МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__» _____ 2017г.

АЛГОРИТМ ШИФРОВАНИЯ ДЕФФИ-ХЕЛЛМАНА

Методические указания по выполнению практических работ по дисциплине «информационная безопасность»

Курск2017

ПРАКТИЧЕСКАЯ РАБОТА №5 «АЛГОРИТМ ШИФРОВАНИЯ ДЕФФИ-ХЕЛЛМАНА»

Цель работы: получение навыков создания зашифрованного сообщения при помощи алгоритма шифрования Деффи – Хеллмана.

Теоретическая часть

Схема Эль-Гамаля (Elgamal) — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамаля лежит в основе бывших стандартов электронной цифровой подписи в США(DSA) и России (ГОСТ Р 34.10-94).

Схема была предложена Тахером Эль-Гамалем в 1985 году. Эль-Гамаль разработал один из вариантов алгоритма Диффи-Хеллмана. Он усовершенствовал систему Диффи-Хеллмана и получил два алгоритма, которые использовались для шифрования и для обеспечения аутентификации. В отличие от RSA алгоритм Эль-Гамаля не был запатентован и, поэтому, стал более дешевой альтернативой, так как не требовалась оплата взносов за лицензию. Считается, что алгоритм попадает под действие патента Диффи-Хеллмана.

Выполнение работы

Генерация ключей

1. Генерируется случайное простое число p.
2. Выбирается целое число g — первообразный корень p.
3. Выбирается случайное целое число x такое, что $1 < x < p$.
4. Вычисляется $y = g^x \bmod p$.
5. Открытым ключом является тройка (p, g, y), закрытым ключом — число x.

Шифрование

Сообщение *M* должно быть меньше числа *P*. Сообщение шифруется следующим образом:

Выбирается сессионный ключ — случайное целое число k такое, что $1 < k < p-1$

Вычисляются числа $a = g^k \bmod p$ и $b = y^k M \bmod p$.

Пара чисел (*a*, *b*) является шифротекстом.

Нетрудно видеть, что длина шифротекста в схеме Эль-Гамаля длиннее исходного сообщения *M* вдвое

Расшифровывание

Зная закрытый ключ *x*, исходное сообщение можно вычислить из шифротекста (*a*, *b*) по формуле:

$$M = b\left(a^x\right)^{-1} \bmod p$$

При этом нетрудно проверить, что

$$\left(a^x\right)^{-1} \equiv g^{-kx} (\bmod p)$$

и поэтому

$$b\left(a^x\right)^{-1} \equiv (\mathrm{y}^k \mathrm{M}) g^{-kx} = \left(g^{xk} M\right) g^{-xk} \equiv M \left(\bmod p\right).$$

Для практических вычислений больше подходит следующая формула:

$$M = b\left(a^x\right)^{-1} \bmod p = b a^{(p-1-x)} \bmod p$$

Пример:

Шифрование

Допустим, что нужно зашифровать сообщение $M = 5$.

Произведем генерацию ключей:

Пусть $p = 11, g = 2$. Выберем $x = 8$ - случайное целое число x такое, что $1 < x < p$.

Вычислим $y = g^x \bmod p = 2^8 \bmod 11 = 3$.

Итак, открытым ключом является тройка $(p, \mathrm{g}, \mathrm{y}) = (11, 2, 3)$, а закрытым ключом - число $x = 8$.

Выбираем случайное целое число k такое, что $1 < k < (p-1)$. Пусть $k = 9$.

Вычисляем число $a = g^k \bmod p = 2^9 \bmod 11 = 512 \bmod 11 = 6$.

Вычисляем число $b = y^k M \bmod p = 3^9 5 \bmod 11 = 19683 \cdot 5 \bmod 11 = 9$.

Полученная пара $(a, b) = (6, 9)$ является шифротекстом.

Расшифрование

Необходимо получить сообщение $M = 5$ по известному шифротексту $(a, b) = (6, 9)$ и закрытому ключу $x = 8$.

Вычисляем M по формуле: $M = b\left(a^x\right)^{-1} \bmod p = 9\left(6^8\right)^{-1} \bmod 11 = 5$

Получили исходное сообщение $M = 5$.

Так как в схему Эль-Гамаля вводится случайная величина k ,то шифр Эль-Гамаля можно назвать шифром многозначной замены. Из-за случайности выбора числа k такую схему еще называют схемой вероятностного шифрования. Вероятностный характер шифрования является преимуществом для схемы Эль-Гамаля, так как у схем вероятностного шифрования наблюдается большая стойкость по сравнению со схемами с определенным процессом шифрования. Недостатком схемы шифрования Эль-Гамаля является удвоение длины зашифрованного текста по сравнению с начальным текстом. Для схемы вероятностного шифрования само сообщение M и ключ не определяют шифротекст однозначно. В схеме Эль-Гамаля необходимо использовать различные значения случайной величины k для шифровки различных

сообщений M и M’. Если использовать одинаковые k, то для соответствующих шифротекстов (a,b) и (a',b') выполняется соотношение $b(b')^{-1} = M(M')^{-1}$. Из этого выражения можно легко вычислить M', если известно M.

Варианты заданий

№	Исходный текст
1	Шумит дубравушка к непогодушке
2	Утром вороны каркают к дождю
3	Сорока на хвосте принесла
4	Снег холодный, а от мороза укрывает
5	Сирень или берёза, а всё дерево
6	Сегодня не тает, а завтра кто знает
7	Розы без шипов не бывает
8	Не высок лесок, а от ветра защищает
9	На всех и солнышко не светит
10	Красна ягодка, да на вкус горька
11	В осеннее ненастье семь погод на дворе
12	Ветром ветра не смеряешь
13	Пропущенный час годом не нагонишь
14	Счастливые часов не наблюдают
15	Друг неиспытанный, как орех не расколотый
16	Дружи с теми, кто лучше тебя самого
17	Крепкую дружбу и топором не разрубишь
18	Кто друг прямой, тот брат родной
19	лучше выслушать упрёки друга, чем потерять его
20	Одна пчела много мёду не принесёт
21	С тем не ужиться, кто любит браниться
22	Старый друг лучше новых двух
23	На чужой сторонушке рад родной воробушке
24	Народы нашей страны дружбой сильны
25	Поднявший меч от меча и погибнет
26	При солнце тепло, при Родине добро
27	Старая слава новую любит
28	Любишь кататься - люби и саночки возить
29	Кто пахать не ленится, у того хлеб родится
30	На печи не храбрись, а в поле не трусь

Библиографический список

1. Панасенко, С. Алгоритмы шифрования [Текст] / С. Панасенко. Спб: БХВ-Петербург, 2009, 576 стр.

2. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография [Текст] / А.Г. Ростовцев, Е.Б. Маховенко. М: АНО НПО "Профессионал", 2005, 480 стр.

3. Рябко, Б. Я., Фионов, А. Н. Основы современной криптографии для специалистов в информационных технологиях [Текст] / Б. Я. Рябко, А. Н. Фионов. М: Научный мир, 2004, 179 стр.

4. Смарт, Н. Криптография [Текст] / Н. Смарт. М: Техносфера, 2006, 528 стр.