно отметить 3 направления использования ЭК в криптографии:

* в алгоритмах согласования (передачи) ключевой информации (на основе идеи Диффи – Хеллмана);
* в алгоритмах асимметричного шифрования/дешифрования сообщений;
* в алгоритмах генерации/верификации ЭЦП.

# **Реализация алгоритма Диффи – Хеллмана на основе ЭК**

Рассмотрим наиболее общий случай. Предположим, что *Eр* – это ЭК над *F*р, а *Q* – заранее определенная и согласованная сторонами **А** и **В** точка на *E*.

Отправитель **A** выбирает тайное случайное число *k*A, вычисляет точку *Р*А = *k*A*Q* и отправляет ее получателю **B**. **B** действует аналогично: он случайным образом выбирает число *k*B, вычисляет случайное число *k*A, вычисляет точку *Р*В = *k*В*Q* и отправляет результат стороне **A**.

Общий ключ *P* = *k*A*k*B*Q*. Отправитель **A** вычисляет *P* путем умножения числа *Р*В, полученного от получателя **B**, на его секретное число *k*A. Похожим образом действует другая сторона.

# **Реализация алгоритма зашифрования/расшифрования на основе ЭК**

Принимаем также во внимание, что зашифрованное сообщение *М* или каждый зашифрованный блок (*mi*) этого сообщения состоят из двух чисел. Обратимся к лабораторной работе № 8, где блок шифртекста (*ci*) в соответствии с выражениями (8.9), и (8.10) мы обозначали двумя символами *аi* и *bi* и вычисляли как  
*аi* ≡ *gk* mod *p*, *bi* ≡ (*ykmi*) mod *p*.

Поскольку символы *а* и *b* мы зарезервировали в текущей работе для обозначения параметров ЭК, то блок шифртекста сейчас будем обозначать соответственно символами *Сi*1 и *Ci*2.

При использовании ЭК зашифрование предполагает представление сообщения в виде точки *Р* (или представления каждого блока сообщения в виде разных точек *Рi*) ЭК с известной точкой *G* и известным *Q*. Соответственно шифртекст – это две точки на той же  
ЭК: *С*1 и *C*2 или *Сi*1 и *Ci*2.

Предположим, что шифруемое сообщение *М* – это точка *Р* на ЭК. Сторона **А** выбирает некоторое случайное число *k* и далее выполняет вычисления с использованием открытого ключа стороны **В**:

*С*1 = *kG*, *С*2 = *P* + *kQ*. (11.9)

Получатель для расшифрования сообщения вычисляет:

*P* = *С*2 – *dC*1. (11.10)

Знак «–» в (11.10) означает сложение с инверсией: инверсией по отношению к точке (*х*, *у*) является точка (*х*, –*у*) на ЭК.

Сравнительная оценка влияния размера ключа (в битах) для классической асимметричной системы шифрования (RSA) и асимметричной системы на основе ЭК дана американским институтом стандартов NIST, которую мы приводим ниже в виде табл. 11.5.

Таблица 11.5

**Размер ключей, обеспечивающих примерно одинаковый уровень криптостойкости**

|  |  |
| --- | --- |
| **Классический RSA** | **На основе ЭК** |
| 102 | 160 |
| 2048 | 224 |
| 3072 | 256 |
| 3680 | 384 |

# **Реализация ЭЦП на основе ЭК**

Рассмотрим генерацию и верификацию ЭЦП на основе алгоритма DSA и ЭК (EC) – ЕСDSA. Обращаем внимание на то, что используется ключевая информация отправителя (стороны **А**). Генерация ключей происходит так же, как и в последнем примере. Однако в анализируемом здесь случае во внимание должен приниматься еще один известный параметр ЭК: порядок точки *G*, т. е. число *q*.

Краткая характеристика алгоритма генерации и верификации ЭЦП состоит в следующем. Полагаем, что отправитель подписывает хеш *Н*(*М*) сообщения *М*.

**Генерация ЭЦП.**

1. Выбрать число *k* (1 < *k* < *q*), *q* – порядок точки *G*.
2. Вычислить точку *kG* = (*х*, *у*), вычислить *r* ≡ *x* mod *q*; при *r* = 0 изменить *k* и повторить шаг 2.
3. Вычислить *t* ≡ *k*–1 mod *q* (например, на основе расширенного алгоритма Евклида).
4. Вычислить *s* = (*t* (*H*(*M*) + *dr*)) mod *q*; при *s* = 0 изменить *k* и повторить алгоритм.

Стороне **В** отсылаются сообщение *М* и ЭЦП (числа *r* и *s*).

**Верификация ЭЦП.** Получатель знает алгоритм хеширования, который использовался отправителем, открытый ключ отправителя, с помощью чего выполняет следующие операции над *М* и полученной ЭЦП (обозначения чисел оставим без изменений).

1. Проверить выполнение условия: 1 < *r*, *s* < *q*; если условие не выполняется, то легитимность подписи не подтверждается, в противном случае – выполняются дальнейшие шаги.
2. Вычисляются *Н*(*М*) и *w* ≡ *s*–1 mod *q*.
3. Вычисляются *u*1 ≡ *w Н*(*М*) (mod *q*), *u*2 ≡ *wr* (mod *q*).
4. Вычисляются *Gu*1 + *Qu*2 = (*x'*, *y'*), *v* ≡ *x'* mod *q*.
5. Сравниваются *v* и *r*; если равенство выполняется, подтверждается легитимность подписи и целостность полученного сообщения.