On the connections between RSA cryptosystem and the Fibonacci numbers

József Dénes †
1122. Budapest, Csaba u. 10.
Budapest, Hungary

Tamás Dénes
1182. Budapest, Marosvásárhely u. 13/a.
Budapest, Hungary
e-mail: titoktan@freemail.hu

To the memory of my father József Dénes, in 2002 which is the year of his 70^{th} birthday and his death too.

Abstract

Necessary condition for u_p being a Fibonacci prime is p being a prime number, an other necessary condition by Theorem 1. of [3] for u_p greater or equal 5 is a Fibonacci prime number if $u_p = 6k + 1$ or $u_p = 6k - 1$. If u_p is not a prime number, then its prime factorization form as $u_p = \prod(6r \pm 1)(6s \pm 1)$ by C.P.S. (Theorem 2. of [3]) and does not posses a factor which equal to a Fibonacci number. We are saying in this paper on the Fibonacci pseudoprimes, on the Fibonacci twin primes and on an important theorem which states: *To every integer m have an a_n Fibonacci-type sequence, that holds $m = a_n$.* Consequently if the RSA modulus is a Fibonacci number, the cryptosystem is also vulnerable.

Mathematics Subject Classifications (2000). 11A07, 11A41, 11A51, 11B39, 11T71

RSA cryptosystem

The RSA cryptosystem invented by Rivest, Shamir and Adleman, was first published in the August 1977 issue of Scientific American. The cryptosystem most commonly used for providing privacy and ensuring authenticity of digital data.
We began by describing a simplied version of RSA encription. Let N=pq be the product of two large primes of the same size, say $\left[\frac{n}{2}\right]$ bits, each. Let e, d be to positive integers satisfying *ed≡1 mod* $\varphi(N)$ where $\varphi(N) = (p-1)(q-1)$ is the order of the multiplicate cyclic group of order $\varphi(N)$. A message is element M∈ $Z^*_{N(\varphi)}$, to encrypt M one should c=$M^e \mod N$.

To solve the ciphertext, the legitimate receiver computes $c^d \equiv M \mod N$. Indeed $c^d = M^{ed} \equiv M \mod N$ by Fermat (1601-1665) and Euler (1707-1783) theorems.

Fermat little theorem:
If p is prime, then for any integer a, we have $a^{p-1} \equiv 1 \mod p$

We say that a composite number n is a pseudoprime, if $a^{n-1} \equiv a \mod n$ holds. (Holds for at least base $a \geq 2$).

Examples:
$n = 91$ is a pseudoprime base 3, since 91 is composite number and $3^{91} \equiv 3 \mod 91$.
Similarly, 341 is a pseudoprime base 2, because $2^{341} \equiv 2 \mod 341$.

For each integer $a \geq 2$ there are infinitely many pseudoprimes base a.

A composite integer n for which $a^n \equiv a \mod n$ for every integer $(a, n) = 1$ is a Carmichael number. An integer n is a Carmichael number if and only if n is positive, composite, square-free, and for each prime p divinding n we have $p - 1$ dividing $n - 1$.
There are infinitely many Carmichael number.

Examples:
Let us denote the Carmichael number by c_i (i=1,2,3, ...), then $c_1 = 561 = 3{\cdot}11{\cdot}17$, $c_2 = 1105 = 5{\cdot}13{\cdot}17$, $c_3 = 1729 = 7{\cdot}13{\cdot}19$, $c_4 = 2465 = 5{\cdot}17{\cdot}29$.

In [8] one can find that the inadvertent use of a Carmichael number instead of a prime factor in a modulus of an RSA cryptosystem is likely to make the system totally vulnerable, but that such numbers may be deterted.

The first attack on an RSA public key (N, e) to consider is factoring of the modulus N. But other attacks due to D.N. Lehmer (see [5],[10]) and G.J. Simmons (see [9]) also exist.

Method of D.N.Lehmer is the following: Since $N = pq = a^2 - b^2 \quad (p \neq q, \;\; p, q > 2)$ Fermat's Christmas theorem would apply:

We set $a_0 = \left[\sqrt{N}\right], \quad \textit{and let} \quad a_k = a_0 + k$ for k=1,2,3, ...

One looks succesively at $a_1^2 - N, \;\; a_2^2 - N, \;\; a_3^2 - N, ...$ to see if any of these is a perfect square. If one would suppose that N has two prime factors than the iteration steps are decreased by approximately with $\frac{1}{6}$. Since $N = pq = (6u \pm 1)(6v \mp 1) \quad (u, v = 1, 2, 3, ...)$ holds. In [5] S.W.Golomb gave the number 8.616.460.799 the Jevons' number. In [5] factorization of Jevons' number was realized in 56 steps, by our method 19 steps might be required to obtain the result (8.616.460.799= 689.681· 96.079)

It is worth mentioning when N=pq then $N \equiv \pm 1 \mod 6$.

Although twenty years of research have led to a number of fascinating attacks, none of them is devastating (see [1]).

For factoring, 155 digits is the current record for worst-case numbers. A very famous factorization was of the 129-digit challenge number enunciated in M.Gardner's Mathematical Games column in 1977 (Scientific American). The number

RSA129 =114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

had been laid as a test case for the then new RSA cryptosystem. Some projected that 40 quadrillion years would be required to factor RSA129. Nevertheless, in 1994 it was factored.
As follows:

3490529510847650949147849619903898133417764638493387843990820577
X
32769132993266709549961988190834461413177642967992942539798288533,

and the secret message was decrypted to reveal: "THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE." The opinion of Gardner contradicts to the facts.

A prime number p is said to be a *strong prime* if $q = 2p + 1$ is also a prime number. From the theorem 1. in [3] we have the following condition of strong prime:

p is a strong prime iff $p = 6k - 1$ and $q = 12k - 1$ is also a prime number $(k = 1, 2, 3, \ldots)$.

Examples:

k	p	q
1	5	11
2	11	23
4	23	47
5	29	59
7	41	83
9	53	107

Remark. The product of two strong prime numbers equals to strong modulus. Let us suppose that p and q are the strong primes. It follows that the N=pq is the strong modulus $\frac{\varphi(N)}{4}$.
Theorem 3.4.4. in [2] p 125. says:

For each odd composite integer $n > 9$ we have $S(n) \leq \frac{\varphi(n)}{4}$ where
$S(n) = \{a \ mod \ n : n$ is a strong pseudo prime base $a\}$

An other "expert" has the opinion *"I recommend against specifically generating strong primes. The length of primes is much more important than the structure."*
The authors have the contrary opinion (see e.g. [5]).

Fibonacci numbers

If the modulus is a Fibonacci number the RSA cryptosystem is also vulnerable.

We define the Fibonacci numbers as a sequence: $u_1 = 1,\ u_2 = 1,\ u_3 = 2,\ u_4 = 3,\ u_5 = 5,\ ...,\quad F = \{u_1, u_2, u_3, u_4, u_5, ...\}$

By other words it is recurrence relation where each number after the second is the sum of the two preceding numbers in the sequence.

The formula in [7] p56 reads as follows: $u_{2n} = u_{n+1}^2 - u_{n-1}^2 \quad (n \geq 1)$ implies $u_{2n} = (u_{n+1} + u_{n-1})(u_{n+1} - u_{n-1}) \quad .$

Example: $\quad u_{20} = 6765,\ u_{11} = 89,\ u_9 = 34 \Rightarrow (89+34)(89-34) = 6765 = 123 \cdot 55$

Remark. If the modulus $N = u_{2n}$ then the factorization trivial from the above.

Example:

$N = u_8 = (u_5 + u_3)(u_5 - u_3) = (5+2)(5-2) = 7 \cdot 3 = 21$

Let us suppose that N have two prime factors (as it is usual, if N is an RSA modulus), then $n = 3k \pm 1$ is the sufficiency condition of $N = u_{2n}$. It follows from that property of Fibonacci numbers, which says that a Fibonacci number is even iff its index is $3k$ form (u_{3k} are always even) and each other case are odd.

Example:

n=6 $\Rightarrow \quad u_{12} = (u_7 + u_5)(u_7 - u_5) = (13+5)(13-5) = 18 \cdot 8$, where 18 and 8 are not prime numbers.

Trivially the above result can be generalized as follows:

$$\sum_{i=k}^{l} u_{4i} = u_{2l+1}^2 - u_{2k-1}^2 \quad k \geq 1$$

Example: $\quad \sum_{i=2}^{4} u_{4i} = u_8 + u_{12} + u_{16} = u_5^2 - u_3^2 + u_7^2 - u_5^2 + u_9^2 - u_7^2 = u_9^2 - u_3^2$

If we take $u_1 = 1 \quad and \quad u_2 = 3$ we have 1, 3, 4, 7, 11, 18, 29, 47,... which we shall call the *Lucas sequence*, in honor of the nineteenth century French mathematician E.Lucas. Formula I_7 ([7] p 56) says as follows: $u_{2n} = u_n l_n \quad where \quad l_n - n$th element of Lucas sequence. The modulus *(N=pq)* happened to be a Fobonacci number u_{2n} then the prime factors are u_n respectively l_n.

Example: $u_8 = 21 \quad u_4 = 3 \quad l_4 = 7 \Rightarrow \quad 21 = 3 \cdot 7$

By $u_p = P$ Fibonacci prime we define that P is a prime number.

Necessary condition for u_p being a Fibonacci prime is p being a prime number. It is immediate since every Fibonacci number u_k devides every Fibonacci number u_{nk} for n=1,2,3,... or if r is divisable by s, there u_r divisable by u_s (see Theorem III. p 39 [7]).
An other necessary condition (by [3] Theorem 1.) for $u_p \geq 5$ is a Fibonacci prime number if $u_p = 6k \pm 1$.
If u_p is not a prime number, then its prime factorization form as $u_p = \prod (6r \pm 1)(6s \pm 1)$ (by [3] Theorem 2.) and does not posses a factor which equal to a Fibonacci number. The sufficient condition for u_p being a Fibonacci prime is as given below.

If p is prime then

$$u_{p-1} \equiv 0 \mod p \qquad when \quad p \equiv \pm 1 \mod 5$$

$$u_{p+1} \equiv 0 \mod p \qquad when \quad p \equiv \pm 2 \mod 5$$

$$u_p \equiv 0 \mod p \qquad when \quad p \equiv 0 \mod 5 \text{ hold.}$$

(see Theorem 3.5.1. p 131 of [2])

The Fibonacci pseudoprime test is not just a curiosity. It is the sufficiency condition of u_p (p is a prime number) being a Fibonacci prime.
$u_{p-\varepsilon_p}$ where ε_p the Legendre symbol $\left(\frac{a}{5}\right)$.

For odd prime p the Legendre symbol $\frac{a}{p}$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \quad if & a \equiv 0 \mod p \\ 1 \quad if & a \; is \; a \; quadtratic \; residue \mod p \\ -1 \, if & a \;\; is \, a \, quadratic \; nonresidue \mod p \end{cases}$$

$u_p^{u_{p-\varepsilon_p}} \equiv u_p \mod u_{p-\varepsilon_p}$

We say that a composite number is a Fibonacci pseudoprime if the above equality holds. In p 57 of [7] one can find the formula which says $u_{n-1}u_{n+1} = u_n^2 + (-1)^n \quad n \geq 1$. That formula gives opportunity to introduce the Fibonacci twin primes.

Consider the case of twin primes, meaning two primes that differ by 2. Let p and $p+2$ be twin primes if $u_p \quad and \quad u_{p+2}$ Fibonacci numbers also prime numbers then we called $u_p,\ u_{p+2}$ Fibonacci twin primes. By Fibonacci twin primes says the above formula as follows: $u_{6k-1}u_{6k+1} = u_{6k}^2 + (-1)^{6k} = s \quad k \geq 1$

The existence of Fibonacci twin primes is equvivalent to s with two prime factors.

Examples:

$u_5 = 5,\ u_7 = 13, \quad u_6^2 + 1 = 65 \rightarrow \quad 65 = 5 \cdot 13$

$u_{11} = 89,\ u_{13} = 233, \quad u_{12}^2 + 1 = 20737 \rightarrow \quad 20737 = 89 \cdot 233$

Let us denote $n(s)$ the number of squares Fibonacci numbers, *n(pw)* the number of Fibonacci twin primes, *n(Pw)* the number of twin primes.
Obviously $n(s) \leq n(pw) \leq n(Pw)$ holds.
The formula (56 p [7]) reads as follows: $u_{2n+1} = u_{n+1}^2 + u_n^2 \quad n \geq 1$ implies that $d > 1$ the common divisor of u_{n+1} and u_n , u_{2n+1} can be represented as a product (see pp 234-235 of [4]. Theorem III. p 39 of [4] (see pp 22-29 of [11]) as follows: u_n is divisible by u_m if and only if n is divisible by m.

Examples:

$$u_7^{u_8} \equiv u_7 \mod u_8 \quad \Rightarrow \quad 13^{21} \equiv 13 \mod 21$$
$$u_{11}^{u_9} \equiv u_{11} \mod u_9 \quad \Rightarrow \quad 89^{55} \equiv 89 \mod 55$$

In such a way it is not safe the modulus (of RSA system) equal to Fibonacci prime.
See [4] p 234 $x^2 + y^2 = n$ implies $(x^2+y^2)(u^2+v^2) = (xu - yv)^2 + (xy + yv)^2$

A prime number of form $4k+1$ has a natural number $c, \quad c^2 + 1 \equiv 0 \mod p$
Related to RSA system the modulus N=pq $(c_1^2+1)(c_2^2+1) \equiv 0 \mod pq$ (see [7] p 42).
We say that the a_n is a Fibonacci-type sequence, if $a_1,\ a_2$ are arbitrary natural numbers and $a_n = a_{n-1} + a_{n-2}$.
The connection of Fibonacci-type number and Fibonacci number is the above equality:

$a_n = a_1 \cdot u_{n-2} + a_2 \cdot u_{n-1}$

Theorem:

To every integer m have an a_n Fibonacci-type sequence, that holds $m = a_n$.

Open problem:

The $m = a_n$ is not a unique correspondence, thus the following open problem is very important in the cryptography:

m is a given natural number. Which is the maximal n index of Fibonacci-type sequence like that $m = a_n$?

Example:

$m = 18 \quad \to \quad a_1 = 6, \quad a_2 = 6, \quad a_3 = 12, \quad a_4 = 18 (n = 4)$

$\to \quad a_1 = 2, \quad a_2 = 1, \quad a_3 = 3, \quad a_4 = 4, \quad a_5 = 7, \quad a_6 = 11, \quad a_7 = 18 \ (n = 7)$

References

[1] Dan Boneh: Twenty years of attacks on the RSA cryptosystem, Notices of the AMS February 1999. pp 203-213

[2] R. Crandall, C. Pomerance: Prime Numbers, Springer, New York, 2001.

[3] T. Dénes: Complementary prime-sieve, *PU.M.A, Volume 12, Number 2, 2001. 197-207*

[4] Erdős Pál, Surányi János: Válogatott fejezetek a számelméletből (in Hungarian) (Selected chapters from the theory of numbers), Polygon, Szeged, 1996.

[5] S.W. Golomb: On factoring Jevons' number, CRYPTOLOGIA, July 1996. No 3 p 243-246

[6] Elemér Kiss: Mathematical gems from the Bolyai chests (Translation from Hungarian version), Tipotex Limited, Budapest, 1999.

[7] V.E. Hoggatt, Jr.: Fibonacci and Lucas Numbers, Houghton Mifflin Company, Boston, 1969.

[8] R.G.E. Pinch: On using Carmichael numbers for public key encryption system (Available via internet)

[9] G.I. Simmons: Cryptology. The Mathematics of Secure Communications, The Mathematical Intelligencer (1979) 233-246

[10] G.I. Simmons (ed): Contemporary Cryptology, IEEE Press, New York, 1992.

[11] N.N. Vorobyov: Fibonacci Numbers, Boston, D.C. Heath & Co., 1963.

APPENDIX

i	Fibonacci numbers u_i	*Prime representation*
1	1	
2	1	
3	2	prime
4	3	prime
5	5	prime $(6k-1)$
6	8	2^3
7	13	prime $(6k+1)$
8	21	$3 \cdot 7$
9	34	$2 \cdot 17$
10	55	$5 \cdot 11$
11	89	prime $(6k-1)$
12	144	$2^4 \cdot 3^2 = 12^2$
13	233	prime $(6k-1)$
14	377	$13 \cdot 29$
15	610	$2 \cdot 5 \cdot 61$
16	987	$3 \cdot 7 \cdot 47$
17	1.597	prime $(6k+1)$
18	2.584	$2^3 \cdot 17 \cdot 19$
19	4.181	$37 \cdot 113$
20	6.765	$3 \cdot 5 \cdot 11 \cdot 41$
21	10.946	$2 \cdot 13 \cdot 421$
22	17.711	$89 \cdot 199$
23	28.657	prime $(6k+1)$
24	46.368	$2^5 \cdot 3^2 \cdot 7 \cdot 23$
25	75.025	$5^2 \cdot 3001$
26	121.393	$233 \cdot 521$
27	196.418	$2 \cdot 17 \cdot 53 \cdot 109$
28	317.811	$3 \cdot 13 \cdot 29 \cdot 281$
29	514.229	prime $(6k-1)$
30	832.040	$2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61$
31	1.346.269	$557 \cdot 2417$
32	2.178.309	$3 \cdot 7 \cdot 47 \cdot 2207$
33	3.524.578	$2 \cdot 89 \cdot 19801$

34	5.702.887	$1597 \cdot 3571$
35	9.227.465	$5 \cdot 13 \cdot 141961$
36	14.930.352	$2^4 \cdot 3^3 \cdot 17 \cdot 19 \cdot 107$
37	24.157.817	$73 \cdot 149 \cdot 2221$
38	39.088.169	$37 \cdot 113 \cdot 9349$
39	63.245.986	$2 \cdot 233 \cdot 135721$
40	102.334.155	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 41 \cdot 2161$
41	165.580.141	$2789 \cdot 59369$
42	267.914.296	$2^3 \cdot 13 \cdot 29 \cdot 211 \cdot 421$
43	433.494.437	prime $(6k - 1)$
44	701.408.733	$3 \cdot 43 \cdot 89 \cdot 199 \cdot 307$
45	1.134.903.170	$2 \cdot 5 \cdot 17 \cdot 61 \cdot 109441$
46	1.836.311.903	$139 \cdot 461 \cdot 28657$
47	2.971.215.073	prime $(6k + 1)$
48	4.807.526.976	$2^6 \cdot 3^2 \cdot 7 \cdot 23 \cdot 47 \cdot 1103$
49	7.778.742.049	$13 \cdot 97 \cdot 6168709$
50	12.586.269.025	$5^2 \cdot 11 \cdot 101 \cdot 151 \cdot 3001$
51	20.365.011.074	$2 \cdot 1597 \cdot 6376021$
52	32.951.280.099	$3 \cdot 233 \cdot 521 \cdot 90481$
53	53.316.291.173	$953 \cdot 55945741$
54	86.267.571.272	$2^3 \cdot 17 \cdot 19 \cdot 53 \cdot 109 \cdot 5779$
55	139.583.862.445	$5 \cdot 89 \cdot 661 \cdot 474541$
56	225.851.433.717	$3 \cdot 7^2 \cdot 13 \cdot 29 \cdot 281 \cdot 14503$
57	365.435.296.162	$2 \cdot 37 \cdot 113 \cdot 797 \cdot 54833$
58	591.286.729.879	$59 \cdot 19489 \cdot 514229$
59	956.722.026.041	$353 \cdot 2710260697$
60	1.548.008.755.920	$2^4 \cdot 3^2 \cdot 5 \cdot 11 \cdot 31 \cdot 41 \cdot 61 \cdot 2521$
61	2.504.730.781.961	$4513 \cdot 555003497$
62	4.052.739.537.881	$557 \cdot 2417 \cdot 3010349$
63	6.557.470.319.842	$2 \cdot 13 \cdot 17 \cdot 421 \cdot 35239681$
64	10.610.209.857.723	$3 \cdot 7 \cdot 47 \cdot 1087 \cdot 2207 \cdot 4481$
65	17.167.680.177.565	$5 \cdot 233 \cdot 14736206161$
66	27.777.890.035.288	$2^3 \cdot 89 \cdot 199 \cdot 9901 \cdot 19801$
67	44.945.570.212.853	$269 \cdot 116849 \cdot 1429913$
68	72.723.460.248.141	$3 \cdot 67 \cdot 1597 \cdot 3571 \cdot 63443$
69	117.669.030.460.994	$2 \cdot 137 \cdot 829 \cdot 18077 \cdot 28657$
70	190.392.490.709.135	$5 \cdot 11 \cdot 13 \cdot 29 \cdot 71 \cdot 911 \cdot 141961$
71	308.061.521.170.129	$6673 \cdot 46165371073$

72	498.454.011.879.264	$2^5 \cdot 3^3 \cdot 7 \cdot 17 \cdot 19 \cdot 23 \cdot 107 \cdot 103681$
73	806.515.533.049.393	prime $(6k+1)$
74	1.304.969.544.928.657	$73 \cdot 149 \cdot 2221 \cdot 54018521$
75	2.111.485.077.978.050	$2 \cdot 5^2 \cdot 61 \cdot 3001 \cdot 230686501$