Тиунов Андрей Юрьевич
студент
Кротова Елена Львовна
канд. физ.-мат. наук, доцент
ФГБОУ ВПО «Пермский национальный
исследовательский политехнический университет»
г. Пермь, Пермский край

АЛГОРИТМ ПРОТОКОЛА «ПОДБРАСЫВАНИЯ МОНЕТЫ»

Аннотация*: в современном мире очень важен вопрос безопасности, так как ежедневно появляются новые технологии и с ними появляются новые угрозы. Поэтому, чтобы сохранить конфиденциальность, разрабатываются новые методы шифрования конфиденциальных сведений. В данной статье показано на примере, как работает метод RSA.*

Ключевые слова*: шифрование, безопасность, данные, криптография, подбрасывание монеты, RSA.*

Алина и Борис хотят провести жеребьевку. К примеру, подбросить монету, но при этом они находятся друг от друга удалённо, в разных городах. В данной ситуации существует вероятность, что тот, кто подбрасывает монету, после броска монеты, может солгать другому, а другой может ему не поверить. Поэтому появилась нужда в алгоритме, выдающий независимый случайный результат. В 1981 году Мануэль Блюм опубликовал статью о протоколе «подбрасывания монеты по телефону» (CoinFlippingByTelephone), причём в заголовке своей работы он назвал это методом решения «нерешаемых задач». Для решения проблемы было использовано добавления в процесс третьего лица, на которое Алина и Борис возлагали доверие. Протокол позволял сторонам генерировать случайное число, состоящее из m бит и состоял он из 7 этапов:

1. Борис генерирует большое целое число Блюма $N = PQ$, где P и Q – это два больших простых числа, удовлетворяющих условию $P \equiv Q \equiv 3(mod4)$. После отправляет N Алине. На каждом этапе данного алгоритма выходные данные

получаются из x_n путём взятия либо бита чётности, либо одного или больше наименее значимых бит x_n.

2. Алина генерирует m случайных больших целых чисел: x1, x2, …, xm. В данном случае результатами жеребьёвки считаются числа $\left(\frac{Xi}{N}\right), i = 1,2, \dots, m$. Далее вычисляет числа $y_{i=Xi^2}(mod\ N)$, и отправляет их Борису.

3. Борис генерирует случайные знаки b1, b2, …, bm, пытаясь угадать знаки чисел $\left(\frac{Xi}{N}\right)$. Далее вычисляет числа, после чего отправляет их Бобу.

4. Алина сообщает Борису результаты угадывания, отправляя ему числа x1, x2, …, xm.

5. Борис проверяет выполнение условия $y_{i=Xi^2}(mod\ N)$, и открывает Алине числа P и Q.

6. Алина проверяет условия и проверяет, являются ли числа P и Q простыми.

7. Алина и Борис формируют случайную последовательность битов r_i, где $i = 1,2, \dots, m$ так, что r_i = 1 если $\left(\frac{Xi}{N}\right) = b_i$ (Борис угадал знак) и r_i = 0 если $\left(\frac{Xi}{N}\right) \neq b_i$ (Борис не угадал знак).

Получается алгоритм, при котором Алина и Борис могут создать неслучайные последовательности, но при этом они не знают последовательности друг друга пока не сформируют общую конечную, которую можно считать случайной. В конечном счёте третьим лицом можно назвать функцию $y_{i=Xi^2}(mod\ N)$. Данная функция является односторонней, и основана на сложности задачи восстановления дискретного логарифма, которую пока нельзя решить за разумное время. Точно так же как пока не решена задача факторизации числа, при соответствующих больших простых числах P и Q. Модифицированная версия протокола уже в 5 шагов:

1. Алина выбирает случайное большое целое число x, вычисляет $y = g^x mod\ p$ и посылает y Борису.

2. Борис генерирует случайный бит b, случайное большое целое число k, вычисляет $r = y^b g^k mod\ p$ и посылает r Алине.

3. Алина генерирует случайный бит c и посылает его Борису.

4. Борис посылает Алине b и k.

5. Алина проверяет, выполняется ли сравнение $r = y^b g^k mod\ p$. Если да, то результатом выполнения протокола будет бит $d = b \oplus c$.

Здесь уже более наглядно отображено, то что для работы протокола достаточно лишь временного сокрытия жеребьёвок и открытия их уже после получения результата.

На данной задаче основан алгоритм RSA, который на данный момент считается настолько надёжным, что ему доверяют большинство существующих вопросов информационной безопасности. Его используют крупные организации для зашифрования своих конфиденциальных сведений. Но, к сожалению, время идет, технологии развиваются ежедневно и надежность данных алгоритмов скоро будет сильно снижаться.

Список литературы

1. Тригуб С.Н. Современная криптография: теория и практика / С.Н. Тригуб. – М.: Издательский дом «Вильямс», 2005. – 768 с.

2. Ященко В.В. Введение в криптографию / В.В. Ященко [и др.]. – М.: МЦНМО, 2000. – 288 с.

3. Coin Flipping By Telephone – published by Manuel Blum: University of California at Berkeley. – 1981.