Лабораторная работа № 5

Алгоритм RSA

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Генерация ключей RSA:

- Выбираются два различных случайных простых числа p и q заданного размера.
- Вычисляется их произведение $n = pq$, которое называется модулем.
- Вычисляется значение функции Эйлера от числа n:

$$\varphi(n) = (p-1)(q-1).$$

- Выбирается целое число $e: 1 < e < \varphi(n)$, взаимно простое со значением функции $\varphi(n)$. Число e называется *открытой экспонентой.*
- Вычисляется число d, обратное к числу e по модулю $\varphi(n)$, то есть число, удовлетворяющее сравнению:

$$ed \equiv 1 \big(mod \varphi(n)\big).$$

Число d называется *секретной экспонентой*. Обычно, оно вычисляется при помощи расширенного алгоритма Евклида.

- Пара $\{e, n\}$ публикуется в качестве *открытого ключа RSA*.
- Тройка $\{d, p, q\}$ играет роль *закрытого ключа RSA* и держится в секрете.

Шифрование RSA.

Для открытого ключа $\{e, n\}$ и открытого теста m вычисляется:

$$C = E(m) = m^e \ mod \ n.$$

Расшифрование RSA.

Для зашифованного сообщения C и закрытого ключа $\{d, p, q\}$ вычисляется:

$$m = D(c) = c^d \ mod \ n.$$

Метод Ферма: факторизация, использующая разность квадратов

Известный из алгебры метод Ферма состоит в вычислении квадратов по модулю n для целых x, чуть больших $\sqrt{n}$, в надежде встретить полный квадрат y^2. Метод быстро работает, если $n = pq$ и числа p, q близки друг другу.

Суть метода.

Пусть надо разложить на множители число n. Если удастся найти два числа x и y такие, что $x^2 - y^2 = n$, то $(x + y)(x - y) = n$. Числа $(x + y)$ и $(x - y)$ являются множителями n, возможно, тривиальными (когда одно из этих чисел 1, а другое n.) Эти два числа x и y, дающие $x^2 - y^2 = n$, найдутся, если найдётся такое целое x, что $x^2 - n$ является квадратом. Тогда $x^2 - (x^2 - n)$ — разность квадратов, равная n.

Поиск начинают с $x = \lfloor\sqrt{n}\rfloor + 1$, наименьшего возможного числа, при котором разность $x^2 - n$ положительна. Увеличивают x на 1 и вычисляют $x^2 - n$, пока $x^2 - n$ не окажется точным квадратом. Если это произошло, пытаются разложить n как $(x - \sqrt{x^2 - n})(x + \sqrt{x^2 - n})$. Если это разложение тривиально, продолжают увеличивать *x*.

Бесключевое чтение

Для открытого ключа $\{e, n\}$ и зашифрованного сообщения C получить M. Это возможно путем итеративного возведения зашифрованного сообщения C в степень e. Необходимо найти такое j для которого выполняется:

$$C^{e^j} mod\ n \equiv C, \text{тогда } C^{e^{j-1}} mod\ n \equiv M.$$

Метод Винера

При выборе закрытой экспоненты возможна ситуация, когда $d < n^{0.25}$. Тогда можно определить d за полиномиальное время с помощью атаки Винера, опирающейся на непрерывные дроби.

$$ed \equiv 1\big(mod\varphi(n)\big),$$

следовательно

$$\exists k: ed - k\varphi = 1, \quad \left|\frac{e}{\varphi} - \frac{k}{d}\right| = \frac{1}{d\varphi}, \quad \varphi \approx n,$$

$$|n - \varphi| = |p + q - 1| < 3\sqrt{n}, \qquad \frac{e}{n} \sim \frac{k}{d},$$

$$\left|\frac{e}{n} - \frac{k}{d}\right| = \left|\frac{ed - kn}{dn}\right| = \left|\frac{ed - k\varphi - nk + k\varphi}{dn}\right| = \left|\frac{1 - k(n - \varphi)}{dn}\right| \leq \left|\frac{3k\sqrt{n}}{dn}\right| < \frac{1}{2d^2}.$$

Винер показал, что если

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{2d^2},$$

то

$$\frac{k}{d} - \text{подходящая дробь в разложении дроби} \frac{e}{n}.$$

Таким образом, можно узнать закрытую экспоненту, поочерёдно подставляя знаменатели подходящих дробей в выражение:

$$(m^e)^d = m \, mod \, n$$

для некоторого случайного числа m. Получив равенство, найдем d.

Задания лабораторной работы

Задание 1. Алиса и Боб используют RSA-64. Известен открытый ключ Алисы $\{e, n\}$. Используя методы факторизации числа, получить закрытый ключ $\{d, p, q\}$.

Задание 2. Алиса и Боб используют RSA-128. Известен открытый ключ Алисы $\{e, n\}$ и то, что при генерации p, q была допущена ошибка в их расположении друг относительно друга на числовой оси. Получить закрытый ключ $\{d, p, q\}$.

Задание 3. Алиса и Боб используют RSA-128. Известен открытый ключ Алисы $\{e, n\}$ и зашифрованное сообщение C. Необходимо узнать открытый текст M.

Задание 4. Алиса и Боб используют RSA-128. Известен открытый ключ Алисы $\{e, n\}$ и то, что при генерации d была допущена ошибка. Получить закрытую экспоненту d.

Выбор варианта.

Ваш вариант для выполнения лабораторной работы соответствует вашему номеру в списке. Для проверки значений, полученных в ходе лабораторной работы, необходимо рассчитать значение хэш-функции (файл для расчета hash.py) от данных, представленных в ASCII кодировке.