КРИПТОГРАФИЯ АЛГЕБРАИЧЕСКИХ КРИВЫХ В ПРОТОКОЛЕ АУТЕНТИФИКАЦИИ СУБЪЕКТА ПО СХЕМЕ «ЗАПРОС-ОТВЕТ»

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Панькова В. В.

Саломатин С. Б. – к.т.н., доцент

Одной из основных составляющих систем безопасности является аутентификация пользователя: подтверждение личности отправителя или получателя информации. Задача надёжной аутентификации пользователей, т.е. подтверждение соответствия удалённого субъекта тому, за кого он себя выдаёт, решается средствами криптографии.

Действительно защищённой от перехвата при прослушивании является схема «запрос-ответ», вследствие невозможности извлечения информации о пароле в открытом виде из-за необратимости применённого криптографического преобразования.

По методу схемы «запрос-ответ» верификатор генерирует случайное или псевдослучайное число, отвечающее только одному требованию – уникальности, т.е. неповторяемости с течением времени, и высылает его претенденту. Претендент производит какое-либо однонаправленное криптографическое преобразование (блочное шифрование или хэширование) над парольной фразой и присланным запросом и высылает результат верификатору. Верификатор производит независимо от клиента такие же преобразования и сверяет получившийся у него результат с присланным ответом претендента.

Алгебраические кривые в средствах криптографии повышают стойкость и предоставляют дополнительный параметр маскировки – вида кривой. В общем случае алгебраическая кривая над конечным полем $GF(q)$ определяется множеством точек $P(x, y, z)$, чьи координаты x, y и z являются элементами поля, и задаётся многочленом, например, $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3$, коэффициенты которого $a_i \in GF(q)$ задают вид кривой. Алгебраические кривые, стойкие по отношению к методу логарифмирования, могут быть использованы для целей аутентификации по схеме «запрос-ответ». Такую схему использует криптографический протокол аутентификации субъекта на основе метода доказательства с нулевым разглашением знаний.

В процессе аутентификации участвуют претендент, верификатор и доверенная сторона, например центр управления и распределения ключей. Предполагается, что каждому претенденту присвоен уникальный идентификационный номер I_A.

Первый этап включает задание системных параметров. Центр управления и распределения ключей определяет кривую и точку P на ней, которая после q - кратного сложения с самой собой образует «нулевую» точку кривой. Секретным ключом претендента является сгенерированное случайным образом число d, а открытым ключом точка Q, определяемая как произведение $Q = d \cdot P$. Идентификационный номер I_A и открытый ключ Q претендента сохраняются в базе данных верификатора.

На этапе информационного обмена претендент доказывает верификатору свою идентичность: верификатор выбирает случайным образом число h и передаёт его претенденту. Претендент генерирует своё случайное число k, $0 < k < q$. Вычисляет x-координату точки, т.е. $r = k \cdot P$, вычисляет y-координату точки, т.е. $s = (r \cdot d + k \cdot h) \bmod q$, и передаёт верификатору точку (r, s).

Этап проверки знаний претендента: верификатор принимает точку с координатами (r, s) и производит вычисления: $Z_1 = (s \cdot (h^{-1})) \bmod q$, $Z_2 = ((-r) \cdot (h^{-1})) \bmod q$, $R = (Z_1 \cdot P + Z_2 \cdot Q)$.

В заключение верификатор проверяет равенство $r = R$. Если оно верно – принимается решение о том, что претендент доказал свои знания и раунд аутентификации завершён успешно, иначе - решение об отсутствии у претендента требуемых знаний.

Таким образом, средства криптографической защиты с использованием алгебраических кривых преобразуют информацию с помощью обратимого математического алгоритма, а стойкость криптографической системы определяется используемыми алгоритмами и степенью секретности ключа. Криптографический протокол аутентификации по схеме «запрос-ответ» позволяет реализовать простые программно-аппаратные комплексы, способные аутентифицировать своего владельца без раскрытия информации о записанном секретном ключе. Это означает, что в случае перехвата данных, риску подвергается не сам ключ, а только данные сеанса, которые нельзя использовать повторно, так как при каждом новом раунде аутентификации верификатор генерирует новое случайное число.

Список использованных источников:

1. Конеев, И.Р, Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.
2. Саломатин, С. Б. Методические указания к лабораторной работе Криптографические протоколы. – Минск: БГУИР, 2002. – 22 с.