Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

**Отчет по лабораторной работе №3**

**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=4877.

Описание шагов, выполняемых участниками протокола - Алисой и Бобом для получения общего секрета.

Значения a и p известны всем и держатся в открытом доступе.

**Алиса:**

1. Выбирает случайно число из промежутка {1,2,3,…,p-1} и держит его в секрете.
2. По формуле вычисляет и помещает его в открытый источник.
3. Высчитывает ключ по формуле

**Боб:**

1. Выбирает случайно число из промежутка {1,2,3,…,p-1} и держит его в секрете.
2. По формуле вычисляет и помещает его в открытый источник.
3. Высчитывает ключ по формуле

**Вывод:**

Криптографическая стойкость алгоритма Диффи — Хеллмана (то есть сложность вычисления K=gabmodp по известным p, g, A=gamodp и B=gbmodp), основана на предполагаемой сложности проблемы [дискретногологарифмирования](http://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D0%B5_%D0%BB%D0%BE%D0%B3%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Однако, хотя умение решать проблему дискретного логарифмирования позволит взломать алгоритм Диффи — Хеллмана, обратное утверждение до сих является открытым вопросом.

**Модель атакующего:**

1)атакующий должен решить задачу вычисления дискретных логарифмов, получив из справочника *Yi* и *Yj*решить уравнение  и вычислить *Zij.*Таким образом он мог бы узнать общий ключ.

2)если передача ведется по каналу в котором возможна модификация, то атакующий мог бы перехватить данные и изменить их. В данном случае алгоритм Диффи — Хеллмана не работает.Когда в канале возможна модификация данных, появляется очевидная возможность вклинивания в процесс генерации ключей «злоумышленника-посредника» по той же самой схеме, что и для асимметричной криптографии.

Ключ является недостаточно большим. Если атакующий будет использовать метод подбора то с легкостью подберет нужный ключ. Для обеспечения достаточной стойкости взлома ключа необходимо использоватьXi и Xj порядка и p порядка . Число a не обязано быть большим и обычно имеет значение в пределах первого десятка.

К примеру мы имеет компьютер с частотой 2.3 GHz. Пусть компьютер имеет производительность 40 млрд операций в секунду, тогда знаю длину p можно легко посчитать, сколько нужно сделать умножений ().Так как p = 4877, то операции умножения. Найти Z не составит труда.

Для обеспечения достаточной защещенности от атаки с компьютером способным произвести 40 млрд операций в секундупонадобится выбрать p из диапазона 2^175. На подбор такого пароля уйдет 10 лет.

Чтобы обеспечить защиту от атакуюего с характеристиками суперкомпьютера(10^15 операций в сек) понадобиться выбрать p из диапазона 2^245. На подбор такого пароля уёдет примерно 10 лет.