TERNOPIL NATIONAL ECONOMIC UNIVERSITY, UKRAINE
DEGGENDORF INSTITUTE OF TECHNOLOGY, GERMANY
UNIVERSITY OF SOUTH BOHEMIA, CZECH REPUBLIC
IEEE GERMANY SECTION / COMMUNICATIONS SOCIETY GERMAN CHAPTER (COM19)

2020 10th International Conference on

ADVANCED COMPUTER INFORMATION TECHNOLOGIES ACIT'2020

Conference Proceedings

Deggendorf, Germany
September 16-18, 2020

2020 10th International Conference on Advanced Computer Information Technologies

ACIT'2020

Organized by:

Ternopil National Economic University, Ukraine
Deggendorf Institute of Technology, Germany
University of South Bohemia, Czech Republic
IEEE Czechoslovakia Section
IEEE Germany Section / Communications Society German Chapter (COM19)

IEEE Catalog Numbers
ISBN: 978-1-7281-6760-2
Part Number: CFP20S92-ART

CONTENTS

SECTION 1
Mathematical Models of Objects and Processes

SECTION 2
Specialized Computer Systems

SECTION 3
Artificial Intelligence and Machine Learning

SECTION 4
Software Engineering

SECTION 5
Information in Economic Activity and Digital Business Modeling

SECTION 6
Smart Grids and Intelligent Consumers

SECTION 7
Cyber Security and IT Law

SECTION 8
Image Processing

SECTION 9
Information Technologies in Historical Science

The Monte Carlo Type Method of Attack on the RSA Cryptosystem

Marek Wojtowicz
Institute of Mathematics
Kazimierz Wielki University
in Bydgoszcz
Bydgoszcz, Poland
mwojt@ukw.edu.pl

Dmytro Bodnar
Department of Economic Cybernetics
and Informatics
Ternopil National Economic University
Ternopil, Ukraine
bodnar4755@ukr.net

Ruslan Shevchuk
Department of Computer Science
Ternopil National Economic University
Ternopil, Ukraine
rsh@tneu.edu.ua

Oksana Bodnar
Institute of Pedagogics and Psychology
Ternopil Volodymyr Hnatiuk
National Pedagogical University
Ternopil, Ukraine
bodnarotern@ukr.net

Iryna Bilanyk
Pidstryhach Institute for Applied Problems of Mechanics and
Mathematics NAS of Ukraine
Lviv, Ukraine
i.bilanyk@ukr.net

***Abstract* — The RSA cryptosystem is the most widely used cryptosystem, and its security is based on the difficulty of factorization of big integers.**

We study the possibility of determination of the secret key of an RSA cryptosystem by means of the Monte Carlo method applied to the continued fraction method. We develop and extend similar techniques studied earlier by Wiener, de Weger, and others.

Keywords — RSA, Cryptanalysis, Continued fraction, Monte Carlo method.

I. Introduction

RSA is an asymmetric encryption algorithm which works with a public and private keys called a key pair [1]; see below.

Let p, q be two large prime numbers, $N := pq$ be the modulus of RSA, $\varphi(N) := (p-1)(q-1)$ be the Euler function of *N*, and let e, d be the public and private key pair, less than $\varphi(N)$ and relatively prime with $\varphi(N)$, with

$$ed \equiv 1\left(\bmod \varphi(N)\right). \tag{1}$$

Then the encryption function *E*(*M*) of a message *M* (with gcd(*M*,*N*)=1) is of the form

$$E(M) \equiv M^e \pmod N,$$

and the decryption function *D*(*S*) of an encrypted message *S* is of the form

$$D(S) \equiv S^d \pmod N.$$

Then, by (1), we have $D(E(M)) \equiv M \pmod N$.

Nowadays, RSA seems to be extremely secure, yet at the cost of the width of the modulus N. It has survived over 20 years of scrutiny and is in widespread use throughout the world [2,3]. The standard attack on the RSA cryptosystem involves factorization of *N*. Then, by (1) and the form of *D*, every message written with the public key can be decrypted.

In 1990, Wiener [4] proposed another method of attack on RSA. He proved that if $d < \frac{1}{3}N^{1/4}$ then d is the denominator of a convergent of the continued fraction determining the representation of the number e/N. The method is based on the following property [5, Theorem 184]:

If A is a real number and P/Q is an irreducible fraction such that

$$\left|A - \frac{P}{Q}\right| < \frac{1}{2Q^2}, \tag{2}$$

then P/Q is one of convergents of the continued fraction representing A.

In 2002, de Weger [6] showed that Wiener's attack on RSA can be strongly improved: by replacing (in Wiener's method) the continued fraction expansion of e/N by

$$A := \frac{e}{N - 2\sqrt{N} + 1}, \tag{3}$$

the key d can be obtained if the following relation holds:

$$\delta < \frac{3}{4} - \beta, \tag{4}$$

where $\delta = \log_N d$ and $\beta = \log_N |p-q|$, i.e.,

$$d = N^{\delta} \text{ and } \Delta := |p-q| = N^{\beta} \text{ for } \beta \in [\frac{1}{4}, \frac{1}{2}];$$

in the case of Wiener's attack we have $\delta < \frac{1}{4}$.

From inequality (4) it follows that the difference $\Delta = N^{\beta}$ cannot be too small. For example, if $\Delta < N^{1/4}$ then the attack by means of de Weger's method allows us to determine efficiently the private key d, because then $d < \sqrt{N}$, thus $\delta < 1/2$, which significantly improves Wiener's result.

Hence the practical conclusion follows: when constructing a specific RSA system, it is necessary to choose prime numbers p, q, so that the number Δ is at least of the order of $\sqrt{N}$, and $d > N^{1/3}$.

Wiener's idea to attack on the RSA system by the method of continued fractions was developed in subsequent years among others by Blomer and May [7] (2004), Dujella [5] (2004), Nitaj [8] (2008), Maitra and Sarkar [9] (2008), and Chen, Hsueh, and Lin [10] (2009).

978-1-7281-6760-2/20/$31.00 ©2020 IEEE

On page 20 of [6], de Weger suggests to consider the possibility of improving his results by including the numerical value of the public key e to the security analysis of the RSA system, i.e., examining the resistance of a given RSA system to a continued fraction attack with respect to the size of $\alpha := \log_N e$ (de Weger assumed that $\alpha \sim 1$, i.e., $e \approx N$).

The first research in this direction was carried out by Maitra and Sarkar [9]: they showed that if $q < p < 2q$, the RSA system is not secure (N can be factorized in $poly(\log N)$ time), when

$$d < \frac{1}{2}N^s \text{ and } ed^2 = O\left(N^{3/2-2s}\right),\ s < \frac{1}{2}.$$

By considering the convergents of the continued fraction expansion of the number

$$\frac{e}{N - \frac{3}{\sqrt{2}}\sqrt{N} + 1}, \tag{5}$$

Maitra and Sarkar obtained a generalization of inequality (4) with extra conditions on p, q.

In 2009, Chen, Hsueh, and Lin [10] applied the method of continued fractions to the number

$$\frac{e}{N - \frac{a+b}{\sqrt{ab}}\sqrt{N} + 1}, \text{ where } a, b > 0, \tag{6}$$

showing that the private key d can be determined if $\delta < \frac{3}{4} - \gamma$, where $\gamma = \log_N |ap - bq|$ (i.e., $|ap - bq| = N^\gamma$).

If $a = b = 1$, this method reduces to de Weger's attack (3), and to the Maitra-Sarkara method (5) for $a = 2b$.

The problem of factorization of large natural numbers, with applications to Mersenne numbers, was recently studied in the papers [11,12].

II. Main Result

Theorem 1. *Let e,d be two positive integers <φ(N) fulfilling relation* (1):

$$ed = 1 + k\varphi(N) \text{ for some natural number } k,$$

where $N = pq$ *and*

$$q > p + 2\sqrt{p} + 1. \tag{7}$$

Then there exists a real number $c' \in [2, c_0]$, $c_0 = \sqrt{9/2}$, *such that the following equality holds true:*

$$\frac{e}{N - c'\sqrt{N} + 1} = \frac{k}{d}.$$

Proof. Let F be a function on $[2, c_0]$ of the form

$$F(c) = \frac{e}{N - c\sqrt{N} + 1} - \frac{k}{d}.$$

(Notice that $k < e$ because $d < \varphi(N)$, where $e\varphi(N) > ed = 1 + k\varphi(N) > k\varphi(N)$. Hence we should check only denominators d_j of the convergents k_j/d_j with numerators $k_j < e$, i.e., whether $2^{ed_j} \equiv 2 (mod\, N)$.)

We shall prove that

$$F(2) < 0 < F(c_0), \tag{8}$$

because then the result holds by the continuity of F.

Set $W = \left(N - c\sqrt{N} + 1\right) \cdot d$. Notice that $W > 0$ for $c \in [2, c_0]$. Then

$$W \cdot F(c) = ed - k\varphi(N) -$$
$$-k\left(N + 1 - c\sqrt{N} - N + (p+q) - 1\right) =$$
$$1 - k\left(p + q - 2\sqrt{pq} - (c-2)\cdot\sqrt{pq}\right). \tag{9}$$

But since, by (7), $p + q - 2\sqrt{pq} > 1$, from (9) we obtain

$$W \cdot F(2) < 1 - k \le 0,$$

which is the left hand side of (8).

Now, by (9),

$$W \cdot F(c_0) = 1 - k\left(q + p - c_0\sqrt{pq}\right).$$

Thus, $F(c_0) > 0$ if $q + p - c_0\sqrt{pq} \le 0$, i.e.,

$$\sqrt{\frac{q}{p}} + \sqrt{\frac{p}{q}} \le c_0.$$

The latter inequality is equivalent to

$$\frac{p}{q} + 2 + \frac{q}{p} \le c_0^2 = \frac{9}{2},$$

thus, setting $x = p/q$, we obtain $x + x^{-1} - 2.5 \le 0$, i.e., $x^2 - 2.5x + 1 = (x-2)\cdot(x-0.5) \le 0$.

But since, by assumption, $x = p/q < 2$, the latter inequality holds true, which implies, by the above series of equivalences and implications, that $F(c_0) > 0$. This is the second required inequality in (8). The proof is complete.

Corollary. *Let* $c = \sqrt{5 - \frac{1}{r}}$, *where* $r \in [1, 2]$, *thus* $c \in [2, c_0]$. *If the conditions of Theorem 1 are satisfied then there exists a rational number* r*, such that the private key* d *can be determined by a convergent of the continued fraction expansion of the number*

$$w(c) := \frac{e}{N - c\sqrt{N} + 1}. \tag{10}$$

III. Example

In practice, the corollary implies the effectiveness of the Monte Carlo method, which relies on a random selection of rational numbers $r_j,\ j=1,2,\ldots$ from the interval $[1,2]$ and testing the congruence

$$2^{ed_j} \equiv 2 (mod\, N)$$

by means of denominators *dj* of consecutive convergents of the continued fraction expansion of the numbers $w(c_j)$, *j*=1,2,…, where c_j depends on r_j as in the Conclusion.

The numbers r_j can also be determined using the dyadic sequence:

$$1;\ 2;\ 1+\frac{1}{2};\ 1+\frac{1}{2^2},1+\frac{3}{2^2};\ 1+\frac{1}{2^3},1+\frac{3}{2^3},1+\frac{5}{2^3},1+\frac{7}{2^3};\ldots,(11)$$

or a sequence of fractions determined by consecutive primes p_k:

$$1;\ 2;\ 1+\frac{1}{2};\ 1+\frac{1}{3},1+\frac{2}{3};\ldots;\ 1+\frac{1}{p_k},1+\frac{2}{p_k},\ldots,1+\frac{p_k-1}{p_k};\ldots (12)$$

or a sequence of fractions $1+a/b$, where a,b are natural coprime numbers such that $a<b$:

$$1;\ 2;\ 1+\frac{1}{2};\ 1+\frac{1}{3},1+\frac{2}{3};\ 1+\frac{1}{4},1+\frac{3}{4};\ 1+\frac{1}{5},\ldots,1+\frac{4}{5};\ldots (13)$$

For example, for 9-digit prime numbers

$$p=231961001,\ q=371131003,$$

their product (modulus of an RSA) is a 17-digit number

$$N=qp=86087918958014003,$$

and

$$\varphi(N)=(q-1)(p-1)=86087918354922000.$$

In this example, we have $\delta=\beta=1/2$, whence $\delta+\beta=1>3/4$, so the necessary conditions (2) for de Weger's attack on the above RSA system are not satisfied.

We will now demonstrate the effectiveness of the Monte Carlo type attack described in the Corollary.

Testing the fractions of numbers $w(c)$ with the sequence of the form (11) we get that d is the denominator of the 11th convergent of the continued fraction expansion of number $w_1=w(c)=w\left(\sqrt{1-r^{-1}}\right)$ for $r=1+304395/2^{20}=1+304395/1048576$:

$$\left[0;1;\frac{108}{109},\frac{217}{219},\frac{8354}{8431},\frac{8571}{8650},\frac{291197}{293881},\frac{590965}{596412},\frac{22747867}{229557537},\right.$$

$$\left.\frac{46086699}{46511486},\frac{68834566}{69469023},\frac{\mathbf{114921265}}{\mathbf{115980509}},\frac{643440891}{649371568}\right].$$

By applying the sequence of the form (12) we can determine d for a lower denominator of the number $r-1$: k/d is the 10th convergent of the continued fraction expansion of $w_2=w(c(1+30826/106189))$; of course, here the 6-digit number 106189 is prime:

$$\left[0;\ 1,\frac{108}{107},\frac{217}{219},\frac{8354}{8431},\frac{8571}{8650},\frac{291197}{293881},\frac{590965}{596412},\right.$$

$$\left.\frac{22747867}{22957537},\frac{46086699}{46511486},\frac{\mathbf{114921265}}{\mathbf{115980509}},\frac{12342662054}{12456425949}\right].$$

The smallest denominator $r-1$ is obtained by testing the convergents of the continued fraction expansion of $w(c)$ by means of the sequence (13). The fraction k/d is the 10th convergent for $w_3=w(c(1+1947/6707))$, and the 4-digit number 6707 is composite (here $6707=19\cdot 353$):

$$\left[0;1;\frac{108}{109},\frac{217}{219},\frac{8354}{8431},\frac{8571}{8650},\frac{291197}{293881},\frac{590965}{596412},\right.$$

$$\left.\frac{22747867}{22957537},\frac{46086699}{46511486},\frac{\mathbf{114921265}}{\mathbf{115980509}},\frac{6136913744}{6193478463}\right].$$

Note that the first ten convergents of the continued fraction expansion of w_2 and w_3 are identical.

IV. Some Recommendations for Possible Using the Continued Fractions Tools in Cryptanalysis

Using a not widely spread properties of continued fractions we could improve the above algorithm or expand its possibilities. We build an expansion of a rational number by using the Euclidean algorithm. The representation is formed by subtracting away the integer part of a number and repeatedly inverting the remainder and subtracting away the integer part until the remainder is zero (for rational numbers). For irrational numbers this process is infinite. Furthermore, for algebraic irrationalities continued fractions are periodic.

Let a real number α have an expansion into a simple continued fraction

$$\alpha=b_0+\cfrac{1}{b_1+\cfrac{1}{b_2+\ddots}}=b_0+\frac{1}{b_1}\,\frac{1}{+b_2}+\ldots=b_0+\mathop{K}_{n=1}^{\infty}\frac{1}{b_n},\ (14)$$

where b_0 is an integer, and b_k are positive integers.

In the algorithm described in the previous paragraph, we calculate the m th numerators A_m and m th denominators B_m of the m th approximant (convergent) of the continued fraction (14)

$$\frac{A_m}{B_m}=b_0+\frac{1}{b_1}\,\frac{1}{+b_2}+\ldots\frac{1}{+b_m}.$$

But besides the convergents of continued fractions the best approximation we may obtain is by means of mediants. The mediant of two fractions *a/b* and *c/d* is defined as *(a+c)/(b+d)*. There we can apply the following mediants:

$$\frac{kA_m+A_{m-1}}{kB_m+B_{m-1}},$$

where $k=1,2,\ldots,b_{m+1}-1,\ m\geq 1$ if $b_{m+1}>1$.

Let us consider how we can calculate the m th approximant of a continued fraction. There are a couple of methods. It can be done by starting with b_m, and adding and inverting a proper fraction at each step back to b_0. This is the algorithm "from bottom to top".

Another way of calculating is "from top to bottom". It is based on the Wallis-Euler recurrence relations [13-15]:

$$\begin{aligned} A_m &= b_m A_{m-1} + A_{m-2},\ m \ge 1, \\ B_m &= b_m B_{m-1} + B_{m-2},\ m \ge 1, \end{aligned} \tag{15}$$

where

$$A_{-1} = 1,\ A_0 = b_0,\ B_{-1} = 0,\ B_0 = 1 .$$

Computation can be accelerated if we count only even or odd denominators of a continued fraction by means of the following formulas:

$$A_{2n+1} = \left(1 + b_{2n} b_{2n+1} + \frac{b_{2n+1}}{b_{2n-1}}\right) A_{2n-1} - \frac{b_{2n+1}}{b_{2n-1}} A_{2n-3},\ n \ge 1,$$

$$B_{2n+1} = \left(1 + b_{2n} b_{2n+1} + \frac{b_{2n+1}}{b_{2n-1}}\right) B_{2n-1} - \frac{b_{2n+1}}{b_{2n-1}} B_{2n-3},\ n \ge 1,$$

with the initial conditions

$$A_1 = b_0 b_1 + 1,\ A_{-1} = 1,\ B_1 = b_1,\ B_{-1} = 0,$$

or

$$A_{2n+2} = \left(1 + b_{2n+1} b_{2n+2} + \frac{b_{2n+2}}{b_{2n}}\right) A_{2n} - \frac{b_{2n+2}}{b_{2n}} A_{2n-2},\ n \ge 1$$

$$B_{2n+2} = \left(1 + b_{2n+1} b_{2n+2} + \frac{b_{2n+2}}{b_{2n}}\right) B_{2n} - \frac{b_{2n+2}}{b_{2n}} B_{2n-2},\ n \ge 1,$$

with the initial conditions

$$A_0 = b_0,\ A_2 = b_0 b_1 b_2 + b_0 + b_2,\ B_0 = 1,\ B_2 = b_1 b_2 + 1 .$$

Despite the fact that there are recurrent formulas for "from top to bottom" calculation, we can also apply other formulas that allow us to find the numerators and denominators of approximants immediately; in particular, the Euler-Minding formulas

$$A_m = b_0 b_1 \ldots b_m \left(1 + \sum_{k=0}^{m-1} \frac{1}{b_k b_{k+1}} + \sum_{k_1=0}^{m-3} \frac{1}{b_{k_1} b_{k_1+1}} \sum_{k_2=k_1+2}^{m-1} \frac{1}{b_{k_2} b_{k_2+1}} + \right.$$
$$\left. + \ldots + \sum_{k_1=0}^{m+1-2s} \frac{1}{b_{k_1} b_{k_1+1}} \sum_{k_2=k_1+2}^{m+3-2s} \frac{1}{b_{k_2} b_{k_2+1}} \cdots \sum_{k_s=k_{s-1}+2}^{m-1} \frac{1}{b_{k_s} b_{k_s+1}} \right),$$

$$B_m = b_1 b_2 \ldots b_m \left(1 + \sum_{k=1}^{m-1} \frac{1}{b_k b_{k+1}} + \sum_{k_1=1}^{m-3} \frac{1}{b_{k_1} b_{k_1+1}} \sum_{k_2=k_1+2}^{m-1} \frac{1}{b_{k_2} b_{k_2+1}} + \right.$$
$$\left. + \ldots + \sum_{k_1=1}^{m+1-2r} \frac{1}{b_{k_1} b_{k_1+1}} \sum_{k_2=k_1+2}^{m+3-2r} \frac{1}{b_{k_2} b_{k_2+1}} \cdots \sum_{k_r=k_{r-1}+2}^{m-1} \frac{1}{b_{k_r} b_{k_r+1}} \right)$$

where $s = \left[\frac{m+1}{2}\right]$, $r = \left[\frac{m}{2}\right]$.

V. Conclusion

The RSA cryptosystem security problem is considered in the terms of vulnerability to a Monte Carlo attack.

By generalizing the de Weger attack method, using the continued fraction technique, the Monte Carlo method has been shown to be effective for decrypting the private key of a given RSA system.

In the attached example, we showed that our method can cover a much broader group of cases than the de Weger method. In addition, the same result was obtained with the help of three independent methods of selecting the rational parameter *r* from the interval (1.2), allowing to find such a value of the tested which allows us determining the private key.

More detailed results along with the appropriate software will be included in a separate article.

References

[1] R. L. Rivest, A. Shamir and L. M. Adleman, "A Method for Obtaining Digital Signature and Public-Key Cryptosystems" *Communications of ACM*, Vol. 21, No. 2, 1978, pp. 120-126. doi:10.1145/359340.359342.

[2] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Computer Science*, vol. 78, pp. 617–624, 2016

[3] Z. Hercigonja, D. Gimnazija, and C. Varazdin, "Comparative analysis of cryptographic algorithms and advanced cryptographic algorithms," *International Journal of Digital Technology & Economy*, vol. 1, no. 2, pp. 1–8, 2016.

[4] M. Wiener, "Cryptanalysis of short RSA secret exponents", *IEEE Transactions on Information Theory*, Vol. 36, pp. 553–558, 1990.

[5] A. Dujella, "Continued fractions and RSA with small secret exponent" *Tatra Mountains Mathematical Publications*, vol. 29, pp. 101–112, 2004.

[6] B. De Weger, "Cryptanalysis of RSA with small prime difference" *Applicable Algebra in Engineering, Communication and Computing*, Vol 13 (1), pp. 17-28, 2002.

[7] J. Blomer, A. May "A Generalized Wiener Attack on RSA, Public key cryptography" *in Proc. of 7th international workshop on theory and practice in public key cryptography*, Singapore, March 1–4, 2004. Proceedings. Bao, Feng (ed.) et al., Berlin: Springer. Lecture Notes in Computer Science 2947, 1–13 (2004).

[8] A. Nitaj "Another generalization of Wiener's attack on RSA" *in Vaudenay, S. (ed.) Africacrypt 2008. Lecture Notes in Computer Science*, Springer-Verlag Vol. 5023, pp. 174–190, 2008.

[9] S. Maitra, S. Sarkar, Wu, Tzong-Chen (ed.) et al., "Revisiting Wiener's attack – new weak keys in RSA" *in Proc. of 11th international conference, ISC 2008*, Taipei, Taiwan, 2008.

[10] C.-Y. Chen, C.-C. Hsueh, Y.-F. Lin, "A Generalization of de Weger's Method" *in Proc. of Fifth International Conference on Information Assurance and Security*, Xi'an, Taiwan, pp. 344-347

[11] M. Kasianchuk, I. Yakymenko, S. Ivasiev et al. "The method of factorizing multi-digit numbers based on the operation of adding odd numbers" // *CEUR Workshop Proceedings, 8th International Conference Advanced Computer Information Technologies, ACIT 2018*; Ceske Budejovice, Czech Republic, June 2018. – P. 232-235.

[12] S. Ivasiev, I. Yakymenko, M. Kasianchuk, R. Shevchuk et al. "Effective algorithms for finding the remainder of multi-digit numbers" *in Proc. of 2019 9th International Conference on the Advanced Computer Information Technologies (ACIT-2019),* Ceske Budejovice, Czech Republic, June 2019, pp. 175–178.

[13] H.S. Wall, "Analytic Theory of Continued Fractions", *Reprinted by the American Mathematical Society*, Providence RI, 2000.

[14] A. Cuyt, V. Brevik Petersen, B. Verdonk, H. Waadeland, W. B. Jones. *Handbook of Continued Fractions for Special Functions*, Dordrecht: Springer, 2008.

[15] L. Lorentzen, H. Waadeland, "Continued fractions", *Convergence theory, Amsterdam, Paris: Atlantis Press/Word Scientific*, Vol. 1 2008.