

【Original Work】

Fast method of factoring decomposition of RSA cipher vol.0

Toshiro Takami

【Abstract】

We found that prime numbers repeat every 30, and all prime numbers are represented by $30m + n$ (positive integer including m is 0, n is a prime number smaller than 30 excluding 2 and 5).

If the end of the multiplication of the giant prime and the giant prime here is 5, it can be seen that any of the ends of each gigantic prime is 5. In other words, the one multiplied by a huge prime number and a huge prime number,

$$(30m + n) * (30s + t) = 900ms + 30(mt + ns) + nt$$

(positive integer including s is 0, t is a prime number smaller than 30 excluding 2 and 5)

.

nt includes something that is not a prime number. 33, 63, 93 and so on.

For example

$$1976869607 = 27109 * 72923 \text{ (both primes 27109 and 72923)}$$

, But this factorization is unknown to third parties.

1976869607 is a 10 digit integer and has 1 first. ms is counted as a positive integer of 6 digits (although there is a possibility of 7 digits).

Register with the last number of nt (the last digit) and prime factorize.

In the upper number, the last digit of nt is 7.

The last digit of nt is 7

$$(3, 19) (7, 11) (13, 19) (13, 29) (19, 23) (23, 29)$$

.

A program that prime factorization can be solved quickly when paying attention to the last 7.

First, divide by 3, 7, 11, 13, 17, 19, 23, 29 to see if it is an integer. If it is an integer it has that number as a prime factor.

The last 607 of 1976869607 is a prime number.

A huge odd number (one multiplied by a huge prime number and a huge

prime number) can be factorized using this factor.
By using this, it seems that the rupture of the RSA encryption becomes faster.

【Discussion】

$$(30m + n) * (30s + t) = 900ms + 30(mt + ns) + nt$$

The last number of RSA encryption is 7

(3, 19) (7, 11) (13, 19) (13, 29) (19, 23) (23, 29)

(Only third parties know 1976869607).

Below, I randomly picked up prime numbers and tried it.

$$72911 * 43063 = 3139766393 = 3.139766393 \times 10^9$$

393 is not prime number. 6393 is not prime number.

$$72617 * 43049 = 3126089233 = 3.126089233 \times 10^9$$

233 is prime number.

$$72469 * 43189 = 3129863641 = 3.129863641 \times 10^9$$

641 is prime number.

$$72277 * 60527 = 4374709979 = 4.374709979 \times 10^9$$

979 is not prime number. 9979 is also not prime number.

$$66103 * 50033 = 3307331399 = 3.307331399 \times 10^9$$

399 is not prime number. But 1339 is prime number.

$$72307 * 68023 = 4918539061 = 4.918539061 \times 10^9$$

61=prime number.

$$72421 * 61007 = 4418187947 = 4.418187947 \times 10^9$$

947 is prime number.

$$72901 * 23327 = 1700561627 = 1.700561627 \times 10^9$$

627 is not prime number. But 1627 is prime number.

$72431 \times 27067 = 1960489877 = 1.960489877 \times 10^9$
877 is prime number. 9877 is not prime number.

$72383 \times 34123 = 2469925109 = 2.469925109 \times 10^9$
109 is prime number. 5109 is not prime number.

$72767 \times 42023 = 3057887641 = 3.057887641 \times 10^9$
877 is prime number.

$71821 \times 41341 = 2969151961 = 2.969151961 \times 10^9$
961 is not prime number. 1961 is not prime number.

$72923 \times 39857 = 2906492011 = 2.906492011 \times 10^9$
11 is prime number. 2011 is prime number.

$61781 \times 55603 = 3435208943 = 3.435208943 \times 10^9$
943 is not prime number. 8943 is not prime number.

$72623 \times 41011 = 2978341853 = 2.978341853 \times 10^9$
853 is prime number. 1853 is not prime number.

$72313 \times 41453 = 2997590789 = 2.997590789 \times 10^9$
789 is not prime number.

$72287 \times 44983 = 3251686121 = 3.251686121 \times 10^9$
121 is not prime number. 6121 is prime number.

$44651 \times 25073 = 1119534523 = 1.119534523 \times 10^9$
523 is prime number. 4523 is prime number.

$64433 \times 56477 = 3638982541 = 3.638982541 \times 10^9$
541 is prime number. 2541 is not prime number.

$72379 \times 55889 = 4045189931 = 4.045189931 \times 10^9$
931 is not prime number. 9931 is not prime number.

$72911 \times 56989 = 4155124979 = 4.155124979 \times 10^9$
979 is not prime number. 4979 is not prime number.

$69857 \times 59611 = 4164245627 = 4.164245627 \times 10^9$
627 is not prime number. 5627 is not prime number.

$72719 \times 28219 = 2052057461 = 2.052057461 \times 10^9$
461 is prime number. 7461 is not prime number.

$72577 \times 45659 = 3313793243 = 3.313793243 \times 10^9$
243 is not prime number. 3243 is not prime number.

$72661 \times 35023 = 2544806203 = 2.544806203 \times 10^9$
203 is not prime number. 6203 is prime number.

$71707 \times 32381 = 2321944367 = 2.321944367 \times 10^9$
367 is prime number. 4367 is not prime number.

$72383 \times 60209 = 4358108047 = 4.358108047 \times 10^9$
47 is prime number. 8047 is not prime number.

$70381 \times 44587 = 3138077647 = 3.138077647 \times 10^9$
647 is prime number. 7647 is not prime number.

$68447 \times 32077 = 2195574419 = 2.195574419 \times 10^9$
419 is prime number. 4419 is not prime number.

[Reference]

1) https://en.wikipedia.org/wiki/Prime_number



I am a psychiatrist now and also a doctor of brain surgery before.
home

〒854-0067

47-8 kuyamadai, Isahaya City, Nagasaki Prefecture, Japan

Born on November 26, 1961

Currently 56 years old

I would like to receive an email. I will not answer the phone.

mmm82889@yahoo.co.jp

