information

MDPI

Article

Composite Numbers That Give Valid RSA Key Pairs for Any Coprime p

Barry Fagin

Department of Computer Science, US Air Force Academy, Colorado Springs, CO 80840, USA; barry.fagin@usafa.edu; Tel.: +1-719-339-4514

Received: 13 August 2018; Accepted: 25 August 2018; Published: 28 August 2018

Abstract: RSA key pairs are normally generated from two large primes p and q. We consider what happens if they are generated from two integers s and r, where r is prime, but unbeknownst to the user, s is not. Under most circumstances, the correctness of encryption and decryption depends on the choice of the public and private exponents e and d. In some cases, specific (s, r) pairs can be found for which encryption and decryption will be correct for any (e, d) exponent pair. Certain s exist, however, for which encryption and decryption are correct for any odd prime $r \nmid s$. We give necessary and sufficient conditions for s with this property.

Keywords: cryptography; abstract algebra; RSA; computer science education; cryptography education

MSC: [2010] 11Axx 11T71

1. Notation and Background

Consider the RSA public-key cryptosystem and its operations of encryption and decryption [1]. Let (p, q) be primes, $n = p * q$, $\phi(n) = (p-1)(q-1)$ denote Euler's totient function and (e, d) the encryption/decryption exponent pair chosen such that $ed \underset{\phi(n)}{\equiv} 1$. Let $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* = U_n$ be the group of units mod n, and let $a \in U_n$. Encryption and decryption operations are given by:

$$(a^e)^d \equiv (a^{ed}) \equiv (a^1) \equiv a \bmod n$$

We consider the case of RSA encryption and decryption where at least one of (p, q) is a composite number s. This situation might arise in the presence of a flawed primality tester or in the classroom when a teacher wishes to demonstrate in RSA what happens if one of (p, q) is not a true prime. This is the context in which this question arose for the author. Security in this case is obviously weaker, since the modulus is now easier to factor, but how is correctness affected?

First, we note that RSA can be implemented using n as the product of multiple primes, with the Chinese remainder theorem used to recover the message [2]. In multi-prime RSA, (e, d) are chosen such that $ed \underset{\phi(n)}{\equiv} 1$, just as with two-prime RSA. The only difference is that the totient function $\phi(n) = (p-1)(q-1)$ can no longer be used. For example, for three-prime RSA with primes (p, q, r), the totient function is given by $\phi(n = pqr) = (p-1)(q-1)(r-1)$.

For a composite number s (that the user incorrectly believes is prime) and a true prime r used to generate keys with standard two-prime RSA, encryption and decryption exponents would be chosen using the (incorrect) pseudo-totient $\phi'(n = sr) = (s-1)(r-1)$, choosing (e, d) such that $ed \underset{\phi'(n)}{\equiv} 1$. In this case, encryption and decryption are given by:

$$(a^e)^d \underset{n=sr}{\equiv} (a^{ed}) \underset{n=sr}{\equiv} x$$

where x is no longer mathematically guaranteed to be a.

Given the conditions above, under what circumstances will we have $(a^e)^d \equiv a$? Is correct RSA even possible given the use of the wrong totient function? We investigate this question here.

2. Witnesses for Tuples (s, r, e, d)

Let n, e, d, a, s, r be as described. Let $ord(a)$ denote the order of a in U_n. Let us call the fraction of elements of U_n, the order of which does not divide $(ed - 1)$ the witness ratio of (s, r, e, d). For these elements $(a^e)^d \not\equiv a$; they testify to the composite nature of s. Tuples (s, r, e, d) with a witness ratio of zero are said to be witness-free. For RSA encryption with those values, the composite nature of s will never be detected.

Example

Consider $s = 10, r = 7$. We have $n = 10 * 7 = 70, \phi'(n) = (s - 1)(r - 1) = 54$. The elements of U_n are:

$$U_n = 1, 3, 9, 11, 13, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 51, 53, 57, 59, 61, 67, 69$$

The set of orders of $a \in U_n$ is:

$$O_n = 1, 2, 3, 4, 6, 12$$

Suppose we choose $e = 35, d = 17$ as our exponent pair. We have $ed = 595 \underset{\phi'(n)}{\equiv} 1, (ed - 1) = 594$. The element $a = 9$ will be encrypted correctly, because $ord(9) = 6$ and $6 \mid 594$. The element $a = 13$, by contrast, is a witness because $ord(13) = 4$ and $4 \nmid 594$. As a check, $9^{595} \underset{70}{\equiv} 9$, but $13^{595} \underset{70}{\equiv} 27 \neq 13$.

For this combination of (s, r, e, d), the values of a = (1, 9, 11, 19, 29, 31, 39, 41, 51, 59, 61, 69) all have orders in U_n that divide $(ed - 1) = 594$, which means they will encrypt and decrypt correctly. The remaining values of a = (13, 17, 23, 27, 33, 37, 43, 47, 53, 57, 67) do not. These values serve as witnesses to the composite nature of s. Since both sets are of identical cardinality, the witness ratio for $(s, r, e, d) = (10, 7, 35, 17)$ is 0.5, so we might say the impostor $s = 10$ masquerading as a prime has a 50% chance of escaping detection. This assumes only a single element is encrypted. For all (s, r, e, d) that are not witness-free, the chances of an impostor s escaping detection decrease with the length of the message. Similar calculations will show that for $(s, r, e, d) = (35, 17, 5, 109)$, the witness ratio is 2/3, and for $(s, r, e, d) = (437, 29, 29, 421)$, the witness ratio is 0.99.

3. Witness-Free Tuples (s, r, e, d)

Let $\lambda(n)$ denote the Carmichael function, the maximum order of any element in U_n. By Lagrange's theorem, and the fact that for integers a and b, $a \mid b \leftrightarrow$ all divisors of $a \mid b$, we see that those tuples (s, r, e, d) with the property $\lambda(n) \mid (ed - 1)$ are exactly those that are witness-free.

For example, suppose we keep $(s = 10, r = 7)$ from above, but now choose $e = 11, d = 59$. We have $(ed - 1) = 648$. Recall $O_n = 1, 2, 3, 4, 6, 12$. All elements of O_n now divide $(ed - 1) = 648$, so $(s, r, e, d) = (437, 29, 29, 421)$ is witness-free. For example, $9^{649} \underset{70}{\equiv} 9, 31^{649} \underset{70}{\equiv} 31, 57^{649} \underset{70}{\equiv} 57$, etc.

Equivalently, (s, r, e, d) is witness-free when (e, d) with $ed \underset{\phi'(n)}{\equiv} 1$ also posses the property $ed \underset{\phi(n)}{\equiv} 1$. For a given (s, r) with $n = sr$, such (e, d) can always be found by computing L = $lcm(\phi(n), \phi'(n))$ and finding $ed \underset{L}{\equiv} 1$. Such a procedure will by construction give $ed \underset{\phi'(n)}{\equiv} 1$ and $ed \underset{\phi(n)}{\equiv} 1$, yielding an (s, r, e, d) that is witness-free.

For example, consider the semiprimes $s = 257 * 263, r = 269 * 271$. We have:

$$\begin{aligned}
&n = 4927316309\\
&s = 67591\\
&r = 72899\\
&\phi'(n) = 4927175820\\
&\phi(n) = 4853329920\\
&L = lcm(\phi'(n), \phi(n)) = 132851165712814080
\end{aligned}$$

Trying $k = 1$, we have:

$$kL + 1 = 132851165712814081 = 13 * 19 * 537858970497223$$

Choosing $e = 13 * 19 = 247, d = 537858970497223$, we have $(67591, 72899, 247, 537858970497223)$ as a witness-free tuple. For example,

$$\begin{aligned}
3^{132851165712814081} &\underset{4927316309}{\equiv} 3\\
150^{132851165712814081} &\underset{4927316309}{\equiv} 150\\
246^{132851165712814081} &\underset{4927316309}{\equiv} 246\\
&etc.
\end{aligned}$$

Since all the primes chosen were >256, if our RSA message consisted of ASCII text encrypted at the byte level (inefficient, but suitable for illustrative purposes), using the above values of (s, r, e, d), two-prime RSA encryption and decryption would work correctly. This is true even though neither s nor r are prime and even though e and d were chosen using the pseudo-totient.

4. Witness-Free Tuples (s, r)

It is possible in some cases to remove the effects of e and d. For those cases, (s, r, e, d) is witness-free for any $ed \underset{\phi'(n=sr)}{\equiv} 1$. For these tuples the composite nature of s cannot be detected solely through RSA encryption and decryption, regardless of the elements encrypted and the public and private exponents chosen.

Theorem 1. *Let s, r be positive integers, $n = sr, \phi'(n) = (s-1)(r-1)$. (s, r) is witness-free $\leftrightarrow \lambda(n) \mid \phi'(n)$.*

Proof. $\rightarrow$: Assume (s, r) is witness-free for all $ed \underset{\phi'(n=sr)}{\equiv} 1$. Let $a \in U_n$ be of order k. We have $ed = 1 + m\phi'(n)$ from some integer $m \geq 0$. Write $\phi'(n)$ as $lk + r$ with $l \geq 0$ and $0 \leq r < k$. We have:

$$a^{ed} \underset{n}{\equiv} a^{1+m\phi'(n)} \underset{n}{\equiv} a^{1+m(lk+r)} \underset{n}{\equiv} a\left(a^{lk+r}\right)^m$$

$$\underset{n}{\equiv} a(a^k)^{lm}(a^{mr}) \underset{n}{\equiv} a1^{lm}(a^{mr}) \underset{n}{\equiv} a(a^{mr}) \underset{n}{\equiv} a(a^m)^r$$

Assume r is non-zero. Since $r < k$, there is no element b in U_n for which $b^r \underset{n}{\equiv} 1$. Therefore, $(a^m)^r \underset{n}{\not\equiv} 1$, which means $a^{ed} \underset{n}{\not\equiv} a$, contradicting our assumption that (s, r) is witness-free. Therefore, $r = 0$, implying $k \mid \phi'(n)$; therefore, $\lambda(n) \mid \phi'(n)$.

$\leftarrow$: Let $\lambda(n) \mid \phi'(n)$. Let $a \in U_n$ be of order k. Since $k \mid \lambda(n), k \mid \phi'(n)$, we can write $lk = \phi'(n)$, $l > 0$. We have $ed \underset{\phi'(n)}{\equiv} 1$ for any (e, d) pair, so $ed = 1 + m\phi'(n)$ for some integer $m \geq 0$. This gives:

$$a^{ed} \underset{n}{\equiv} a^{1+mlk} \underset{n}{\equiv} a(a^k)^{lm} \underset{n}{\equiv} a(1^{lm}) \underset{n}{\equiv} a$$

Therefore, (s, r) is witness-free for all $ed \underset{\phi'(n=sr)}{\equiv} 1$. □

Example

For $s = 10, r = 17, n = sr = 170 = 2 * 5 * 17, \lambda(170) = 16, \phi'(n) = 9 * 16 = 144 = \lambda(170) * 9$. By Theorem 1, $(10, 17)$ is witness-free. For any $ed \underset{144}{\equiv} 1$ and any $a \in U_{170}$, we will have $a^{ed} \underset{n}{\equiv} a$. For example, $11^{145} \underset{170}{\equiv} 11, 121^{289} \underset{170}{\equiv} 121$, etc.

For $s = 10, r = 23$, we have $n = 2 * 5 * 23 = 230, \lambda(230) = 44, \phi'(n) = 9 * 22 = 192, 44 \nmid 192$. By Theorem 1, $(10, 23)$ has witnesses. For example, $13^{385} \underset{230}{\equiv} 93 \neq 13$.

5. Values of s That Yield Witness-Free Tuples for All Odd Primes r

Certain values of s can be constructed such that they can be paired with any odd prime r to produce correct RSA key pairs. The properties of s required by Theorem 1 will hold for all primes $r \leftrightarrow \forall k \in O_s, k \mid (s-1)$, i.e., $\forall a \in U_s, a^{s-1} \underset{s}{\equiv} 1$. This is the definition of a Carmichael number. Thus, any pair (C, r) where C is a Carmichael number and r is a prime will produce functioning RSA keys. This is a known result.

However, if we relax the requirements on s just slightly, so that only pairings with odd primes are of interest, then non-Carmichael numbers can also meet the requirements. Let s be a composite number such that Theorem 1 holds for all odd primes $r \nmid s$. We refer to all such s as strong impostors. We use the modifier strong to indicate that (s, r) is witness-free for all odd primes $r \nmid s$, as opposed to one or a few specific (s, r) that are witness-free.

Theorem 2. *s is a strong impostor $\leftrightarrow \lambda(s) \mid 2(s-1)$.*

Proof. $\rightarrow$: Assume s is a strong impostor. Then, by Theorem 1, for all odd primes $r, \lambda(sr) \mid \phi'(sr) \rightarrow \lambda(sr) \mid (s-1)(r-1)$. Since $\lambda(sr) = lcm(\lambda(s), r-1)$, we have $lcm(\lambda(s), r-1) \mid (s-1)(r-1)$. This holds for all odd primes r, including three, so $lcm(\lambda(s), 2) \mid 2(s-1)$. Since the Carmichael function is even for n > 2, the result follows.

$\leftarrow$: Assume $\lambda(s) \mid 2(s-1)$. Let r be an odd prime. We have $\lambda(sr) = lcm(\lambda(s), r-1) = lcm(2(s-1)k, r-1)$ for some positive integer k. This quantity must divide $(s-1)(r-1)$, and the result follows. □

5.1. Example

The first sixteen strong impostors are:

$$\{4, 6, 8, 12, 15, 24, 28, 66, 91, 276, 435, 532, 561, 616, 703, 946\}$$

(note that the 13th strong impostor, 561, is the first Carmichael number). For any of these numbers s, all tuples (s, r) with r an odd prime and $r \nmid s$ will be witness-free. For example, consider $(s, r) = (66, 179)$. $n = 66 * 179 = 11{,}814$, $\phi'(n) = 65 * 178 = 11{,}570$. Choosing $e = 21, d = 551$, $ed = 11{,}571$, we have $5^{11{,}571} \underset{11{,}814}{\equiv} 5, 91^{11{,}571} \underset{11{,}814}{\equiv} 91$, and so forth. The same results will hold for any odd prime $r \nmid s$, any $ed \underset{\phi'(n=rs)}{\equiv} 1$ and any $a \in U_n$.

5.2. The Structure of Strong Impostors

We can say a couple of things about the structure of strong impostors. First, we note that the exponent of two in their prime factorization is always ≤ 3, and the exponents of all odd primes in their prime factorization are always ≤ 1.

Theorem 3. *Let $s = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$ be a strong impostor, where the primes appear in numerical order and all $e_i \geq 0$. Then, $e_1 \leq 3$, and $\forall i > 1\ e_i <= 1$.*

Proof. Suppose s is an even strong impostor, i.e., $e_1 \geq 1$. By Theorem 2, $\lambda(s) \mid 2(s-1)$.

If $e_1 \leq 2$, we have:

$$\lambda(s) = lcm(2^{e_1-1}, p_2^{e_2-1}(p_2-1) \dots p_m^{e_m-1}(p_m-1))$$

By the properties of the least common multiple, the exponents of all primes p_i in the number above must be $\geq e_i - 1$, and the number itself must divide $2(s-1)$. We have:

$$2(s-1) = 2^{e_1+1} p_2^{e_2} \dots p_m^{e_m} - 2$$

We see by inspection that for all odd primes p_i, no $p_i^{e_i-1}$ can divide $2(s-1)$ if $e_i > 1$, as there will always be a remainder of -2. For $p_1 = 2, 2^{e_1-1}$ can divide $2(s-1)$ only if $e_1 = 1$ or $e_1 = 2$. Therefore, if s is an even strong impostor with $e_1 \leq 2$, we have $\forall\, i > 1\ e_i \leq 1$.

If s is even, but with $e_1 > 2$, we have:

$$\lambda(s) = lcm(2^{e_1-2}, p_2^{e_2-1}(p_2-1) \dots p_m^{e_m-1}(p_m-1))$$

s is unchanged, so the same restrictions on the exponents of odd primes still apply. Applying similar reasoning as before, 2^{e_1-2} can divide $2(s-1)$ only when $e_1 = 2$ or $e_1 = 3$. Therefore, the theorem holds for even strong impostors.

Now, suppose that s is odd. Then:

$$\lambda(s) = lcm(p_2^{e_2-1}(p_2-1), \dots, p_m^{e_m-1}(p_m-1))$$

As before, we require $\lambda(s) \mid 2(s-1)$. We have $s - 1 = p_2^{e_2} \dots p_m^{e_m} - 1$. Since s only contains odd primes, the same conditions are required on its odd prime exponents for $\lambda(s)$ to divide $2(s-1)$. Thus, for all strong impostors, the exponent of two in their prime factorization is ≤ 3, and the exponents of all odd primes are ≤ 1. □

It follows that all odd strong impostors are square-free, and all even strong impostors are free of squares > 4. These s when multiplied by any prime $r \nmid s$ produce non-square-free moduli that yield valid RSA key pairs and witness-free tuples for any $ed \underset{\phi'(n=rs)}{\equiv} 1$.

5.3. Example

Here is the prime factorization of the first eight strong impostors:

$$\begin{aligned} 4 &= 2^2 \\ 6 &= 2 * 3 \\ 8 &= 2^3 \\ 12 &= 2^2 * 3 \\ 15 &= 3 * 5 \\ 24 &= 2^3 * 3 \\ 28 &= 2^2 * 7 \\ 66 &= 2 * 3 * 11 \end{aligned}$$

Note that there are no non-unitary powers of odd primes, and their maximum power of two is three.

We can also see that no strong impostor s can contain an odd prime pair (p_i, p_j) in its factorization such that $p_j \underset{p_i}{\equiv} 1$. This is because if $p_j = kp_i + 1$ appears in the prime factorization of s, we will have $\phi(p_j) = kp_i$, so p_i will appear somewhere in $\lambda(s)$. No such p_i can divide $2(s-1)$ evenly. Thus, no s that contains three in its prime factorization can contain any of the primes $\{7, 13, 19, 31...\}$, no s that containing five can contain any of $\{11, 31, 41, 61...\}$, etc. This is perhaps more clearly seen in the prime factorization of the next eight strong impostors:

$$\begin{aligned} 91 &= 7 * 13 \\ 276 &= 2^2 * 3 * 23 \\ 435 &= 3 * 5 * 29 \\ 532 &= 2^2 * 7 * 19 \\ 561 &= 3 * 11 * 17 \\ 616 &= 2^3 * 7 * 11 \\ 703 &= 19 * 37 \\ 946 &= 2 * 11 * 43 \end{aligned}$$

In addition to the exponents of the primes in the factorization of s, we can say the following things about the primes themselves.

Theorem 4. *Let $s = 2^j p_2 p_3 \dots p_m$, where all p_i are odd primes. s is a strong impostor $\leftrightarrow \forall p_i \mid s, p_i - 1 \mid 2(2^j \prod_{k \neq i} p_k - 1)$.*

Proof. Let s be a strong impostor as described. By Theorem 2, $\lambda(s) \mid 2(s-1)$. We can write s as $s = 2^j \prod_{i=1}^{m} p_i$. Since s is a strong impostor, we must have $(p_i - 1) \mid 2(s-1) \leftrightarrow \forall p_i \mid s$, $(p_i - 1) \mid 2(2^j \prod_{i=1}^{m} p_i - 1) \leftrightarrow (p_i - 1) \mid 2^{j+1} \prod_{i=1}^{m} p_i - 2$. Performing the first step of division by an arbitrary $p_i - 1$, we obtain $s = 2^{j+1} \prod_{i=1}^{m} p_i - 2 = (p_i - 1) * 2^{j+1} \prod_{k \neq i}^{m} p_k + (2^{j+1} \prod_{k \neq i}^{m} p_k - 2)$. Since the latter term is the remainder and must also be evenly divisible by $p_i - 1$ and since the choice of p_i was arbitrary, the result follows. □

5.4. Example

Consider $s = 2926 = 2 * 7 * 11 * 19$. We have $(7-1) \mid 2(2 * 11 * 19 - 1)$, $(11-1) \mid 2(2 * 7 * 19 - 1)$ and $(19-1) \mid 2(2 * 7 * 11 - 1)$. The reader can verify similar results for the first 16 strong impostors presented above.

Put another way, the strong impostors are exactly those $s = 2^j p_2 p_3 \ldots p_m$ where $0 \leq j \leq 3$, and the set of m-1 simultaneous linear congruences $2(2^j \prod_{k \neq i} p_k - 1) \underset{p_i - 1}{\equiv} 0$ has a solution in odd primes p_i.

6. Semiprime Strong Impostors

Impostors can be strong in the sense of producing valid RSA encryption and decryption, while still being easily detected by inspection or the presence of small factors. For example, strong impostors that are even are obviously composite, as are those ending in five or those, the digits of which sum to a multiple of three. Impostors for which the effectiveness of such simple detection techniques is minimized are semiprimes $s = pq$, where p and q are both prime (three of these appear in the first 16 strong impostors above). These impostors are also the hardest to factor. The reader may have noticed that all the semiprime strong impostors shown are prime pairs of the form $(p, 2p-1)$. This is in fact always the case.

Theorem 5. *Let p, q be distinct odd primes, $p < q$. $s = pq$ is a strong impostor $\leftrightarrow q = 2p - 1$.*

Proof. This result is a special case of Theorem 4, with $j = 0$ and $m = 3$. Plugging in these values, we obtain $p_2 - 1 \mid 2(p_3 - 1)$ and $p_3 - 1 \mid 2(p_2 - 1)$. Assume $p_2 < p_3$, and apply a change of variables with $x_2 = p_2 - 1, x_3 = p_3 - 1$. The equations then become $x_2 \mid 2x_3$ and $x_3 \mid 2x_2$. Let $2x_3 = k_1 x_2, 2x_2 = k_2 x_3$. These two equations together imply $k_1 * k_2 = 4$. Since x_2 and x_3 are distinct, we discard the solution $k_1 = k_2 = 2$. Since $x_2 < x_3$, we have $k_1 = 4, k_2 = 1, \rightarrow 2x_2 = x_3 \rightarrow 2(p_2 - 1) = (p_3 - 1) \rightarrow p_3 = 2p_2 - 1$. □

6.1. Example

$(2,3), (3,5), (7,13)$ (as shown previously) and $(19,37)$ are the first four (p,q) prime pairs such that $q = 2p - 1$. Therefore, $s = 6(2 * 3), s = 15(3 * 5), s = 91(7 * 13)$, and $s = 703(19 * 37)$ are the first four semiprime strong impostors.

6.2. Unmasking a Semiprime Strong Impostor

Semiprime strong impostors $s = pq$ are among the most resistant to probabilistic primality tests, because they approach the Rabin limit of $s/4$ bases [3] to which they are strong semiprimes. Nonetheless, $s/4$ remains a small proportion, so like any composite, they will quickly fail probabilistic primality tests like Miller–Rabin. If RSA key generation is implemented properly, there is no worry about a strong impostor slipping through.

There is also a way to unmask a strong impostor s that yields its factors. We have $s = pq = p(2p-1) = 2p^2 - p$, which means $2p^2 - p - s = 0$. s is known, so applying the quadratic formula and considering only the positive solution, we have $p = \frac{1+\sqrt{1+8s}}{4}$. Thus, if you suspect s of being a semiprime strong impostor, multiply it by eight, add one and take the square root. If the result is an integer $\underset{4}{\equiv} 3$, you have caught the impostor red-handed.

7. Constructing Strong Impostors

Theorem 4 and similar results above provide insights into the structure of strong impostors that can be used to construct them. For example, it can be shown that for any even strong impostor, all its odd prime factors are congruent to three mod four. We offer the following additional results for odd

primes p_i, some without proof, but with examples to aid understanding. Proofs can be obtained by combining the specific criteria below with the definition of a strong impostor.

(A) $s = \prod(p, 2p-1)$
(B) $s = \prod(p_1, \ldots, p_m)\ lcm(p_1 - 1, \ldots, p_m - 1) \mid 2(s-1)$
(C) $s = \prod(p, b(p-1)+1, c(p-1)+1)\ lcm(b,c) | 2(pb+pc+1)$
(D) $s = \prod(6k+1, 12k+1, 18k+1, mk+1)\ 36 \mid m, m \mid 72(36k^2+11k+1)$

We have already shown Condition A to be the definition of a two-factor strong impostor; Condition B is the general definition. These are the simplest ways to find strong impostors: sift through the required number of primes until those meeting the required condition are found.

Condition C applies to prime three-tuples that are separated by multiples of $p-1$. Thus, to generate a strong impostor from a prime p, if $b = 2$ does not yield a prime (i.e., Condition A fails), keep incrementing b until a prime of the form $b(p-1)+1$ is found. Then, do the same starting at $c = b+1$. Once $p_2 = b(p-1)+1$ and $p_3 = c(p-1)+1$ are found, apply the indicated lcm criterion. If that fails, continue searching with increasing b and c. For example, $p = 4, b = 4, c = 7$ produce $(5, 17, 29)$, all of which are prime. $lcm(4,7) = 28$ and $28 \mid 2(5*4+5*7+1)$, so $s = 15*17*29 = 2465$ is a strong impostor.

Condition D describes the possible construction of a strong impostor from a Carmichael number of a specific form. $s = \prod(p_1, p_2, p_3) = \prod(6k+1, 12k+1, 18k+1)$ is a Carmichael number for prime p_1, p_2, p_3 [4]. Such a number can be multiplied by a prime of the form $mk+1$ to produce a non-Carmichael strong impostor if an m meeting the indicated criteria can be found. For example, $k = 6, (37, 73, 109)$ are all prime, and therefore, $s = 37*73*109 = 294{,}409$ is Carmichael number. $m = 72$ is the smallest m that meets the criteria of Condition D, and $mk+1 = 72*6+1 = 433$ is prime. Therefore, $s = 294{,}409 * 433 = 127{,}479{,}097$ is a strong impostor.

The author has tested all Carmichael numbers of the indicated form with $k \leq 2^{20}$. Approximately 85% yield strong impostors using this technique.

8. Conclusions and Open Problems

There are 2946 strong impostors below 2^{32}; 2797 are odd, and 149 are even. In this range, true primes are about 2000-times more common than strong impostors. Of the strong impostors, 630 are semiprimes. The number of strong impostors in this range with one through seven factors are $\{2, 630, 498, 1004, 678, 131, 2\}$, respectively. Four and eight are the only strong impostors with one prime factor. The strong impostors with seven factors are 370,851,481 = 7*11*13*17*19*31*37 and 2,719,940,041 = 7*13*17*19*37*41*61. We see by construction that the density of strong impostors is greater than that of the Carmichael numbers, but less than that of the primes. The largest strong impostor known to the author was found using the criteria of Condition D, with k = 1,044,381 and m = 2,827,177,323,983,136. This gives:

$$\begin{aligned} s &= (6k+1)(12k+1)(18k+1)(2,827,177,323,983,136*1044381+1) \\ &= 4,359,071,840,350,709,426,134,393,773,581,398,480,999,153 \end{aligned}$$

Since there is an infinite number of Carmichael numbers [5], there is an infinite number of strong impostors. The author conjectures there is an infinite number of non-Carmichael strong impostors. This is related to well-known conjectures on prime constellations [6]. For example, proving there is an infinite number of two-factor strong impostors would prove there is an infinite number of $(p, 2p-1)$ prime pairs.

For a given p, we might ask if a strong impostor s exists containing p as its smallest factor. We refer to such an s as an extension of p. While extensions have been found by the author for the first 256 primes, it is an open question whether every prime has an extension. Proving this would of course prove there is an infinite number of non-Carmichael strong impostors.

Similar open questions exist for non-Carmichael strong impostors of various forms, such as prime three-tuples in arithmetic progression of the form $(p, p + 6m, p + 12m)$ where $p = 6k + 1$. Examples of strong impostors of this form for $p >= 67$ are currently unknown.

It is an open question whether an infinite number of Carmichael numbers of the form $(6k + 1, 12k + 1, 18k + 1)$ [7] can be extended to non-Carmichael strong impostors using the technique of Condition D.

We have seen the that largest prime factor of a strong impostor must be less than twice the product of the other prime factors. This means the computations required to determine if criteria for Conditions B and C are met for a given input will terminate if the largest prime in the tuple is specified, or if all primes except the largest are specified. For all other cases, termination is not guaranteed. This relates to the open questions above.

Modern implementations of RSA use $\lambda(n)$ instead of $\phi(n)$ in the selection of (e, d). A similar substitution may be made in the examples here, with appropriate algebraic modifications as needed.

Finally, efficient algorithms for finding the smallest extension for a given prime p would be interesting to explore, as well as a deeper understanding of the relationships between each p_i of a strong impostor beyond that presented here.

Funding: Support for this work was provided in part by the Air Force Office of Scientific Research under Grant #1220961 and by the US Air Force Academy Department of Computer Science.

Acknowledgments: The author wishes to thank both his students and his department colleague Carlos Salazar for asking interesting questions, and for Karl Herzinger of the USAFA Department of Mathematics for his assistance and review of this manuscript.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystem. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Hinek, M. *Cryptanalysis of RSA and Its Variants*; CRC Press: Boca Raton, FL, USA, 2010; p. 33487.
3. Rabin, M. Probabalistic Algorithm for Testing Primality. *J. Number Theory* **1980**, *12*, 128–138. [CrossRef]
4. Chernick, J. On Fermat's Simple Theorem. *Bull. Am. Math. Soc.* **1935**, *45*, 269–274. [CrossRef]
5. Alford, W.; Granville, A.; Pomerance, C. There are Infinitely Many Carmichael Numbers. *Ann. Math.* **1994**, *140*, 703–722. [CrossRef]
6. Hardy, G.; Littlewood, E. Some Problems of 'Partitio Numerorum'. III. On the Expression of a Number as a Sum of Primes. *Acta Math.* **1923**, *44*, 1–70. [CrossRef]
7. Dubner, H. Carmichael Numbers of the Form (6m + 1)(12m + 1)(18m + 1). *J. Integer Seq.* **2002**, 5, 02.2.1.