The Role of Regular Integers Modulo n in RSA Cryptography

Klaus Dohmen and Mandy Lange-Geisler
Department of Mathematics
Mittweida University of Applied Sciences,
09648 Mittweida, Germany
{dohmen,mlange1}@hs-mittweida.de

August 3, 2026

Abstract. We investigate a multi-prime multi-power generalization of the RSA cryptosystem for arbitrary moduli $n > 1$, which under reasonable cryptographic assumptions works correctly for almost all messages $m < n$. Based on a new sharpening of Carmichael's theorem, tailored to regular integers modulo n, we prove that this generalization is correct precisely for messages represented by regular integers modulo n, thereby generalizing the original RSA correctness theorem. As in the original RSA scheme, decryption can be accelerated by Chinese remaindering, yielding a corresponding generalization of CRT-RSA.

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

1 Introduction

The RSA cryptosystem, introduced by Rivest, Shamir and Adleman [1] 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 computing $m = c^d \bmod n$. 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 [3] or a product of two prime powers [4]. 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.

One of our main results states that in the original RSA scheme and its CRT variant, the modulus $n = pq$ may be replaced by any multi-prime, multi-power modulus $n > 1$ such that, under reasonable cryptographic assumptions, almost all messages are decrypted correctly with high probability. Moreover, we prove that our generalized RSA scheme is correct precisely for regular messages $m \in \mathbb{Z}_n$, thereby generalizing the original RSA correctness theorem. Since almost all messages are regular modulo n, the probabilistic correctness result mentioned above follows.

The inspiration for this paper stems from the work of Morgado [5, 6] on regular integers modulo n, which has largely been overlooked in the cryptographic literature. In Section 2 we build upon his results in a modified form and provide our own proofs to keep this paper self-contained. This section also presents a new sharpening of Carmichael's theorem tailored to regular integers modulo n, which will be used in a later section. In Section 3 we present our multi-prime, multi-power RSA schemes together with a probabilistic correctness result showing that almost all messages are decrypted correctly. In Section 4 we prove that our generalized schemes are correct precisely for messages represented by regular integers modulo n, which generalizes the original RSA correctness theorem. Finally, Section 5 draws some concluding remarks.

2 Regular integers modulo n

The notion of a regular integer modulo n goes back to Morgado [5], who was inspired by Von Neumann's work on pseudoinverses in regular rings [7].

Definition 1 ([5])**.** For every $n \in \mathbb{N}$ we call $m \in \mathbb{Z}$ *regular modulo* n if there exists $x \in \mathbb{Z}$ such that $m^2 x \equiv m \pmod{n}$. 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 adopt Morgado's notation and write $d \mid^* n$ to denote that d is a unitary divisor of n.

Though the following proposition is adopted from Morgado [5, 6], we provide a new proof, which differs considerably from the original in terms of evidence, length and simplicity.

Proposition 1 ([5, 6]). *For every $n \in \mathbb{N}$ 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) $\gcd(m, n) \,|^* n$.

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 $\gcd(m, n) \,|^* n$.

(c) $\Rightarrow$ (a): From $\gcd(m, n) \,|^* n$ we deduce $\gcd(\gcd(m, n), n/\gcd(m, n)) = 1$. Equivalently, this can be stated as $\gcd(m, n/\gcd(m, n)) = 1$. 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 [5].

Proposition 2 ([5]). *For every $n \in \mathbb{N}$, 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. □

As a prerequisite for the following theorem we recall the definition of Carmichael's lambda function (Definition 2) and Carmichael's theorem (Proposition 3).

Definition 2 ([8]). Let $n \in \mathbb{N}$ with prime factorization $n = p_1^{e_1} \dots p_r^{e_r}$. Then, $\lambda(n)$ is defined by

$$\lambda(n) = \operatorname{lcm}(\lambda(p_1^{e_1}), \dots, \lambda(p_r^{e_r})),$$

where

$$\lambda(1) = 1, \quad \lambda(2) = 1, \quad \lambda(4) = 2, \quad \lambda(2^e) = 2^{e-2} \quad (e > 2),$$

and

$$\lambda(p^e) = p^{e-1}(p - 1) \quad (e \geq 1)$$

for all odd primes p.

Proposition 3 ([8]). *For every $n \in \mathbb{N}$ and $m \in \mathbb{Z}$ which is coprime with n,*

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

or equivalently,

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

As the following novel theorem reveals for $k = 1$, this latter congruence holds if and only if m is regular modulo n. Thus, it sharpens and completes Carmichael's theorem.

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

(a) m is regular modulo n.

(b) $m^{k\lambda(n)+1} \equiv m \pmod{n}$ for each $k \in \mathbb{N}$.

(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, $\gcd(m, n) \,|^* n$, 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 Proposition 3, $m^{\lambda(t)} \equiv 1 \pmod{t}$, 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. $\square$

Remark 1. Since $\lambda(n)$ divides Euler's totient function $\varphi(n)$ for every $n \in \mathbb{N}$, the preceding theorem remains valid when $\lambda(n)$ is replaced by $\varphi(n)$. In the special case $k = 1$, this yields a weaker statement originally due to Morgado [6], which sharpens and completes Euler's theorem by establishing the equivalence $m^{\varphi(n)+1} \equiv m \pmod{n}$ if and only if m is regular modulo n. Notably, Morgado's proof is considerably more elaborate, as it relies on a two-fold application of Dirichlet's theorem on primes in arithmetic progressions.

In view of this remark, the results established in the following sections remain valid when $\lambda(n)$ is replaced by $\varphi(n)$.

3 Multi-prime multi-power RSA

We consider a natural generalization of the RSA scheme, where the modulus $n = p_1^{e_1} \cdots p_r^{e_r}$ is composed of r distinct primes $p_1, \ldots, p_r$ with exponents $e_1, \ldots, e_r$. We refer to such a scheme as being of type $(e_1, \ldots, e_r)$. In this sense, the original RSA scheme is of type $(1, 1)$. Our generalized RSA scheme is as follows.

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

A) Key generation:

1. Randomly choose r distinct primes $p_1, \ldots, p_r$.
2. Compute $n = p_1^{e_1} \ldots p_r^{e_r}$ and $\lambda(n)$.
3. Choose $1 < e < \lambda(n)$ coprime to $\lambda(n)$.
4. Compute $1 < d < \lambda(n)$ such that $ed \equiv 1 \pmod{\lambda(n)}$.
5. Delete $p_1, \ldots, p_r$ and $\lambda(n)$.
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 $m \in \mathbb{Z}_n$.
2. $\mathrm{dec}(c) = c^d \bmod n$ for $c \in \mathbb{Z}_n$.

A corresponding generalization of CRT-RSA for accelerating decryption requires the distinct prime factors of n and their multiplicities to be included in the private key, for example in the form

$$(n, d, p_1, \ldots, p_r, e_1, \ldots, e_r),$$

where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n.

While key generalization and encryption are as in the generalized RSA scheme above, decryption of a message $c \in \mathbb{Z}_n$ proceeds as follows.

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

1. For $i = 1, \ldots, r$ compute $m_i = c^{d \bmod \lambda(p_i^{e_i})} \bmod p_i^{e_i}$ if $p_i \nmid c$, otherwise put $m_i = 0$.

2. Find $m = \mathrm{dec}(c)$ by applying the Chinese Remainder Theorem to the system

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

A concrete example

We consider a small example scheme of type $(2, 1, 2)$, which does not provide any real security. We choose $p_1 = 2$, $p_2 = 3$ and $p_3 = 5$, and compute $n = 2^2 3^1 5^2 = 300$ and $\lambda(n) = 20$, following steps 1 and 2 in the key generation phase. We then choose $e = 3$ and compute $d = 7$, according to steps 3 and 4. Our public key is thus $(n, e) = (300, 3)$, and our private key is $(n, d) = (300, 7)$.

In order to encrypt $m = 11$, we compute $\mathrm{enc}(11) = 11^3 \bmod 300 = 131$. Decryption of 131 gives $\mathrm{dec}(131) = 131^7 \bmod 300 = 11$. For $m = 14$, the situation is different:

$\mathrm{enc}(14) = 14^3 \bmod 300 = 44$, while $\mathrm{dec}(44) = 44^7 \bmod 300 = 164$, which is not correct. (The attentive reader will observe that 11 is regular modulo 300, whereas 14 is not.)

In practice, when employing large key sizes, incorrect decryptions are negligibly unlikely, as the following theorem shows.

Theorem 2. *Let $n = p_1^{e_1} \dots p_r^{e_r}$ be a modulus for the generalized (CRT-)RSA scheme with distinct k-bit primes $p_1, \dots, p_r$. Then, under uniform distribution, for each $m \in \mathbb{Z}_n$,*

$$\mathit{Prob}\,[\mathrm{dec}(\mathrm{enc}(m)) \equiv m \pmod{n}] \geq 1 - \frac{r}{2^{k-1}}.$$

We defer the proof of Theorem 2 to Section 4.

Remark 2. Notably, the bound in Theorem 2 depends only on the number and bit length of the distinct prime factors of the modulus, and not on their exponents.

4 Correctness and completeness for regular messages

The following theorem states that our generalized RSA scheme from Section 3 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 3 (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 all messages $m \in \mathbb{Z}_n$,*

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

if and only if m is regular modulo n.

Proof. By step 4 of the key generation phase, $ed = k\lambda(n) + 1$ for some $k \in \mathbb{N}$. Hence, $\mathrm{dec}(\mathrm{enc}(m)) = (m^e)^d = m^{k\lambda(n)+1}$. By Theorem 1, $m^{k\lambda(n)+1} \equiv m \pmod{n}$ if and only if m is regular modulo n. □

Remark 3. The correctness part of Theorem 3 implies the correctness of the original RSA scheme [1], which asserts that if n is a product of two distinct primes, then $\mathrm{dec}(\mathrm{enc}(m)) \equiv m \pmod{n}$ for all $m \in \mathbb{Z}_n$. This implication holds because, for such n, every $m \in \mathbb{Z}_n$ is regular modulo n by Proposition 2.

Since the regular elements in $\mathbb{Z}_n$ form a commutative semigroup with respect to multiplication modulo n, every regular message in $\mathbb{Z}_n$ is encrypted to a regular message in $\mathbb{Z}_n$. For regular messages, the correctness of the CRT decryption method is justified by the following theorem.

Theorem 4. *Let $(n, d, p_1, \dots, p_r, e_1, \dots, e_r)$ be the private key for the generalized CRT-RSA scheme. Then, for every regular message $c \in \mathbb{Z}_n$ and each $i = 1, \dots, r$,*

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

Proof. If $p_i \nmid c$, then $\gcd(c, p_i^{e_i}) = 1$. Hence, by Proposition 3, $c^{\lambda(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}$. Therefore, with $q = \lfloor d/\lambda(p_i^{e_i}) \rfloor$,

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

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, $\gcd(c, n) \mid^* n$. 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 $\mathrm{dec}(c) \equiv c^d \equiv (p_i^{e_i})^d q^d \equiv 0 \pmod{p_i^{e_i}}$. □

The proof of Theorem 2 now follows from Theorems 3 and 4 together with Theorem 5 below.

Theorem 5. *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, the probability that m is regular modulo n is bounded below by $1 - r/2^{k-1}$.*

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

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

Remark 4. Sharper bounds could be obtained by analyzing the number $\varrho(n)$ of regular elements in $\mathbb{Z}_n$ and deriving strong probabilistic estimates for the ratio $\varrho(n)/n$. The sequence $(\varrho(n))_{n \geq 1}$ appears as sequence A055653 in the On-Line Encyclopedia of Integer Sequences (OEIS) [9]. In this context, the formula

$$\varrho(n) = \sum_{d \mid^* n} \varphi(d),$$

originally due to Morgado [5] and re-derived by several authors (see, e.g., [10]), may prove useful.

5 Conclusion

In this paper, we presented generalized RSA and CRT-RSA schemes for arbitrary multi-prime, multi-power moduli $n > 1$, with encryption and decryption as in standard RSA. The novelty and significance of these generalized schemes stem from their connection with the fascinating concept of regular integers modulo n, which has not been investigated in previous cryptographic research. Restricting messages to regular integers modulo n entails no practical disadvantages: for primes of bit length k in the modulus, almost all messages in a probabilistic sense are correctly decrypted.

Despite the generality of our RSA schemes, not all multi-prime multi-power variants are special cases of our constructions. The Takagi scheme [3], for instance, as well as its

generalization by Lim et al. [4], employ a different key generation procedures as well as distinct encryption and decryption methods, which only work for messages $m \in \mathbb{Z}_n^*$—a proper subset of the set of regular integers modulo n. However, the modulus $n = p^{b-1}q$ ($b \geq 3$) used in the Takagi scheme (similar for $n = p^r q^s$ in the scheme by Lim et al.) can be safely employed with our generalized RSA and CRT-RSA schemes, resulting in a decryption error probability of at most $1/2^{k-2}$ for messages $m \in \mathbb{Z}_n$, when p and q are k-bit primes. Since this probability is already negligible for moderate values of k (e.g., $k = 512$), such errors can be safely disregarded in practice.

Regarding the security of our generalized RSA and CRT-RSA schemes, we refer to the extensive investigations by Lim et al. [4] on moduli of the form $n = p^r q^s$, for various values of r and s, with respect to factorization attacks.

References

[1] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 1978;21:120–126. doi: https://doi.org/10.1145/359340.359342.

[2] Collins T, Hopkins D, Langford S, Sabin M. Public Key Cryptographic Apparatus and Method. U.S. Patent US5848159, 1997.

[3] Takagi T. A fast RSA-type public-key primitive modulo $p^k q$ using Hensel lifting. IEICE Trans Fundam 2004;E87-A(1):94–101.

[4] Lim S, Kim S, Yie I, Lee H. A Generalized Takagi-Cryptosystem with a Modulus of the Form $p^r q^s$. In: Roy B, Okamoto E (eds) Progress in Cryptology – INDOCRYPT 2000. Lecture Notes in Computer Science, vol 1977, 2000. Springer, Berlin, Heidelberg. `https://doi.org/10.1007/3-540-44495-5_25`

[5] Morgado J. Inteiros regulares módulo n. Gaz Mat Lisb 1972;33(125–128):1–5.

[6] Morgado J. A property of the Euler φ-function concerning the integers which are regular modulo n. Port Math 1974;33:185–191.

[7] von Neumann J. On regular rings. Proc Nat Acad Sci 1936;22:707–713. doi: https://doi.org/10.1073/pnas.22.12.707.

[8] Carmichael RD. On composite numbers p which satisfy the Fermat congruence $a^{p-1} \equiv 1 \bmod p$. Amer Math Monthly 1912;19(2):22–27. doi: https://doi.org/10.2307/2972687.

[9] The On-Line Encyclopedia of Integer Sequences. The OEIS Foundation Inc; https://www.oeis.org [Accessed 30 Apr 2026].

[10] Tóth L. Regular integers modulo n. Ann Univ Sci Budapest Sect Comp 2008;29:263–275.