$N = pq$

$29083 = 229 \times 127$

Checking is easy

Factorization is Hard.

g.c.d $(a, b) = c$

Let $a = mc$ $\quad b < a.$
$b = nc$

$r = a - bq$: c divides r

$= (m - nq)c$

$q_1 = \left[\frac{a}{b}\right]$ $\quad r_1 = a - bq_1$

$q_2 = \left[\frac{b}{r_1}\right]$ $\quad r_2 = b - q_2 r_1$

$q_3 = \left[\frac{r_1}{r_2}\right]$ $\quad r_3$: $q_{n+1} = \frac{r_{n-1}}{r_n}.$

$r_n = c$

$$
\begin{array}{r|l}
 & 3 \\
\hline
24 & 75 \\
 & 72 \\
\hline
 & 3 \\
\end{array}
$$

$$
\begin{array}{r|l}
 & 8 \\
\hline
3 & 24 \\
 & 24 \\
\hline
 & \cdot\cdot \\
\end{array}
$$

Period Finding

1. Given N, Choose a random $m < N$ which is coprime with N

2. Powers of m

$$F_N(a) = m^a \mod N$$

The smallest value of a $(= P)$

$$m^P = 1 \mod N.$$

is Period of this function.

$N = 21.$

Choose $m = 2$

$2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32 = 11 \pmod{21}$

$2^6 = 64 = 1 \pmod{21}$

Period. $P = 6$

$m \in \{2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

$$x^2 = 1 \mod N$$

If N is an odd prime

$$x = \pm 1$$

If N is a composite number

Non-trivial solns

$$x = \pm a \mod N$$

$$x^2 = 1 \mod 41$$

$N = 55$; $x = \pm 21$

8×55

$$x^2 = 441 = 1 \mod 440.$$

$$= 1 \mod 55$$

$m^P = 1 \mod N.$ — $x = m^{P/2}$

If P is odd, Algorithm fails

If P is even

$$(m^{P/2}+1)(m^{P/2}-1) = 0 \mod N.$$

If $m^{P/2}+1 = kN$ Algorithm fails.

Will contain factors of N

$N = 21$; $m = 2$, $P = 6$.

$$(m^{P/2}+1)(m^{P/2}-1) = 0 \bmod N$$

$$(2^3+1)(2^3-1)$$

9 $\quad$ 7

$N = 35$; $\quad$ $m = 13$

$13^2 = 169$

$13^4 = 28561 = 35 \times 816 + 1$

$P = 4$

$(13^2+1)(13^2-1)$

$= 170 \times 168$

Factor 5 (170)

Factor 7 (168)