АЛГОРИТМ ФОРМИРОВАНИЯ СЕКРЕТНЫХ КЛЮЧЕЙ ДЛЯ ГРУППЫ ПОЛЬЗОВАТЕЛЕЙ

Радчук Ю.С., Ипанов А. В., Куржеевский И.В.
Научный руководитель: Куржеевский И.В.
Академия военно-морских сил имени П.С. Нахимова, Украина
Севастопольский национальный технический университет, Украина
E-mail: kurg_igor@mail.ru

Аннотация — В работе рассмотрен алгоритм формирования секрета для группы пользователей.

1. Введение

Одним из первых и самых распространенных протоколов открытого распределения ключей является протокол Диффи-Хеллмана, который предназначен для формирования общего секрета между группой пользователей, обменивающимися конфиденциальной информацией по открытому каналу с использованием открытых и секретных ключей [1].

2. Основная часть

Открытое распределение ключей на сегодняшний день — это наиболее перспективный способ управления ключами, используемый практически во всех системах защиты информации. Он заключается в том, что пользователи независимо генерируют секретные ключи, на их основе вырабатывают так называемые открытые ключи, которыми обмениваются. Далее каждый из абонентов сети на основе своего секретного и открытого ключа партнера вырабатывает ключ, с помощью которого сообщение для отправки. Получатель на основе теперь уже своего секретного и открытого ключа отправителя изготавливает ключ, с помощью которого расшифровывает документ. Таким образом, сообщение недоступно посторонним.

Рассмотрим случай формирования общего секрета для трех пользователей *A, B* и *C*. Формируется общий открытый ключ Y для трех пользователей

$$Y = Y_A Y_B Y_C = a^{x_A + x_B + x_C} \bmod p .$$

Пользователь *A* посылает пользователям *B* и *C* число

$$Z_A = Y^{x_A} = a^{(x_A + x_B + x_C)x_A} \bmod p .$$

Пользователь *B* отправляет пользователю *C* числа

$$Z_B = Y^{x_B} = a^{(x_A + x_B + x_C)x_B} \bmod p ;$$

$$Z_{AB} = Z_A{}^{x_A} = a^{(x_A + x_B + x_C)x_B x_A} \bmod p .$$

Пользователь *C* посылает пользователю *A* число

$$Z_{BC} = Z_B{}^{x_C} = a^{(x_A + x_B + x_C)x_C x_B} \bmod p ,$$

и пользователю *B* число

$$Z_{AC} = Z_A{}^{x_C} = a^{(x_A + x_B + x_C)x_C x_A} \bmod p .$$

После этого пользователи *A, B* и *C* вычисляют общий секретный ключ:

$$Z_{ABC} = Z_{BC}{}^{x_A} = a^{(x_A + x_B + x_C)x_A x_B x_C} \bmod p;$$

$$Z_{ABC} = Z_{AC}{}^{x_B} = a^{(x_A + x_B + x_C)x_A x_B x_C} \bmod p;$$

$$Z_{ABC} = Z_{AB}{}^{x_C} = a^{(x_A + x_B + x_C)x_A x_B x_C} \bmod p. \quad [3]$$

Этот алгоритм имеет один недостаток. Формирование общего секрета для трех пользователей требует раскрытия общего секрета для двух пользователей третьему, например, пользователю *A* предоставляется число $Y_{BC} = Y_C{}^{x_B} \bmod p$, которое является общим секретом для пользователей *B* и *C*. Авторы А.А. Молдавян, Н.А. Молдавян предлагают такой алгоритм: пользователь *A* посылает пользователю *B* и *C* число $Z_A = Y^{x_A} \bmod p$. Пользователь *B* отправляет пользователю *C* числа $Z_B = Y^{x_B} \bmod p$ и $Z_{AB} = Z_A{}^{x_B} \bmod p$. Но это решение имеет недостаток, так как пользователь С знает общий секрет пользователей *A* и *B* [3].

Этот недостаток можно устранить, если каждая пара пользователей будет общаться между собой, используя сформированный ключ по другому модулю. Для каждого сеанса связи, согласно алгоритму Нидхема-Шредера, авторы предлагают вычислять сеансовое значение модуля [2]. Например, пара пользователей *A* и *B* договариваются на n сеансов связи. Две стороны создают n модулей, последовательно хешируя общее для них число n раз

$$h_1 = H(m), h_2 = H(h_1), h_n = H(h_{n-1}) .$$

В качестве модулей при передачи сообщений будут применять эти вычисленные значения в обратном порядке.

3. Заключение

Рассмотренный алгоритм позволяет создать общий секретный ключ как для группы из трех пользователей, обменивающимися конфиденциальной информацией, так и для каждой пары из этой группы так, что секретный ключ каждой пары не будет известен третьему пользователю.

4. Список литературы

[1] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер. — М.: Триумф, 2003. — 816 с.
[2] Needham R.M. Using encryption for authentication in large networks of computers / R.M. Needham, M.D. Schroeder // Commun. ACM. — 1978. — Т. 21, № 12. — С. 993 — 999.
[3] Молдавян А.А. Введение в криптосистемы с открытым ключом / А.А. Молдавян, Н.А. Молдавян. — СПб.: БХВ-Петербург, 2005. — 288с.

THE GENERATION ALGORITHM OF THE SECRET KEYS FOR THE USERS GROUP

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

Abstract — The algorithm of the generation of the secret keys for the users group is considered.