Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

**Отчет по лабораторной работе №4**

**по курсу «СиМОИБ»**

**на тему: «Открытое распространение ключей»**

|  |  |
| --- | --- |
| Выполнил студент группы 821703: | Веренич К.О. |
| Проверил: | Захаров В. В. |

**МИНСК**

**2020**

**Вариант 5**

**Задание:**

Для заданного простого p найти a - примитивный элемент конечного поля GF(P) и выполнить обмен ключами при p=1877.

Описание шагов, выполняемых участниками протокола, Алисой и Бобом, для вычисления общего секрета:

1. P = 1877 - большое простое число, g = 3 - первообразный корень по модулю P.

2. Участник протокола Алиса:

(a) Выбирает число a ∈ [1; p − 1] и держит его в секрете:

(b) Вычисляет значение A = g amodP и передаёт его Бобу:

(c) Вычисляет значение BamodP = g a∗bmodP.

3. Участник протокола Боб:

(a) Выбирает число b ∈ [1; p − 1] и держит его в секрете;

(b) Вычисляет значение B = g bmodP и передаёт его Алисе:

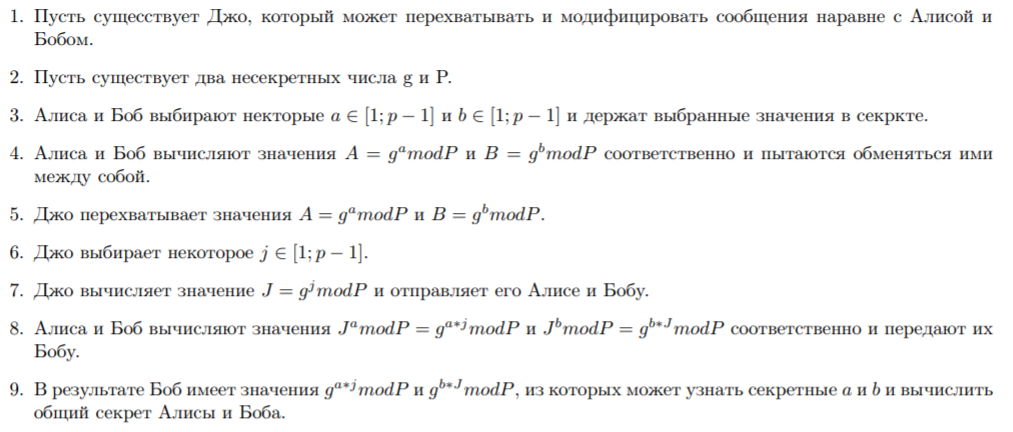
(c) Вычисляет значение AbmodP = g a∗bmodP.

В результате Алиса и Боб могут сгенерировать ключ шифрования, используя общий секрет в качестве стартового значения генератора.

**Вывод:**

Выводы: При правильном выборе параметров протокол Диффи-Хеллмана устойчив к пассивным атакам. Однако он не способен противостоять атаке «человек посредине», так как ни Алиса, ни Боб не могут точно знать, кто на самом деле является их собеседником.

Атака «человек посредине»:



Криптографическая стойкость алгоритма Диффи — Хеллмана, то есть сложность вычисления K = g abmodP по известным P, g, A, B, основана на сложности вычисления дискретого логарифма. Дискретное логарифмирование аналогично обычному логарифмированию в поле действительных чисел. Однако, в отличие от последней задачи, в которой решение является приближенным, задача о вычислении дискретного логарифма имеет точное решение. Это приводит к тому, что задача Диффи — Хеллмана и задача дискретного логарифмирования считаются трудноразрешимыми.

**Способы повышения криптографической стойкости алгоритма Диффи-Хеллмана:**

1. Следует выбирать P размером не менее 2048 бит.

2. Можно включить в процесс генерации ключей настоящие случайные числа. Для генерации таких чисел могут быть использованы небольшие изображения.

3. Для устойчивости к атакам "человек посредине" можно использовать цифровую подпись.

**Оценка сложности подбора ключа:**

1. f = f(x) = a xmodP. Функция f может быть вычислена за время O(n3 ), где n = log2 P. Для варианта P = 1877, n = log2 1877 = 10.8742. Максимальное количество операций 10.8742 = 2065. Современные суперкомпьютеры способны обрабатывать 2 48 операций в секунду. Следовательно, необходимое значение P будет подобрано на таком компьютере за доли секунды, а именно за 2 −37 секунд.

2. Предпочитаемым временем подбора установим отметку в 100 лет, что равно 2 32 секунд. n = 280∗1/3 = 227 , соответственно, размер P = 227 бит (около 100 млн. бит).