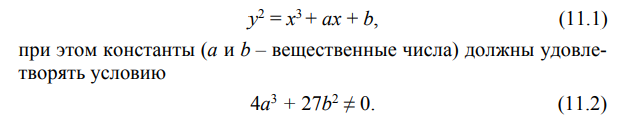
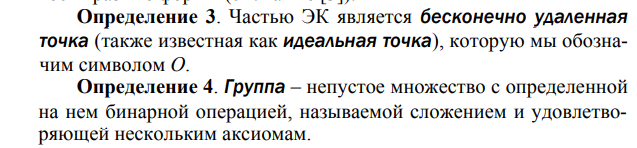
**ЭК над действительными числами**

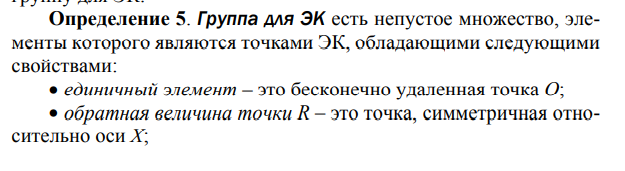
Криптография базируется на задачах факторизации, дискретного логарифмирования и операциях над точками эллиптичекой кривой.

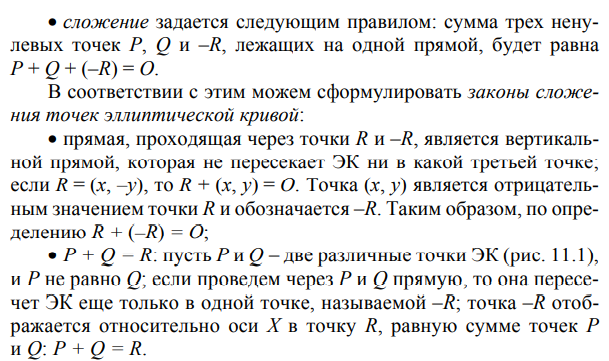
Эллиптические кривые – математический объект, который может быть определен над любым полем. Определение 2. Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением



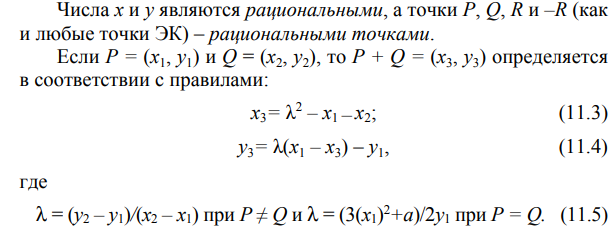
Формула (11.1) называется уравнением Вейерштрасса, а условие (11.2) исключает из рассмотрения кривые с особыми точками или особые кривые.





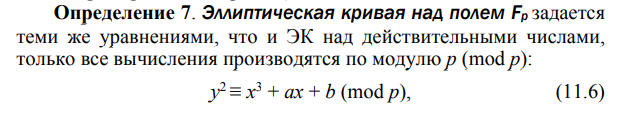


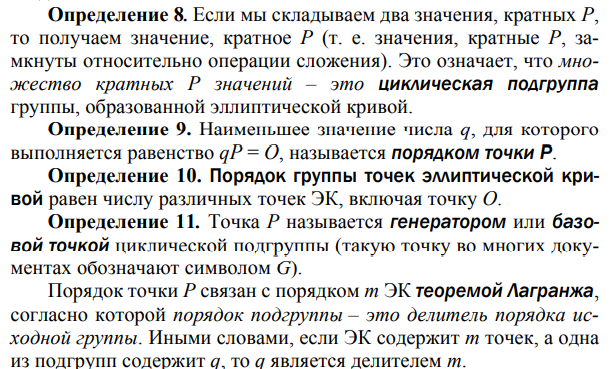
если P = Q? В этом случае мы можем говорить об операции удвоения точки: P + Р = 2Р

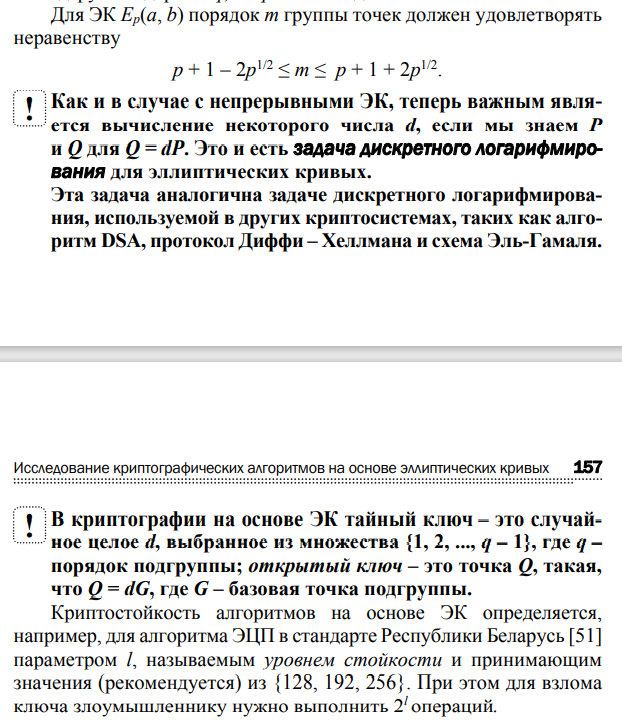
 Из этого следует, что число λ – угловой коэффициент секущей, проведенной через точки Р = (х1, у1) и Q = (х2, у2). При Р = Q секущая превращается в касательную

**ЭК над конечными полями**

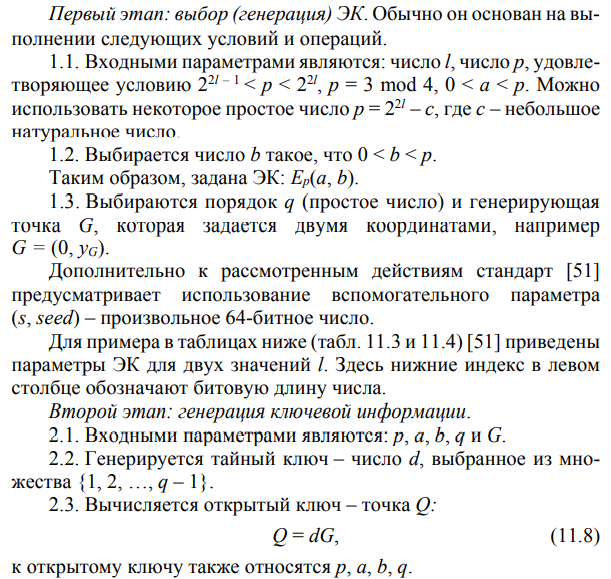
Конечное поле – это множество конечного числа элементов. Примером конечного поля является множество целых чисел по модулю p, где p – простое число.

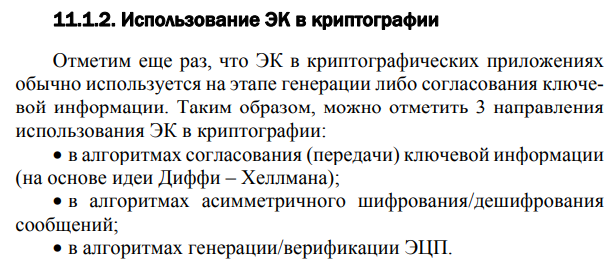


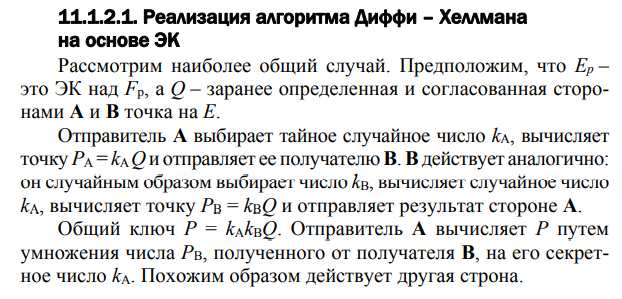




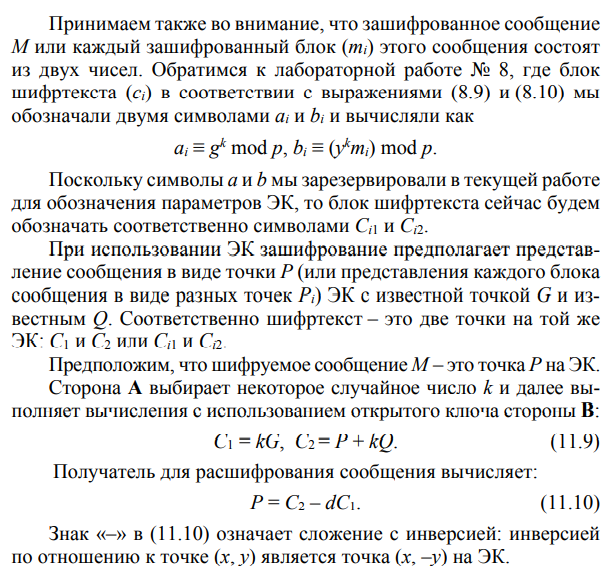
**Основные этапы генерации ключевой информациина основе ЭК**

****

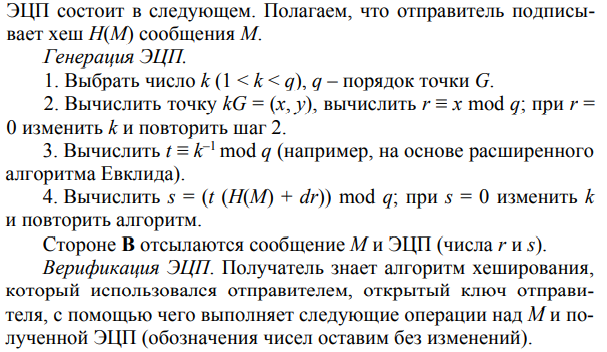
****

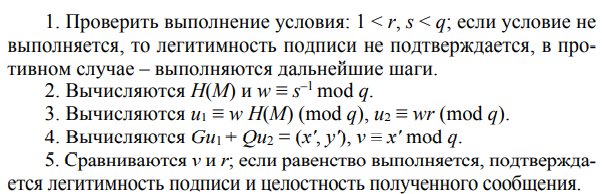
****

**Реализация алгоритма зашифрования/расшифрования на основе ЭК. На примере Эль-Гамаля**

****

Реализация ЭЦП на основе ЭК

****

****