ЗАДАНИЕ 13. Метод Диксона:
Вход: Составное число $n$,
Выход: $p$— простой делитель числа $n$.

Алгоритм

1. Составить базу разложения $B = \{p_1, p_2, \ldots, p_h\}$, состоящую из всех простых чисел $p \le \sqrt{e^{\sqrt{\ln n \cdot \ln(\ln n)}}}$.
2. Выбрать случайное целое $b$, $\sqrt{n} \le b \le n$.
3. Вычислить $a = b^2 \bmod n$.
4. Проверить число $a$ на $B$-гладкость пробными делениями. Если $a$ является $B$-гладким, то есть $a = p_1^{\alpha_1(b)} p_2^{\alpha_2(b)} \cdots p_h^{\alpha_h(b)}$, то запомнить векторы:
   $\overline{\alpha}(b) = (\alpha_1(b), \alpha_2(b), \ldots, \alpha_h(b))$ и
   $\overline{e}(b) = (\alpha_1(b) \bmod 2, \alpha_2(b) \bmod 2, \ldots, \alpha_h(b) \bmod 2)$.
5. Повторять процедуру генерации чисел $b$ до тех пор, пока не будет найдено $h + 1$ $B$-гладких чисел $b_1, b_2, \ldots, b_{h+1}$.
6. Методом Гаусса найти линейную зависимость среди векторов $\overline{e}(b_1), \overline{e}(b_2), \ldots, \overline{e}(b_{h+1})$, т.е. $\overline{e}(b_{i_1}) \oplus \overline{e}(b_{i_2}) \oplus \cdots \oplus \overline{e}(b_{i_t}) = \overline{0}$, $1 \le t \le h + 1$, и положить:
   $x = b_{i_1} \cdot b_{i_2} \cdots b_{i_t} \bmod n$;
   $y = p_1^{\frac{1}{2}(\alpha_1(b_{i_1}) + \alpha_1(b_{i_2}) + \ldots + \alpha_1(b_{i_t})) \bmod n} \cdot p_2^{\frac{1}{2}(\alpha_2(b_{i_1}) + \alpha_2(b_{i_2}) + \ldots + \alpha_2(b_{i_t})) \bmod n} \cdot \ldots$
   $\cdot p_h^{\frac{1}{2}(\alpha_h(b_{i_1}) + \alpha_h(b_{i_2}) + \ldots + \alpha_h(b_{i_t})) \bmod n} = \prod_{j=1}^{h} p_j^{\frac{1}{2}(\alpha_j(b_{i_1}) + \alpha_j(b_{i_2}) + \ldots + \alpha_j(b_{i_t})) \bmod n}$.
7. Проверить $x \equiv \pm y \bmod n$. Если так, то повторить процедуру генерации новых чисел $b$. Если нет, то $n = pq$, где p = $(x + y, n)$, $q = (x - y, n)$.

ЗАМЕЧАНИЕ. Вариант этого алгоритма, когда в качестве $p_1 = -1$, и на шаге 3 в качестве $a = b^2 \bmod n$ берут вычет наименьший по абсолютной величине и проверяют его на $B$-гладкость. Например, по модулю 7 вычетами являются 0, 1, 2, 3, 4, 5, 6, а наименьшие по абсолютной величине будут: – 3, – 2, – 1, 0, 1, 2, 3.

*Метод непрерывных дробей* в алгоритме Диксона:

Строить базу разложения из малых простых чисел $p_i$, по которым $n$ является квадратичным вычетом, т.е. $\left(\frac{n}{p_i}\right) = 1$. В качестве чисел $b$ берём числители $P_i$ подходящих дробей к числу $\sqrt{n}$, для которых значения $P_i^2 (\bmod n)$ являются $B$-гладкими.

ЗАДАНИЕ 14. Разложение на множители по известным показателям RSA и значению функции Эйлера:

1. Вычисление параметров системы RSA.

Вход: длина простых чисел $p$ и $q$.

1) Генерация двух простых чисел $p$ и $q$ (сохранить в одном файле).
2) Вычисление $n = pq$, $\varphi(n) = (p - 1)(q - 1)$.
3) Генерация случайного $e$ с условием НОД($e$, $\varphi(n)$) = 1.
4) Вычисление $d$ с условием $ed \equiv 1 (\mathrm{mod}\ \varphi(n))$.

Выход: файл чисел $p$ и $q$,
файл открытого ключа ($n$, $e$),
файл закрытого ключа $d$.

2. Разложение на множители по известному значению функции Эйлера.

Вход: числа $n$ и $\varphi(n)$.

Выход: числа $p$ и $q$, делители $n$.

Задача: Решаем квадратное уравнение $x^2 - (n - \varphi(n) + 1)x + n = 0$, его корни и есть числа $p$ и $q$.

3. Разложение на множители по известным показателям RSA.

Вход: файл открытого ключа ($n$, $e$),
файл закрытого ключа $d$.

1. Представить число $ed - 1$ в виде $ed - 1 = 2^f s$, где $s$ нечётное число.
2. Выбрать случайное число $a$, $2 \le a \le n - 2$, и вычислить $u \leftarrow a^s \pmod n$, $v \leftarrow u^2 \pmod n$.
3. Пока $v \ne 1$, полагаем $u \leftarrow v$, $v \leftarrow u^2 \pmod n$.
4. При $u = -1$ вернуться на шаг 2. В противном случае вычислить $p \leftarrow$ НОД($u - 1$, $n$), $q \leftarrow$ НОД($u + 1$, $n$).
5. Результат: $p$, $q$.

Выход: файл чисел $p$ и $q$.

https://drive.google.com/open?id=0B2AKc7ibPQ_WNXNNdGdaQXdYd1E