General Multi-Prime Multi-Power RSA—A Generalization of RSA and CRT-RSA to Regular Integers Modulo n

Klaus Dohmen and Mandy Lange-Geisler

Department of Mathematics, Mittweida University of Applied Sciences,
Mittweida, Germany
{dohmen,mlange1}@hs-mittweida.de

Abstract. We present a multi-prime multi-power generalization of RSA for arbitrary integer moduli $n > 1$ and messages $m < n$ which are regular modulo n, meaning that they have a John-von-Neumann pseudoinverse modulo n. We prove that our RSA generalization is correct in the sense that it works for all regular messages modulo n, and complete in the sense that it works for no other message. Our correctness and completeness result, which implies the original RSA correctness theorem, is proved in a rigorous way based on a new sharpening of Charmichael's theorem established in this paper. As for CRT-RSA, decryption can be accelerated by Chinese remaindering, which results in a multi-prime multi-power generalization of CRT-RSA. We show that the restriction to regular messages modulo n is negligible by proving that under reasonable assumptions almost all messages are regular modulo n. More precisely, we give a probabilistic argument that for k-bit primes $p_1, \ldots, p_r$ the probability that a random message fails to be regular modulo $n = p_1^{e_1} \ldots p_r^{e_r}$ is at most $r/2^{k-1}$, which quickly tends to 0 as $k \to \infty$, and which shows that our general scheme can be used even with primes of moderate length.

Keywords: RSA · CRT-RSA · multi-prime · multi-power · regular integer modulo n · lambda function · Carmichael's theorem · Euler's theorem

1 Introduction

The RSA cryptosystem, introduced by Rivest, Shamir and Adleman [7] in 1978, is a widely used cryptographic technique, which even nowadays is a subject of extensive research. It utilizes a public key (n, e) for encryption and a private key (n, d) for decryption, where n is a product of distinct primes p and q, and $1 < e, d < \nu(n)$ such that $ed \equiv 1 \pmod{\nu(n)}$, where $\nu(n)$ denotes Euler's totient function $\varphi(n)$ as in the original RSA paper or Carmichael's function $\lambda(n)$ as in most modern implementations for reasons of efficiency. Encryption of $m \in \mathbb{Z}_n = \{0, \ldots, n-1\}$ is performed by computing $c = m^e \bmod n$, while decryption is achieved by $m = c^d \bmod n$. Due to the mathematical symmetry between the public and the private key, RSA can also be used for digital signatures by reversing the roles of encryption and decryption.

Since the introduction of RSA, several variants have been established to improve its efficiency during key generation and decryption, such as multi-prime RSA, where n is a product of three or more distinct primes [2], and restricted multi-power RSA, where n is a product of a prime and a prime power [8]. These variants are useful in scenarios where the advantages of smaller key sizes or faster decryption justify potential security trade-offs – for example, in resource-constrained environments. Although these variants are seemingly related, there is not yet a unified foundation or framework for them. This is where the present paper comes in, which attempts to provide as general a framework as possible for such variants. However, some variants do not fit into this framework, since they rely on different key generation techniques or encryption and decryption methods that defer basically from the standard RSA methods.

Our main result is a generalization of the standard RSA scheme, which can be used with any multi-prime multi-power modulus $n > 1$ and which uses the standard RSA methods for key generation as well as for encryption and decryption. Our generalized RSA scheme is proven to be correct for any message $m \in \mathbb{Z}_n$ which is regular modulo n, meaning that m has a pseudoinverse in the John-von-Neumann sense [5]. This is not a serious restriction, since it turns out that under reasonable assumptions almost all $m \in \mathbb{Z}_n$ are regular modulo n.

The inspiring basis for this paper is the work of Morgado [3, 4] on regular integers modulo n, who investigated them in connection with Euler's totient function $\varphi(n)$. In Section 2 we take up his achievements in a modified form and provide our own evidence to keep this paper self-contained. Section 3 deals with a sharpening of Carmichael's theorem and Euler's theorem, which is used in Section 4 to establish our multi-prime multi-power RSA generalization, along with a proof of correctness and completeness. In Section 5 this multi-prime multi-power generalization is extended to a generalized variant of CRT-RSA, which, in its original form [6], is the preferred way of implementing RSA in practice. In Section 6 it is shown that under reasonable assumptions almost all messages are regular modulo n, thus demonstrating that the restriction to regular messages is negligible. In Section 7 some final conclusions are drawn.

2 Regular integers modulo n

The notion of a regular integer modulo n goes back to Morgado [3], who was inspired by Von Neumann's work on pseudoinverses in regular rings [5].

Definition 1 ([3]). *For any $n \in \mathbb{N}$ we call $m \in \mathbb{Z}$* regular modulo n *if there exists $x \in \mathbb{Z}$ such that $m^2x \equiv m \pmod{n}$. In this case, we refer to x as a* pseudoinverse *of m modulo n. We call $m \in \mathbb{Z}_n$* regular*, if m is regular modulo n.*

It follows from the definition that the regular elements in $\mathbb{Z}_n$ constitute a commutative semigroup with respect to multiplication modulo n containing $\mathbb{Z}_n^* = \{m \in \mathbb{Z}_n \mid \gcd(m, n) = 1\}$ as a subgroup.

The phrase "regular modulo n" is related to the concept of a *unitary divisor* d of n, meaning that $d \mid n$ and $\gcd(d, n/d) = 1$. We use $d \parallel n$ to denote that d is a unitary divisor of n.

Though the following proposition is adopted from Morgado [3, 4], we provide a new proof, which differs considerably from the original in terms of evidence, length and simplicity.

Proposition 1 ([3, 4]). *For any $n \in \mathbb{N}$ and $m \in \mathbb{Z}$ the following statements are equivalent:*

(a) *m is regular modulo n,*
(b) $\gcd(m^2, n) = \gcd(m, n)$,
(c) $\gcd(m, n) \parallel n$.

Proof. (a) $\Rightarrow$ (b): Due to Definition 1 there exists $x \in \mathbb{Z}$ such that $m^2 x \equiv m \pmod{n}$. Thus, $m^2 x + nk = m$ for some $k \in \mathbb{Z}$, whence $\gcd(m^2, n) \mid m$ and hence, $\gcd(m^2, n) = \gcd(m, n)$.

(b) $\Rightarrow$ (c): Clearly, $\gcd(m, n) \mid n$. Since $\gcd(m, n)^2 \mid m^2$ and $\gcd(m^2, n) = \gcd(m, n)$ we find that $\gcd\left(\gcd(m, n), \frac{n}{\gcd(m,n)}\right)$ divides $\gcd\left(\frac{m^2}{\gcd(m,n)}, \frac{n}{\gcd(m,n)}\right)$, which gives 1 and shows that $\gcd(m, n) \parallel n$.

(c) $\Rightarrow$ (a): From $\gcd(m, n) \parallel n$ we deduce $\gcd(\gcd(m, n), n/\gcd(m, n)) = 1$, or equivalently, $\gcd(m, n/\gcd(m, n)) = 1$. By Bezout's lemma, there are $x, y \in \mathbb{Z}$ such that $mx + n/\gcd(m, n)y = 1$. Multiplying both sides of this equation with m gives $m^2 x + nm/\gcd(m, n)y = m$. Finally, reducing both sides modulo n reveals that $m^2 x \equiv m \pmod{n}$, which proves that m is regular modulo n. □

For a standard or multi-prime RSA modulus n, all $m \in \mathbb{Z}_n$ are regular modulo n. This follows from the subsequent statement due to Morgado [3].

Proposition 2 ([3]). *For any $n \in \mathbb{N}$ all integers are regular modulo n if and only if n is squarefree.*

Proof. Since n is squarefree if and only if $\gcd(m^2, n) = \gcd(m, n)$ for all $m \in \mathbb{Z}$, the statement follows from Proposition 1. □

3 A sharpening of Carmichael's theorem and Euler's theorem

As a prerequisite for the following theorem we recall the definition of Carmichael's function and Carmichael's theorem.

Definition 2 ([1]). *For $n \in \mathbb{N}$ with prime factorization $n = p_1^{e_1} \dots p_r^{e_r}$ the* Carmichael function *$\lambda(n)$ is defined by $\lambda(n) = lcm(\lambda(p_1^{e_1}), \dots, \lambda(p_r^{e_r}))$, where $\lambda(1) = \lambda(2) = 1$, $\lambda(3) = \lambda(4) = 2$, $\lambda(2^e) = 2^{e-2}$ if $e > 2$, and $\lambda(p^e) = p^{e-1}(p-1)$ for any odd prime p.*

Proposition 3 ([1]). *For any $n \in \mathbb{N}$ and any $m \in \mathbb{Z}$ which is coprime with n,*

$$m^{\lambda(n)} \equiv 1 \pmod{n}.$$

An equivalent formulation is that for all $m \in \mathbb{Z}$ which are coprime with n, $m^{\lambda(n)+1} \equiv m \pmod{n}$. As the following theorem reveals for $k = 1$, this latter congruence holds if and only if m is regular modulo n. Thus, our theorem sharpens and completes Carmichael's theorem.

Theorem 1. *Let $n \in \mathbb{N}$ and $m \in \mathbb{Z}$. Then, the following statements are equivalent:*

(a) m is regular modulo n.
(b) $m^{k\lambda(n)+1} \equiv m \pmod{n}$ for every $k \in \mathbb{N}$.
(c) $m^{k\lambda(n)+1} \equiv m \pmod{n}$ for some $k \in \mathbb{N}$.

Proof. (a) $\Rightarrow$ (b): If m is regular modulo n, then by Proposition 1, $\gcd(m, n) \parallel n$, which implies that $s = \gcd(m, n)$ and $t = n/s$ are coprime. Thus, the claimed congruence is equivalent to

$$m^{k\lambda(n)+1} \equiv m \pmod{s}, \tag{1}$$
$$m^{k\lambda(n)+1} \equiv m \pmod{t}. \tag{2}$$

Since $s \mid m$, Eq. (1) is obvious. Since $t \mid n$ implies $\lambda(t) \mid \lambda(n)$, Eq. (2) can be rephrased as

$$\left(m^{\lambda(t)}\right)^{k\lambda(n)/\lambda(t)} m \equiv m \pmod{t}. \tag{2'}$$

Since $t \mid n$ we have $\gcd(m, t) = \gcd(m, n, t) = \gcd(\gcd(m, n), t) = \gcd(s, t) = 1$. Therefore, by Carmichael's theorem, $m^{\lambda(t)} \equiv 1 \pmod{t}$, which proves Eq. (2') and thus establishes (b).
(c) $\Rightarrow$ (a): It follows from (c) that $x = m^{k\lambda(n)-1}$ is a pseudoinverse of m modulo n. Thus, by Definition 1, m is regular modulo n, which shows (a). The implication (b) $\Rightarrow$ (c) is trivial. □

As a corollary, we obtain a similar result on the Eulerian φ function, which for $k = 1$ goes back to Morgado [4], whose proof is much more elaborate and based on a two-fold application of Dirichlet's theorem on primes in arithmetic progressions. Similar to how Theorem 1 sharpens and completes Carmichael's theorem, the corollary sharpens and completes Euler's theorem that for any m coprime with n, $m^{\varphi(n)} \equiv 1 \pmod{n}$ or equivalently, $m^{\varphi(n)+1} \equiv m \pmod{n}$.

Corollary 1. *Let $n \in \mathbb{N}$ and $m \in \mathbb{Z}$. Then, m is regular modulo n if and only if $m^{k\varphi(n)+1} \equiv m \pmod{n}$ for every (resp. some) $k \in \mathbb{N}$.*

Proof. Since $\lambda(n)$ divides $\varphi(n)$, we may apply Theorem 1 with $k\varphi(n)/\lambda(n)$ in place of k. □

4 Generalized RSA

Our general multi-prime and multi-power RSA scheme requires a prior selection of the exponents in the prime factorization $n = p_1^{e_1} \dots p_r^{e_r}$ of the modulus. For such a selection, we refer to our scheme as of type $(e_1, \dots, e_r)$. In this sense, the original RSA scheme is of type $(1, 1)$ and the multi-prime schemes are of type $(1, \dots, 1)$. Our generalized RSA scheme is as follows.

Generalized RSA scheme of type $(e_1, \dots, e_r)$*:*

A) Key generation:
1. Randomly choose r distinct primes $p_1, \dots, p_r$.
2. Compute $n = p_1^{e_1} \dots p_r^{e_r}$ and $\nu(n) = \lambda(n)$ (alternatively, $\nu(n) = \varphi(n)$).
3. Choose $1 < e < \nu(n)$ coprime to $\nu(n)$.
4. Compute $1 < d < \nu(n)$ such that $ed \equiv 1 \pmod{\nu(n)}$.
5. Delete $p_1, \dots, p_r$ and $\nu(n)$.
6. (n, e) is the public key.
7. (n, d) is the private key.

B) Encryption and decryption:
1. $\mathrm{enc}(m) = m^e \bmod n$ for any regular $m \in \mathbb{Z}_n$.
2. $\mathrm{dec}(c) = c^d \bmod n$ for any regular $c \in \mathbb{Z}_n$.

Remark 1. As with the original RSA scheme, decryption can be accelerated by applying the Chinese Remainder Theorem (CRT). We come back to this in the next section.

Remark 2. The original RSA scheme [7] and its multi-prime variants [2] are specializations of our generalized scheme, since in these schemes the modulus n is squarefree, whence all $m \in \mathbb{Z}_n$ are regular modulo n by Proposition 2.

The following theorem states that our generalized scheme is *correct* in the sense that it works for all regular messages in $\mathbb{Z}_n$ and *complete* in the sense that it works for no other message.

Theorem 2 (Correctness and Completeness). *Let (n, e) be a public key for the generalized RSA scheme, and (n, d) be the associated private key. Then, for any message $m \in \mathbb{Z}_n$,*

$$\mathrm{dec}(\mathrm{enc}(m)) \equiv m \pmod{n}$$

if and only if m is regular modulo n.

Proof. By step 4 of the key generation phase, $ed = k\nu(n) + 1$ for some $k \in \mathbb{N}$ and hence, $\mathrm{dec}(\mathrm{enc}(m)) = (m^e)^d = m^{k\nu(n)+1}$, which by Theorem 1 (in case $\nu(n) = \lambda(n)$) resp. Corollary 1 (in case $\nu(n) = \varphi(n)$) is congruent to m modulo n if and only if m is regular modulo n. □

In view of Remark 2 the preceding theorem implies the RSA correctness theorem [7], which states that for the original RSA scheme, where n is a product of two distinct primes, $\mathrm{dec}(\mathrm{enc}(m)) \equiv m \pmod{n}$ for any $m \in \mathbb{Z}_n$.

5 Generalized CRT-RSA

Similar to standard RSA [2] we can speed up decryption by applying the Chinese Remainder Theorem, which results in a generalized scheme for CRT-RSA. This generalized scheme requires the distinct prime factors of n and their multiplicities to be added to the private key (n, d), e.g., in the form $(n, d, p_1, \ldots, p_r, e_1, \ldots, e_r)$, where $n = p_1^{e_1} \ldots p_r^{e_r}$ is the prime factorization of n.

Since the regular elements in $\mathbb{Z}_n$ constitute a commutative semigroup with respect to multiplication modulo n, each regular message in $\mathbb{Z}_n$ is encrypted to a regular message in $\mathbb{Z}_n$. With the extended private key above, decryption of a regular message $c \in \mathbb{Z}_n$ works as follows.

Generalized CRT-RSA scheme of type $(e_1, \ldots, e_r)$*:*

1. For $i = 1, \ldots, r$ compute $m_i = c^{d \bmod \nu(p_i^{e_i})} \bmod p_i^{e_i}$ if $p_i \nmid c$, otherwise put $m_i = 0$. (Depending on the key generation phase in Section 4, $\nu = \lambda$ or $\nu = \varphi$.)
2. Find $m = \mathrm{dec}(c)$ by applying the Chinese Remainder Theorem to the system

$$\begin{aligned} m &\equiv m_1 \pmod{p_1^{e_1}} \\ &\vdots \\ m &\equiv m_r \pmod{p_r^{e_r}} \end{aligned}$$

The correctness of this decryption method is justified by the following theorem.

Theorem 3. *Let (n, d) be a private key for the generalized RSA scheme, where $n = p_1^{e_1} \ldots p_r^{e_r}$ is the prime factorization of n. Then, for any regular message $c \in \mathbb{Z}_n$ and any $i = 1, \ldots, r$,*

$$\mathrm{dec}(c) \equiv \begin{cases} c^{d \bmod \nu(p_i^{e_i})} \pmod{p_i^{e_i}}, & \text{if } p_i \nmid c, \\ 0 \pmod{p_i^{e_i}}, & \text{if } p_i \mid c, \end{cases}$$

where ν denotes Carmichael's λ function, respectively Euler's φ function.

Proof. If $p_i \nmid c$, then $\gcd(c, p_i^{e_i}) = 1$. Therefore, by Carmichael's resp. Euler's theorem, $c^{\nu(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}$ and therefore, with $q = \lfloor d/\nu(p_i^{e_i}) \rfloor$,

$$\mathrm{dec}(c) \equiv c^d \equiv (c^{\nu(p_i^{e_i})})^q c^{d \bmod \nu(p_i^{e_i})} \equiv 1^q c^{d \bmod \nu(p_i^{e_i})} \equiv c^{d \bmod \nu(p_i^{e_i})} \pmod{p_i^{e_i}}.$$

If $p_i \mid c$, then $p_i \mid \gcd(c, n)$ and $\gcd(p_i, n/\gcd(c, n)) \mid \gcd(\gcd(c, n), n/\gcd(c, n))$, which equals 1 since, by Proposition 1, $\gcd(c, n) \parallel n$. Thus, $\gcd(p_i, n/\gcd(c, n))$ equals 1 and hence, $p_i^{e_i} \mid \gcd(c, n)$. This implies that $p_i^{e_i} \mid c$, so $c = p_i^{e_i} q$ for some $q \in \mathbb{Z}$, which finally shows that $\mathrm{dec}(c) \equiv c^d \equiv (p_i^{e_i})^d q^d \equiv 0 \pmod{p_i^{e_i}}$. □

6 Almost all messages are regular

In view of our generalized schemes the question arises as to which messages are regular in $\mathbb{Z}_n$, i.e. can be encrypted and decrypted properly. Fortunately, under reasonable assumptions, almost all messages $m \in \mathbb{Z}_n$ are regular modulo n, as the following probabilistic analysis shows.

Theorem 4. *Let $n = p_1^{e_1} \dots p_r^{e_r}$ with distinct k-bit primes $p_1, \dots, p_r$. Then, under uniform distribution, for any random $m \in \mathbb{Z}_n$,*

$$\mathit{Prob}\,[m \textit{ fails to be regular modulo } n] \leq \frac{r}{2^{k-1}}.$$

Proof. Since any $m \in \mathbb{Z}_n^*$ is regular in $\mathbb{Z}_n$, there are at least $\varphi(n)$ regular elements in $\mathbb{Z}_n$. From this, Euler's product formula and the assumption that each p_i is a k-bit prime we obtain

$$\text{Prob}\,[m \text{ is regular modulo } n] \geq \frac{\varphi(n)}{n} = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \geq \left(1 - \frac{1}{2^{k-1}}\right)^r.$$

Thus, for the complementary event we obtain by applying Bernoulli's inequality

$$\text{Prob}\,[m \text{ fails to be regular modulo } n] \leq 1 - \left(1 - \frac{1}{2^{k-1}}\right)^r \leq 1 - \left(1 - \frac{r}{2^{k-1}}\right),$$

from which the claimed inequality immediately follows. □

Remark 3. The bound in Theorem 4 only depends on the number and bit length of the different prime factors of the modulus and not on its exponents.

Sharper bounds could be obtained by considering the number $\varrho(n)$ of regular elements in $\mathbb{Z}_n$ (sequence A055653 in OEIS [9]) and finding strong probability estimates on $\varrho(n)/n$. The formula $\varrho(n) = \sum_{d \| n} \varphi(n)$, which is due to Morgado [3] and which has been proven in different ways by several authors (see e.g., Tóth [10]), could be helpful in this respect.

7 Conclusion

In this paper we presented generalized multi-prime multi-power RSA and CRT-RSA schemes, where key generation as well as encryption and decryption are as in standard RSA. The novelty and significance of our generalized schemes is due to their obvious connection with the concept of regular integers modulo n, which has not yet been investigated in previous research. The restriction of messages to regular integers modulo n is not a serious restriction, since for primes of bit length k in the modulus, almost all messages are regular modulo n if k is large.

Not all RSA variants are specializations of our generalized RSA or CRT-RSA scheme. The Takagi scheme [8], for instance, uses a different kind of key generation and method of encryption and decryption. However, the modulus

$n = p^{b-1}q$ ($b \geq 3$) of the Takagi scheme can be used with our generalized RSA and CRT-RSA schemes, resulting in an error probability for correct decryption of at most $1/2^{k-2}$, when p and q are k-bit primes. As this is vanishingly small for even moderate values of k, say $k = 1024$, such errors will practically never occur. This, however, does not make the Takagi scheme obsolete. Due to its fast key generation and decryption procedure by Hensel lifting it is a highly efficient scheme that has its own raison d'être.

References

1. Carmichael, R.: On composite numbers p which satisfy the fermat congruence $a^{p-1} \equiv 1 \bmod p$. Amer. Math. Monthly **19**, 22–27 (1912)
2. Collins, T., Hopkins, D., Langford, S., Sabin, M.: Public key cryptographic apparatus and method. U.S. Patent 5 848 159 (1997)
3. Morgado, J.: Inteiros regulares módulo n. Gaz. Mat., Lisb. **33**(125-128), 1–5 (1972)
4. Morgado, J.: A property of the euler φ-function concerning the integers which are regular modulo n. Port. Math. **33**, 185–191 (1974)
5. von Neumann, J.: On regular rings. Proc. Natl. Acad. Sci. **22**(12), 707–713 (1936). https://doi.org/10.1073/pnas.22.12.707
6. Quisquater, J.J., Couvreur, C.: Fast decipherment algorithm for rsa public key cryptosystem. Electron. Lett. **18(21)**, 905–907 (1982)
7. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**, 120–126 (1978). https://doi.org/10.1145/359340.359342
8. Takagi, T.: A fast rsa-type public-key primitive modulo $p^k q$ using hensel lifting. IEICE Trans. Fundam. **E87-A**(1), 94–101 (2004)
9. The On-Line Encyclopedia of Integer Sequences (OEIS): Entry A055653 (2025), https://oeis.org/A055653
10. Tóth, L.: Regular integers modulo n. Annales Univ. Sci. Budapest., Sect. Comp. **29**, 263–275 (2008)