Ермолаева Екатерина, 14 группа, лабораторная №5, 2 вариант

RSA:

RSA

Алгоритм Gen (RSA)

Вход: 1^l.

Выход: открытая экспонента e (долговременные параметры par), модуль n (открытый ключ pk), секретная экспонента d (личный ключ sk).

Шаги:

1. Выбрать натуральное нечетное $e \geqslant 3$.
2. $p, q \xleftarrow{R} PRIMES$: $p \neq q$, p, q — нечетные, $(e, p-1) = 1$, $(e, q-1) = 1$, $\lceil \log_2 p + \log_2 q \rceil = l$.
3. $n \leftarrow pq$ (n является l-битовым числом).
4. Вычислить $\varphi(n) = (p-1)(q-1)$ [условия на p и q гарантируют, что $(e, \varphi(n)) = 1$].
5. Определить $d = e^{-1} \bmod \varphi(n)$.
6. Возвратить (e, n, d).

Алгоритм Ecnr (RSA)

Вход: n, e, $x \in \mathbb{Z}_n$ — открытый текст.

Выход: $y \in \mathbb{Z}_n^*$ – шифтекст.

Шаги:

1. $y \leftarrow x^e \bmod n$.
2. Возвратить y.

Алгоритм Decr (RSA)

Вход: n, d, y.

Выход: x.

Шаги:

1. $x \leftarrow y^d \bmod n$.
2. Возвратить x.

Алгоритм быстрого возведения в степень:

$$a^b \bmod n$$

$b = (b_{l-1} \ldots b_1 b_0)_2$ – двоичная запись, $b_i \in \{0,1\}$

$$a^b = \left(\ldots \left(\left(a^{b_{l-1}} \right)^2 a^{b_{l-2}} \right)^2 \ldots \right)^2 a^{b_0}$$

1. Установить $u \leftarrow 1$.
2. Для $i = l-1, l-2, \ldots, 0$ выполнить:
   (1) $u \leftarrow u \cdot u \bmod n$;
   (2) если $b_i \neq 0$, то $u \leftarrow u \cdot a \bmod n$.
3. Вернуть u.

Алгоритм нахождения обратного по модулю (расширенный алгоритм Евклида):

В то время как "обычный" алгоритм Евклида просто находит наибольший общий делитель двух чисел a и b, расширенный алгоритм Евклида находит помимо НОД также коэффициенты x и y такие, что:

$$a \cdot x + b \cdot y = \gcd(a, b).$$

Т.е. он находит коэффициенты, с помощью которых НОД двух чисел выражается через сами эти числа.

Внести вычисление этих коэффициентов в алгоритм Евклида несложно, достаточно вывести формулы, по которым они меняются при переходе от пары (a, b) к паре $(b\%a, a)$ (знаком процента мы обозначаем взятие остатка от деления).

Итак, пусть мы нашли решение (x_1, y_1) задачи для новой пары $(b\%a, a)$:

$$(b\%a) \cdot x_1 + a \cdot y_1 = g,$$

и хотим получить решение (x, y) для нашей пары (a, b):

$$a \cdot x + b \cdot y = g.$$

Для этого преобразуем величину $b\%a$:

$$b\%a = b - \left\lfloor \frac{b}{a} \right\rfloor \cdot a.$$

Подставим это в приведённое выше выражение с x_1 и y_1 и получим:

$$g = (b\%a) \cdot x_1 + a \cdot y_1 = \left(b - \left\lfloor \frac{b}{a} \right\rfloor \cdot a \right) \cdot x_1 + a \cdot y_1,$$

и, выполняя перегруппировку слагаемых, получаем:

$$g = b \cdot x_1 + a \cdot \left(y_1 - \left\lfloor \frac{b}{a} \right\rfloor \cdot x_1 \right).$$

Сравнивая это с исходным выражением над неизвестными x и y, получаем требуемые выражения:

$$\begin{cases} x = y_1 - \left\lfloor \frac{b}{a} \right\rfloor \cdot x_1, \\ y = x_1. \end{cases}$$

Параметры RSA:

p = 684391453787369

q = 938396705691661

n = 642230685637593717537170429909

ϕ(n) = 642230685637592094749010950880

e = 245372344253915653531369256899

d = 605386166262476612522775455179

Результаты зашифрования/расшифрования:

X1 = 184712154522842417799563173273

Y1 = Encr(X1) = 120595678337547166852120120039

Decr(Y1) = 184712154522842417799563173273

Y2 = 447204864183801463638208868116

X2 = Decr(Y2) = 222294727900343367551030300654

Бонус. Метод факторизации (Ро-алгоритм Полларда):

Пусть N составное целое положительное число, которое требуется разложить на множители. Алгоритм выглядит следующим образом[11]:

1. Случайным образом выбирается небольшое число x_0[12] и строится последовательность $\{x_n\}, n = 0, 1, 2, \ldots$, определяя каждое следующее как $x_{n+1} = F(x_n) \pmod N$.
2. Одновременно на каждом *i*-ом шаге вычисляется $d = \mathrm{GCD}(N, |x_i - x_j|)$ для каких-либо i, j таких, что $j < i$, например, $i = 2j$.
3. Если $d > 1$, то вычисление заканчивается, и найденное на предыдущем шаге число d является делителем N. Если N/d не является простым числом, то процедуру поиска делителей продолжается, взяв в качестве N число $N' = N/d$.

На практике функция $F(x)$ выбирается не слишком сложной для вычисления (но в то же время не линейным многочленом), при условии того, что она не должна порождать взаимно однозначное отображение. Обычно в качестве $F(x)$ выбираются функции $F(x) = x^2 \pm 1 (\bmod N)$[12] или $F(x) = x^2 \pm a (\bmod N)$[13]. Однако функции $x^2 - 2$ и x^2 не подходят[10].

Если известно, что для делителя p числа N справедливо $p \equiv 1 \pmod k$ при некотором $k > 2$, то имеет смысл использовать $F(x) = x^k + b$[10].