Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Зюзин В.В., Коробов А.В., Васильев А.О. Алгоритм Шамира // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2020. – №7 (июль). – АРТ 90-эл. – 0,2 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.056.5

Зюзин Владислав Дмитриевич
магистрант 1-ого курса,
факультет «Сети и системы связи»
МТУСИ
г. Москва, Российская Федерация
Коробов Александр Владимирович
магистрант 1-ого курса,
факультет «Сети и системы связи»
МТУСИ
г. Москва, Российская Федерация
Васильев Антон Олегович
магистрант 1-ого курса,
факультет «Сети и системы связи»
МТУСИ
г. Москва, Российская Федерация
v.d.zyuzin@gmail.com

АЛГОРИТМ ШАМИРА

Аннотация: В данной статье приводится полное описание алгоритма Шамира, пример работы на реальных числах, а также его иллюстрация его на структурной схеме.

Ключевые слова: Абонент, число, сообщение, символ.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Zyuzin Vladislav Dmitrievich
1-st year master student,
features «Networs and communication systems»
MTUCI
Moscow, Russian Federation
Korobov Alexander Vladimirovich
1-st year master student,
features «Networs and communication systems»
MTUCI
Moscow, Russian Federation
Vasilyev Anton Olegovich
1-st year master student,
features «Networs and communication systems»
MTUCI
Moscow, Russian Federation

SHAMIR'S ALGORITHM

Abstract: This article provides a full description of the Shamir algorithm, an example of how it works on real numbers, and an illustration of it on a block diagram.

Keywords: Subscriber, number, message, symbol.

Алгоритм Шамира – это первый алгоритм, позволяющий организовывать обмен секретными сообщениями по открытой линии связи для абонентов, не имеющим защищённых каналов связи и секретных ключей.

Существуют два Абонента А и Б.

При отправке сообщения от Абонента А к Абоненту Б, первый генерирует случайное простое число p (которое передаёт Абоненту Б) и вычисляет числа c_A и d_A так, чтобы удовлетворяло следующему условию:

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

$$c_A d_A \bmod (p-1) = 1 \quad (1)$$

где c_A - открытое число Абонента А;

d_A - закрытое число Абонента А;

p - случайное простое число.

Число d - это инверсия открытого числа c по модулю $p-1$, то есть:

$$cd \bmod p = 1 \text{ или } c^{-1} \bmod p = 1 \quad (2)$$

При этом $d < p$, а числа c и p взаимно простые.

Затем Абонент Б вычисляет числа $c_Б$ и $d_Б$ так, чтобы удовлетворяло следующему условию:

$$c_Б d_Б \bmod (p-1) = 1 \quad (3)$$

где $c_Б$ - открытое число Абонента А;

$d_Б$ - закрытое число Абонента А;

p - случайное простое число.

Когда оба Абонента вычислили свои секретные ключи, Абонента А приступает к трехэтапному протоколу шифрования:

1) С помощью своего открытого числа c_A, вычисляет $x1_A$ по формуле:

$$\begin{aligned} &1x_{A,i} = m_{A,i}{}^{c_A} \bmod p \\ &i = 1, 2, 3, \ldots, N \end{aligned} \quad (4)$$

где $1x_{A,i}$ - зашифрованный символ сообщения Абонента А (1-ый этап);

$m_{A,i}$ - символ исходного сообщения Абонента А;

c_A - открытое число Абонента А;

p - случайное простое число;

N - количество символов сообщения.

Затем Абонент А передаёт Абоненту Б по открытой линии связи зашифрованное сообщение $x1_A$.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

2) Абонент Б, получив $x1_A$ с помощью своего открытого числа $c_Б$ вычисляет $x2_A$ по формуле:

$$x2_{A,i} = x1_{A,i}^{\,c_Б} \bmod p \quad i = 1, 2, 3, \ldots, N \tag{5}$$

где $x2_{A,i}$ - зашифрованный символ сообщения Абонента А (2-ой этап);

$x1_{A,i}$ - зашифрованный символ сообщения Абонента А (1-ый этап);

$c_Б$ - открытое число Абонента Б;

p - случайное простое число;

N - количество символов сообщения.

Затем Абонент Б передаёт Абоненту А по открытой линии связи зашифрованное сообщение $x2_A$.

3) Абонент А, получив $x2_A$ с помощью своего закрытого числа d_A вычисляет $x3_A$ по формуле:

$$x3_{A,i} = x2_{A,i}^{\,d_A} \bmod p \quad i = 1, 2, 3, \ldots, N \tag{6}$$

где $x3_{A,i}$ - зашифрованный символ сообщения Абонента А (3-ий этап);

$x2_{A,i}$ - зашифрованный символ сообщения Абонента А (2-ой этап);

d_A - закрытое число Абонента А;

p - случайное простое число;

N - количество символов сообщения.

Затем Абонент А передаёт Абоненту Б по открытой линии связи зашифрованное сообщение $x3_A$.

4) Абонент Б, получив $x3_A$ с помощью своего закрытого числа $d_Б$ вычисляет $x4_A$ или дешифрует зашифрованное сообщение по формуле:

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

$$x4_{A,i} = x3_{A,i}^{\,d_Б} \bmod p \quad (8)$$
$$i = 1, 2, 3, \ldots, N$$

где $x4_{A,i}$ или $m'_{A,i}$ - дешифрованное сообщение Абонента А;

$x3_{A,i}$ - зашифрованный символ сообщения Абонента А (3-ий этап);

$d_Б$ - закрытое число Абонента А;

p - случайное простое число;

N - количество символов сообщения.

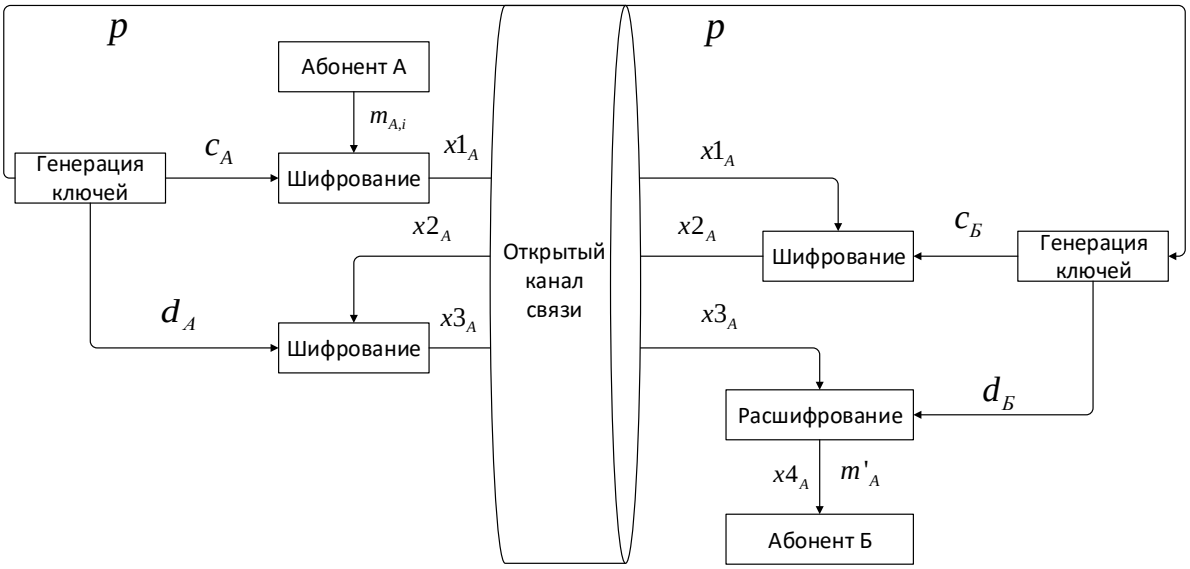

Рисунок 1. Структурная схема алгоритма Шамира

Пример:

Исходное число $m_A = 10$.

Шаг 1. Генерация случайного простого числа p.

Абонент А генерирует случайное простое число $p = 47$, которое передаёт Абоненту Б.

Шаг 2. Формирование Абонентами чисел c и d.

Абоненты формируют числа c и d, согласно условию

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

$cd \bmod(47-1)=1$

$cd \bmod 46=1$

1) Например, Абонент А сформировал число $c_A=11$, тогда d_A будет равно 21.

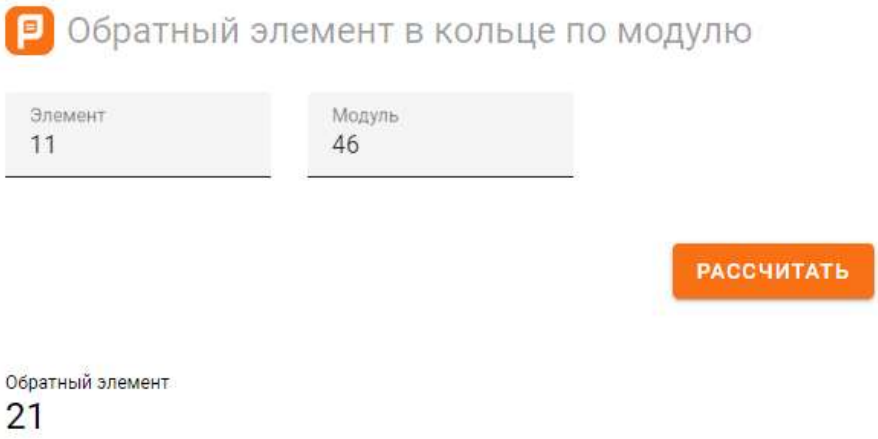

Рисунок 2. Расчёт обратного элемента числа $c_A=11$

2) Например, Абонент Б сформировал число $c_Б=7$, тогда d_A будет равно 33.

Рисунок 3. Расчёт обратного элемента числа $c_Б=7$

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Шаг 3. Шифрование сообщения.

1) Абонент А шифрует своё сообщение $m_A = 10$ своим открытым числом $c_A = 11$:

$$1x_A = 10^{11} \bmod 47 = 22$$

Число $1x_A = 22$ передаёт Абоненту Б.

2) Абонент Б, приняв число $1x_A = 22$, шифрует его своим открытым число $c_Б = 7$:

$$2x_A = 22^7 \bmod 47 = 20$$

Число $2x_A = 20$ передаёт Абоненту А.

3) Абонент А, приняв число $2x_A = 20$, шифрует его своим закрытым числом $d_A = 21$:

$$3x_A = 20^{21} \bmod 47 = 45$$

Число $3x_A = 45$ передаёт Абоненту Б.

Шаг 4. Дешифрование сообщения.

Абонент Б, приняв число $3x_A = 45$, дешифрует его своим закрытым число $d_Б = 33$:

$$4x_A = 45^{33} \bmod 47 = 10$$

Итак, число $4x_A = m_A' = m_A = 10$

Приведём таблицу для данного примера:

Таблица 1. Таблица параметров

m_A	c_A	d_A	$c_Б$	$d_Б$	$1x_A$	$2x_A$	$3x_A$	$4x_A$
10	11	21	7	33	22	20	45	10

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Алгоритм Шамира также можно использовать и на несколько абонентов, но главным недостатком алгоритма считается необходимость многоступенчатого обмена сообщениями, поэтому он не используется повсеместно.

Список использованной литературы:

1. Санников В. Г. Введение в теорию и методы криптографической защиты информации: Учебное пособие. – М.: МТУСИ, 2009.
2. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации: Учебное пособие. М.: Горячая линия – Телеком, 2005.
3. Шифр Шамира // ВикипедиЯ URL: https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%A8%D0%B0%D0%BC%D0%B8%D1%80%D0%B0 (дата обращения: 15.06.2020).

Дата поступления в редакцию: 01.07.2020 г.
Опубликовано: 07.07.2020 г.