RSA for poor men: a cryptosystem based on probable primes to base 2 numbers

Marek Wójtowicz[0000−0003−4644−6713]

Kazimierz Wielki University, Institute of Mathematics
Powstańców Wielkopolskich 2, 85-090 Bydgoszcz, Poland
mwojt@ukw.edu.pl

Abstract. We show it is possible to build an RSA-type cryptosystem by utilizing *probable primes to base 2* numbers. Our modulus N is the product $n \cdot m$ of such numbers (so here both prime and some composite, e.g. Carmichael or Fermat, numbers are acceptable) instead of prime numbers. Moreover, we require for n and m to be co-prime only, and so we don't have to worry about whether any of the numbers n, m is composite or not.
The encryption and decryption processes are similar as those in the RSA. Hence, in this cryptosystem we may apply the above kind of numbers of arbitrary length being still sure that the system works well. The price for that is not so high: the size of a message M (as a number) permitted by the new system must be smaller than log (in base 2) of $n \cdot m$.
The proposed cryptosystem can be applied in the case the numbers n, m are 'sufficiently large' for a user, or as a completion of the classical RSA if m, n are probable primes but possibly not prime, or in a 'secret sharing'-type cryptosystem.
The numbers n, m can be also taken from a narrower class of probable primes to base 2 numbers, e.g., Euler, or strong, or Baillie-PSW.

Keywords: RSA · Probable primes in base 2 · Carmichael numbers · Fermat numbers.

1 Introduction and the result

In this article, we present a variant of the RSA cryptosystem, based on *probable prime to base 2* numbers instead of prime numbers. We assume that the reader is familiar with the classic RSA and knows the basic facts of cryptography, see e.g. [7]. For $K > 1$ an integer, $\mathbf{Z}_K^*$ denotes the multiplicative group of the ring $\mathbf{Z}_K$, i.e., $\mathbf{Z}_K^*$ consists of all positive integers $k < K$ co-prime to K, endowed with multiplication modulo K. The symbol $\log_2 r$ denotes the logarithm in base 2 of a number $r > 0$.

1.1 Motivation and background

Let p, q be two distinct prime numbers. Set $N := p \cdot q$, and let φ and λ be the Euler and Carmichael, respectively, functions on N: $\varphi(N) = (p-1) \cdot (q-1)$, and

$\lambda(N) = \mathrm{lcm}(p-1, q-1)$. The classic RSA cryptosystem, built on p, q and N, encrypts and decrypts a message $M \in \mathbf{Z}_N^*$ using functions E and D, respectively, of the form:

$$E(M) = M^e (\mathrm{mod}\ N),\ \text{and}\ D(C) = C^d (\mathrm{mod}\ N)), \tag{1}$$

where $e, d \in \mathbf{Z}_{\lambda(N)}^*$ fulfill the congruence

$$e \cdot d \equiv 1 (\mathrm{mod}\ \lambda(N)). \tag{2}$$

Since, by Euler's formula

$$x^{\varphi(N)} \equiv 1\ (\mathrm{mod}\ N)\ \text{for all}\ x \in \mathbf{Z}_N^*, \tag{3}$$

$\lambda(N)$ in (2) can be replaced by $\varphi(N)$ because $\lambda(N)$ is the least positive integer t fulfilling the congruence

$$x^t \equiv 1\ (\mathrm{mod}\ N)\ \text{for all}\ x \in \mathbf{Z}_N^*. \tag{4}$$

(and also $\varphi(N)$ is trivially a multiple of $\lambda(N)$). The fact that $E(D(M)) = M$ is the result of congruences (1), (2) and (4)/(3).

The basis of this cryptosystem are two large prime numbers p, q. The problem of primality of a given *odd* positive integer n is a fundamental issue in building cryptosystems utilizing prime numbers. For this purpose, we can use either deterministic primality tests (based mainly on the Pocklington test [9], or AKS [12, Section 21]), or check the primality of n by a probabilistic test such as the Baillie-PSW, or Miller-Rabin test. For a recent review of the effectiveness of all known methods of such tests see the paper by Albrecht, Massimo, Paterson, and Smorovsky [1].

Each of these tests has both advantages and disadvantages. For example, deterministic tests are effective for particular kind of numbers or have other constrains, and probabilistic tests may give erroneous results: in 2005, Bleichenbacher [5] showed that the most popular probabilistic primality test, the Miller-Rabin test, if not well implemented, may pass composite numbers with probability 1. More recently, similar results were published in 2014 by Narayanan [10], and in the 2018 above-cited paper by Albrecht et al. [1]. Hence, every RSA cryptosystem based on such numbers will not work properly.

In this paper, we present a variant of the RSA-cryptosystem free of these drawbacks: it works well on every pair m, n of co-prime positive integers fulfilling the congruence $2^{x-1} \equiv 1 (\mathrm{mod}\ x)$.

1.2 Probabilistic tests and probable primes in base 2

The simplest probabilistic test is based on Fermat's little theorem: if the number n is prime, then each integer $a > 1$ co-prime to n fulfills the congruence:

$$a^{n-1} \equiv 1 (\mathrm{mod}\ n); \tag{5}$$

in particular (as n is odd by assumption),

$$2^{n-1} \equiv 1 \pmod{n}. \tag{6}$$

Hence, congruence (5), as well as its particular form (6), is a *necessary condition* for n to be prime.

Simple probabilistic arguments show that if the number a is chosen randomly, then the probability that n composite will pass test (5) is $\leq 1/2$. Thus, if n fulfills congruence (5) for $a_1, \ldots, a_k$ chosen randomly, the probability that n is prime is $\geq 1 - (1/2)^k$ and tends to 1 as $k \to \infty$.

For $n, a > 1$ two co-prime positive integers, n is said to be a *probable prime to base* a (PRP(a) for short) if it fulfills congruence (5). A composite number which passes positively a test X, say, is referred to as pseudoprime (w.r.t. X).

It is known that

1. The set of all PRP(2)-integers contains an infinite number of composite elements (e.g., Carmichael numbers [2]), along with all Fermat numbers $F_k = 2^{2^k} + 1$, $k = 1, 2, \ldots$ (see [8, Theorem 4.10]), and that
2. Pseudoprimes within the class of PRP(2)-integers are sparse: the probability that a randomly chosen PRP(2)-integer $n \leq 2^{64}$ is composite equals $2.79 \cdot 10^{-10}$ (see [6] and [13, Table 2], cf. [4, Section 2]).

Odd numbers n satisfying Euler's condition

$$a^{(n-1)/2} \equiv \pm 1 (\mathrm{mod}\ n), \tag{7}$$

with $a > 1$ co-prime to n, constitute a narrower subclass of PRP(a)-integers, and are called *Euler's probable primes to base* a (EPRP(a) for short).

A much stronger probability test than (7) stems from the relation: if n is an odd prime and $n = 2^\alpha d + 1$ with $\alpha \geq 1$ and d odd then, for every $a > 1$ co-prime to n,

$$\text{either } a^d \equiv 1 (\mathrm{mod}) \ \text{ or } \ a^{2^\beta \cdot d} \equiv -1 (\mathrm{mod}\ n) \ \text{ for some } 0 \leq \beta < \alpha. \tag{8}$$

Every odd integer $n > 1$ satisfying (8) is called a *base-a strong probable prime*, and the class of such numbers is denoted as SPRP(a). In particular, we have

$$SPRP(2) \subset FPRP(2) \subset PRP(2), \tag{9}$$

with both inclusions proper [4, Subsection 2.2].

It is interesting to note that a combination of Fermat's test (6) and a Lucas test yields a strong probabilistic primality test, referred to as the *Baillie-PSW test*, which is deterministic for numbers $\leq 2^{64} \approx 1.84 \cdot 10^{19}$ (see [4, Section 3]). Hence, we have a completion of the second/right inclusion in (9):

$$Baillie - PSW \subset PRP(2). \tag{10}$$

1.3 Construction of the new cryptosystem

In a few steps, we shall present below our idea of the new cryptosystem; it is easy to see, it has most of the elements from the RSA cryptosystem.

Let us define a Carmichael-type function μ on pairs (n, m) of *distinct* odd integers $n, m > 1$ by the formula

$$\mu(n, m) = \mathrm{lcm}(n - 1, m - 1) \tag{11}$$

(hence μ equals the Carmichael function λ for n, m distinct primes). Now let n, m be two co-prime PRP(2)-integers, and set $N := n \cdot m$. Since $\mu(n, m) = a \cdot (n - 1) = b \cdot (m - 1)$ for some integers $a, b \geq 1$, from the congruences

$$2^{n-1} \equiv 1 (\mathrm{mod}\ n) \ \text{ and } \ 2^{m-1} \equiv 1 (\mathrm{mod}\ m) \tag{12}$$

we obtain $2^{\mu(n,m)} \equiv 1 (\mathrm{mod}\ n)$ and $2^{\mu(n,m)} \equiv 1 (\mathrm{mod}\ m)$, i.e., the number $2^{\mu(n,m)} - 1$ is divided by both n and m, and hence by $N = n \cdot m$:

$$2^{\mu(n,m)} \equiv 1 (\mathrm{mod}\ N). \tag{13}$$

Now we define two parameters e and d – the encryption and decryption keys, respectively – similarly as in the classic RSA system: we choose $e, d > 1$ from the multiplicative group $\mathbf{Z}^*_{\mu(n,m)}$ fulfilling the congruence

$$e \cdot d \equiv 1 (\mathrm{mod}\ \mu(n, m)), \tag{14}$$

i.e.,

$$e \cdot d = 1 + k \cdot \mu(n, m) \ \text{ for some integer } k. \tag{15}$$

Further, with N as above, we define two functions E and D acting from the set of positive integers into positive real numbers:

$$E(x) = 2^{x \cdot e} (\mathrm{mod}\ N), \ \text{and } D(y) = \log_2(y^d (\mathrm{mod}\ N)).$$

We claim that E and D are well defined encryption and decryption functions for all messages M less than $\log_2 N$. (Notice, however, that $D(y)$ is an integer if and only if $y^d (\mathrm{mod}\ N)$ is a power of 2, hence the proposed cryptosystem cannot be applied to digital signing, in general.) This is stated in the theorem below, and its proof is given in Section 3 of this paper.

Theorem. *In the notation as above, for every integer/message M with $1 < M < \log_2 N$, we have $E(D(M)) = M$.*

Remark 1. From (13) and (12) we obtain that the congruence $2^{t \cdot \mu(n,m)} \equiv 1 (\mathrm{mod}\ N)$ holds for every positive integer t, and that

$$2^{\Phi(n,m)} \equiv 1 (\mathrm{mod}\ N), \tag{16}$$

where $\Phi(n, m)$ is an Euler-like function of n, m of the form $\Phi(n, m) = (n - 1) \cdot (m - 1)$. Hence, in our cryptosystem, the function μ can be replaced by Φ (or $t \cdot \mu$ with $t > 1$ an integer) without changing the result.

2 The Algorithm

In the description of the new algorithm we follow all steps of the RSA algorithm.

(KGA) Key Generation Algorithm

1. Generate two large co-prime PRP(2)-integers, n and m, of approximately equal size such that their product $N = n \cdot m$ is of the required bit length.
2. Compute $N = m \cdot m$ and $\mu(n, m) = \mathrm{lcm}(n - 1, m - 1)$.
3. Choose an integer $1 < e < \mu(n, m)$ such that $\gcd(e, \mu(n, m)) = 1$.
4. Compute $1 < d < \mu(n, m)$ such that $ed \equiv 1 (\mathrm{mod}\ \mu(n, m))$.
5. The public key is (e, N) and the private key is (d, N).

(E) Encryption

Sender X does the following:

1. Obtains the recipient Y's public key (N, e).
2. Represents the message as a positive integer M with $1 < M < \log_2 N$.
3. Computes $C = E(M) = 2^{e \cdot M} (\mathrm{mod}\ N)$.
4. Sends C to Y.

(D) Decryption

Recipient Y does the following:

1. Uses the private key (d, N) and computes the number $M_{(2)} = C^d (\mathrm{mod}\ N)$.
2. Computes $M = \log_2 M_{(2)}$.

Remark 2. By Remark 1, the function μ in the above Key Generation Algorithm can be replaced by Φ.

3 Correctness of the Algorithm – proof of the Theorem

Because the numbers $M_{(2)} = 2^M$ and N are co-prime with $M_{(2)} < N$, the 'message' $M_{(2)}$ lies in the multiplicative group $\mathbf{Z}_N^*$. Therefore every power of $M_{(2)}$ modulo N lies in $\mathbf{Z}_N^*$ too. Hence, the result of E, $C := E(M) = M_{(2)}^e (\mathrm{mod}\ N)$, belongs to $\mathbf{Z}_N^*$. Then the formula $C \to C^d (\mathrm{mod}\ N)$ sends C into an element of $\mathbf{Z}_N^*$, and the final element equals 2^M: by (13) and (15), we obtain

$$C^d \equiv M_{(2)}^{ed} \equiv M_{(2)}^{1+k \cdot \mu(n,m)} \equiv 2^{M + k \cdot M \cdot \mu(n,m)} \equiv$$

$$2^M \cdot (2^{\mu(n,m)}) \equiv 2^M \ (\mathrm{mod}\ N),$$

and the latter equals just 2^M because $2^M < N$. Therefore $D(E(M)) = \log_2 2^M = M$, as claimed.

Remark 3. By Remarks 2 and 3, the prof of the theorem goes the same lines as above for Φ instead of μ.

4 Example.

We give below an example to show how the algorithm works in a concrete case.

Step (KGA). We have generated two small composite co-prime PRP2-numbers $n = 341$ and $m = 645$.

Hence $N = 219\ 945$ and $\mu(341, 645) = \text{lcm}(340, 644) = 54\ 740$.

For $e = 257$, we obtain that $d = 213$ fulfills the congruence $ed \equiv 1 (\text{mod } 54\ 740)$. Hence the public and private keys are $(257, 219\ 945)$ and $(213, 219\ 945)$, respectively. The system accepts messages $1 < M < \log_2 219\ 945) = 17.74...$

Step (E). Let $M = 15$. We encrypt M and compute $C = E(M) = 2^{257 \cdot 15} (\text{mod } 219\ 945) = 175988$.

Step (D). We compute $M_{(2)} = 175988^{213} (\text{mod } 219\ 945) = 32768$.

Finally, we compute $\log_2 M_{(2)} = \log_2 32768$ and obtain the sent message $M = 15$.

5 Security and applications

1. The constraint $M < \log_2 N = \log_2 n + \log_2 m$ forces the use of large numbers n, m. For example, if we require $M \approx 2000$ (i.e., our dictionary consists of decimal words ≤ 2000) we need n, m of about 1000 bits each. By item 2 in Subsection 1.2, the probability that n or m is composite is about $5.5 \cdot 10^{-10}$ (and four time less for SPRP(2)-numbers - see the second column in the first Feitsma's table [6]). Moreover, for much larger n, m one can use the Baillei-PSW test because there is not known, as yet, a composite number $n > 2^{64}$ passing that test positively [4, Section 3].
2. The size of n, m depends heavily the 'time of living' of M - it should be much longer than the time needed for factorization of N.
3. The message M can also be devided into a finite number $M_1, M_2, \ldots, M_k$ of sub-messages such that their concatenation $M_1 \circ M_2 \circ \ldots \circ M_k$ yields M, and each M_i sent to a recipient via the above cryptosystem built on randomly chosen sufficiently large co-prime PRP(2)-numbers (n_i, m_i) with proper encryption and decryption keys (e_i, d_i), $i = 1, 2, \ldots, k$. Then, by item 2 in Subsection 1.2, the probability that the message M can be deciphered is $(5.6)^k \cdot 10^{-k \cdot 10}$. In practice, for $k > 2$, this is impossible.
4. Since computers 'like' to work with numbers of type 2^x, $x > 1$ an integer, the proposed cryptosystem can be easily implemented on every laptop with the use of on-line powering and logarithms in base 2. For example, the system works well with numbers (n, m) of the form $(F_r, 2F_r + 2t - 1)$, where F_r is the rth Fermat number and $t > 1$ is an integer such that $2F_r + 2t - 1$ is a PRP(2)-number. For $r = 6$ we may take $t = 65$, whence $\Phi(F_6, 2F_6 + 130 - 1) = 2^{64} \cdot (2^6 5 + 130)$. Then the least encryption key $e = 5$, whence $d = 272225893536750771729930377778311253197$. This cryptosytem accepts $M < 129$.

References

1. Albrecht, R.M., Massimo, J., Paterson, K.G., Smorovsky, J.: *Prime and Prejudice: Primality Testing Under Adversarial Conditions*, In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, October 15–19, 2018, 2018. https://doi.org/10.1145/3243734.3243787
2. Alford, W.R., Granville, A., and Pomerance, C.: *There are Infinitely Many Carmichael Numbers*, Annals of Math. **139** (1994), 703–722. https://doi.org/10.2307/2118576
3. Baillie, R., Wagstaff, S. S. Jr.,*Lucas pseudoprimes*, Math.Comp.,**35** (1980), 1391–1417. https://doi.org/.org/10.1090/S0025-5718-1980-0583518-6
4. Baillie, R., Fiori, A., Wagstaff S.S. Jr.: *Strengthening the Baillie-PSW primality test*, arXiv: 2006.14425v1 [math.NT] 25 June 2020
5. Bleichenbacher, D.: *Breaking a Cryptographic Protocol with Pseudoprimes*, In: Vaudenay S. (eds) Public Key Cryptography - PKC 2005. PKC 2005. Lecture Notes in Computer Science, vol 3386. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-30580-4-2
6. Feitsma, J.: *Pseudoprimes* (2013), http://www.janfeitsma.nl/math/psp2/statistics
7. Koblitz, N.: *A Course in Number Theory and Cryptography*, 2nd ed., Springer-Verlag, New York, 1994. https://doi.org/10.1007/978-1-4419-8592-7
8. Krizek, M., Luca, F., and Somer, L.: *17 Lectures on Fermat Numbers*, Springer-Verlag, New York, 2001. https://doi.org/10.1007/978-0-387-21850-2
9. Maurer, U. M.: *Fast Generation of Prime Numbers and Secure Public-Key Cryptographic Parameters*, J. Cryptology, **8** (1995), 123–155. https://doi.org/10.1007/BF00202269
10. Narayanan, S.: *Improving the Speed and Accuracy of the Miller-Rabin Primality Test*. MIT PRIMES-USA (2014) https://math.mit.edu/research/highschool/primes/materials/2014/Narayanan.pdf.
11. Pomerance, C.; Selfridge, J. L., Wagstaff, S. S. Jr.: *The pseudoprimes to* $25 \cdot 10^9$, Mathematics of Computation. **35 (151)** (July 1980), 1003-1026. https://doi.org/10.1090/S0025-5718-1980-0572872-7
12. Shoup, V.: A Computational Introduction to Number Theory and Algebra, 2nd ed., Cambridge University Press, Cambridge, 2009. https://doi.org/10.1017/CBO9780511814549
13. Staple, B. D.: *The combinatorial algorithm for computing* $\pi(x)$ (2015), https://arxiv.org/pdf/1503.01839.pdf