АЛГОРИТМ РАЗДЕЛЕНИЯ СЕКРЕТА НА ОСНОВЕ «ВЫЧИТАНИЯ» ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Филимонова А.В, Бродовская В.В., Куржеевский И.В.
Научный руководитель: Куржеевский И.В.
Академия военно-морских сил имени П.С. Нахимова, Украина
E-mail: filay40@yandex.ru

Аннотация — В данной работе рассматривается алгоритм разделения секрета на основе «вычитания» точек эллиптической кривой.

1. Введение

Под протоколом понимается распределенный алгоритм с двумя и более участниками. Протокол является криптографическим, если он решает, по крайней мере, одну из трех задач криптографии: обеспечение конфиденциальности, целостности, неотслеживаемости [2]. Компонентами протокола являются участники протокола, каналы связи между участниками, а также либо алгоритмы, используемые участниками, либо постановка той задачи, которую протокол призван решать.

2. Основная часть

Протокол разделения секрета состоит из двух основных фаз [1, 2].

1) На фазе раздачи, или разделения, секрета дилер, знающий секрет m, генерирует n долей секрета m_1, m_2, … , m_n и посылает долю m_i участнику P_i (I = 1,…, n) по защищенному каналу связи. Раздача должна быть организована таким образом, чтобы разрешенные группы участников, собравшись вместе, могли однозначно восстановить секрет m, а неразрешенные — не могли.

2) На фазе восстановления секрета какая–либо группа из структуры доступа Γ объединяет свои доли секретов m_i (I = 1,…, n) так, чтобы получить секрет m.

(n, k) — пороговой схемой разделения секрета ($k \leq n$) называется такая схема, в которой секрет разделяется между n участниками, причем разрешенной группой является любая группа, насчитывающая не менее k абонентов.

Рассмотрим пример алгоритма разделения секрета на основе "вычитания" точек эллиптической кривой: Пусть эллиптическая кривая имеет вид [1] $y^2 = x^3 + ax + b$, где a=7,

b=433088765467672769057659045956550931995942111794451039583252968842033849580 41;

p — модуль по которому будут проводится вычисления;

p=578960446186580977117854925043439539266349923328202820197287920039565648210 41.

Пусть m — секрет, который необходимо разделить между пятью сторонами

m=(5381337063821432292019407594738484912813853791835111752199981649881965971263 8,50212836908552842917956466305265722324317888843255976174930387657138066242683);

Выбираем случайные доли секрета:

m_1=(1264278820474601992557445143886006574951185051114308439798072660843802368 4166,2338213770949474774095119630947317816738002536677003338103679812427449083 4001);

m_2=(2494174060358022463522698029549610543255680239786732000263712914963070716 2397,3623586857320185527749508235474201077223549416186599333315243417736147844 4320);

m_3=(2669906106198297150990724799890955927914010612680054331336087310261563802 3237,4743808261137539816494413732323376991544190031541071678320863322332184268 6969);

m_4=(3509307698426914600331288828913644924720237909308611844992719409833179579 2758,8955608851954140424591189731199887433012090517003297091897186515617904451200);

Пятую долю m_5 авторы рассчитывают с помощью разработанного ими алгоритма «вычитания» точек эллиптической, не имеющего аналога в сети Интернет: $m_5 = m - m_1 - m_2 - m_3 - m_4$;

m_5=(1633310661770965843871883328325001452071222486108975966261595783400250716 67,3084368834763721544893275208237694132560166736019773135768205757362971044288 5).

Для восстановления секрета необходимо сложить доли секрета, представляющие собой координаты точек ЭК, используя алгоритм сложения точек на эллиптической кривой: $m = m_1+m_2+m_3+m_4+ m_5$.

m=(5381337063821432292019407594738484912813853791835111752199981649881965971263 8,5021283690855284291795646630526572232431788884325597617493038765713806624268 3).

3. Заключение

Описанная схема является совершенной и идеальной. Совершенность следует из того, что, объединив менее чем n долей секрета, участники вычислят случайное число, которое не дает никакой информации о секрете. Идеальность очевидна, поскольку каждый участник получает долю секрета, размер которой равен размеру самого секрета. Данный алгоритм был реализован в среде *Aribasw* и *C#* (*SHARP*), успешно прошел тестирование на правильность результатов разделения и восстановления секрета и может быть использован для защиты информации от несанкционированного доступа.

4. Список литературы

[1] ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписью. — Взамен ГОСТ Р 34.10-94; введ. 2002-07-01. — М.: Изд-во стандартов, 2002. — 16 с.

[2] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер. — М.: Триумф, 2003. — 816 с.

ALGORITHM SECRET SHARING BASED ON THE "SUBTRACTION" OF THE ELLIPTIC CURVE

Filimonova A. V., Kurzheievskyi I. V.
Scientific adviser: Kurzheievskyi I. V.
Naval Academy named after P.S. Nakhimov, Ukraine

Abstract — This paper describes an algorithm based on a secret sharing "subtraction" of the elliptic curve.