АЛГОРИТМ ЦИФРОВОЙ ИНФОРМАЦИОННОЙ ПОДПИСИ ЭЛЬ ГАМАЛЯ (EGSA), КАК МЕТОД ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

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

Воронов И. К.

Мельниченко Д. А. – канд. техн. наук, доцент

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Алгоритм Эль-Гамаля может использоваться для формирования электронной подписи или для шифрования данных.

Название EGSA происходит от слов El Gamal Signature Algorithm (алгоритм цифровой подписи Эль Гамаля). Идея EGSA основана на том, что для обоснования практической невозможности фальсификации цифровой подписи может быть использована более сложная вычислительная задача, чем разложение на множители большого целого числа,- задача дискретного логарифмирования. Кроме того, Эль Гамалю удалось избежать явной слабости алгоритма цифровой подписи RSA, связанной с возможностью подделки цифровой подписи под некоторыми сообщениями без определения секретного ключа.

Рассмотрим подробнее алгоритм цифровой подписи Эль Гамаля. Для того чтобы генерировать пару ключей (открытый ключ - секретный ключ), сначала выбирают некоторое большое простое целое число P и большое целое число G, причем $G < P$. Отправитель и получатель подписанного документа используют при вычислениях одинаковые большие целые числа P (~10308 или ~21024) и G (~10154 или ~2512), которые не являются секретными.

Отправитель выбирает случайное целое число *X, 1 < X £ (P -1),* и вычисляет

$$Y = GX \bmod P.$$

Число Y является открытым ключом, используемым для проверки подписи отправителя. Число Y открыто передается всем потенциальным получателям документов.

Число X является секретным ключом отправителя для подписывания документов и должно храниться в секрете.

Для того чтобы подписать сообщение *M*, сначала отправитель хэширует его с помощью хэш-функции h() в целое число m:

$$m = h(M),\ 1<m<(P-1),$$

и генерирует случайное целое число K, $1 < K < (P-1)$, такое, что *K* и *(P-1)* являются взаимно простыми. Затем отправитель вычисляет целое число *a:*

$$a = GK \bmod P$$

и, применяя расширенный алгоритм Евклида, вычисляет с помощью секретного ключа X целое число b из уравнения

$$m = X * a + K * b \ (\bmod (P-1)).$$

Пара чисел *(a,b)* образует цифровую подпись *S*:

S = (a, b), проставляемую под документом *M.*

Тройка чисел (*M, a, b)* передается получателю, в то время как пара чисел (X, K) держится в секрете. После приема подписанного сообщения *(M, a, b)* получатель должен проверить, соответствует ли подпись S = *(a, b)* сообщению M. Для этого получатель сначала вычисляет по принятому сообщению M число *m = h(M),* т.е. хэширует принятое сообщение M. Затем получатель вычисляет значение *A = Ya ab (mod P)* и признает сообщние M подлинным, если, и только если *A = Gm (mod P).* Иначе говоря, получатель проверяет справедливость соотношения

$$Ya\ ab \ (\bmod P) = Gm \ (\bmod P).$$

Можно строго математически доказать, что последнее равенство будет выполняться тогда, и только тогда, когда подпись *S=(a, b)* под документом M получена с помощью именно того секретного ключа *X*, из которого был получен открытый ключ *Y*. Таким образом, можно надежно удостовериться, что отправителем сообщения M был обладатель именно данного секретного ключа *X*, не раскрывая при этом сам ключ, и что отправитель подписал именно этот конкретный документ *M*.

Таким образом алгоритм Эль Гамаля обеспечивает достаточную степень шифрования. Однако выполнение каждой подписи требует нового значения *K,* причем это значение должно выбираться случайным образом. Если нарушитель раскроет когда-либо значение *K*, повторно используемое отправителем, то он сможет раскрыть секретный ключ *X* отправителя. Основное назначение алгоритма - подписание любого электронного документа или идентификация удаленных пользователей.

Список использованных источников:

1. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А Тимофеев, В.Ф Шаньгин – Москва, 2001. – 376 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер – Москва, 2002 – 816 с.