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 *distinct* only, not necessarily coprime, 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 the size of words permitted by the new system: any message M, as a number, must be smaller than $\log_2(n \cdot m)$.

Keywords: RSA · Pseudoprimes in base 2 · Carmichael 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. [2].

Let $n, a > 1$ be two coprime positive integers. Then n is said to be a *probable prime to base a* (PRPa for short) if it fulfills the congruence

$$a^{n-1} \equiv 1 (\mathrm{mod}\ n)\,. \tag{1}$$

By the Fermat little theorem, congruence (1) holds true if n is prime; in particular, for $a = 2$ and *every* n odd prime. As it is well known, the set of all PRP2-integers contains an infinite number of composite elements (e.g., Carmichael numbers [1]), along with all Fermat numbers $F_k = 2^{2^k} + 1$, $k = 1, 2, \ldots$ (see [3, Theorem 4.10]).

Now, in a few simple steps, we shall present 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

$$\mu(n, m) = \mathrm{lcm}(n-1, m-1) \tag{2}$$

(hence μ equals the Carmichael function λ for n, m distinct primes). Now let n, m be two distinct PRP2-integers, and set $N := n \cdot m$. Since $\mu(n, m) = a \cdot (n-1) = b \cdot (m-1)$ for some integers $a, b \geq 11$, from the congruences

$$2^{n-1} \equiv 1 (\mathrm{mod}\ n) \ \text{ and } \ 2^{m-1} \equiv 1 (\mathrm{mod}\ m) \tag{3}$$

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 $N = n \cdot m$:

$$2^{\mu(n,m)} \equiv 1(\mathrm{mod}\ N). \tag{4}$$

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

$$e \cdot d \equiv 1(\mathrm{mod}\ \mu(n, m)), \tag{5}$$

i.e.,

$$e \cdot d = 1 + k \cdot \mu(n, m) \ \text{ forsomeinteger } k. \tag{6}$$

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 $E(D(M)) = M$.*

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 PRP2-integers, n and m, of approximately equal size such that their product $N = m \cdot m$ 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 $ed \equiv 1 (\text{mod } \mu(n,m))$.
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 $C = E(M) = 2^{e \cdot M} (\text{mod } N)$.
4. Sends C to Y.

(D) Decryption

Recipient Y does the following:

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

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

Step (KGA). We have generated two small composite 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 $M = 15$.

3 Correctness of the Algorithm – proof of the Theorem

Because the numbers $M_{(2)} = 2^M$ and N are coprime, the 'message' $M_{(2)}$ lies in the multiplicative group $\mathbf{Z}_N^*$. Hence, the result of E, $C_M := E(M) = M_{(2)}^e (\text{mod } N)$, lies in $\mathbf{Z}_N^*$ too. Then the formula $C_M \to C_M^d (\text{mod } N)$ sends C_M into an element of $\mathbf{Z}_N^*$, and the final element equals 2^M. Therefore $D(E(M)) = \log_2 2^M = M$, as claimed.

References

1. 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
2. Koblitz, N.: *A Course in Number Theory and Cryptography*, Second edition, Springer-Verlag, New York, 1994. https://doi.org/10.1007/978-1-4419-8592-7
3. 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