The RSA Cryptosystem: History, Algorithm, Primes

Michael Calderbank

August 20, 2007

Contents

1 Introduction

Ever since people began to write down events in their lives, there has been a need for cryptography. Cryptography is the encryption of text in such a manner that outsiders to the code cannot understand the code, but the desired reader is able to decrypt the encryption so as to understand the message. For early man, just as for modern man, there has always been a need for secrecy, because it is usually in the interest of both the decoders and encoders that the information not be known to the general public. In times of war, it is essential that the enemy not know what you and your allies are plotting, because winning or losing a war can hinge on the secrecy of the operations so as to surprise the enemy. However, there was one caveat to all the cryptosystems before RSA: they were all based on the fact that both the decoding and encoding parties had to know the method of encryption and the key to decrypting the cipher. In truth, this problem of key distribution is the same problem people were trying to solve when they invented cryptography: the keys and the method of decryption need to be relayed to all the desired readers of the message, but how does one relay the key securely? Why, with encryption, of course. But, then how to you send the key to the encryption of the key to the encryption of the message? As you can see, this caveat of cryptography is an infinite loop between encryption and key distribution that cannot be solved with security ensured for all the desired readers. Indeed, the Germans might have won the war had it not been for the fact that they had to print out their daily settings for the Enigma machine and hand them out to all the Nazi leaders. One of the key-books was intercepted by the English and this led to a crucial defeat for the Germans that crippled their submarine fleet. Anyways, the problem of key distribution remained a problem until the 20th century.

The problem was solved by Whitfield Diffie, working in collaboration with Martin Hellman. The idea came to him in a revelation: "I walked downstairs to get a Coke, and almost forgot about the idea. I remembered that I'd been thinking about something interesting, but couldn't quite recall what it was. Then it came back in a real adrenaline rush of excitement. I was actually aware for the first time in my work on cryptography of having discovered something really valuable." (The source for this quote, and all the other historical material in this section, is [3].) Diffie had discovered a revolutionary type of cipher: his cipher incorporated an asymmetric key. In all the other cryptosystems, decryption is simply the opposite of encryption; these systems employ a symmetric key, because decryption and encryption are symmetrical. In an asymmetrical cipher, there are two distinct keys: the public and private keys. The private key is the decryption key and the public key is the encryption key. If a person, Bob, wants to send a message to another person, Alice, all he has to do is use Alice's public key to encrypt the message. Now the only person in the universe that can decrypt that message is Alice, because she has the private decryption key; Bob encrypts the message using the public key, but he cannot decrypt it: the encryption technique is a one-way function, which is irreversible unless the decoder has a special piece of knowledge unknown to the rest of the world (the private key). Although Diffie conceived of a general concept of an asymmetric cipher, he did not actually have a specific one way function that met his requirements. However, his paper (published in 1975) showed that there was indeed a solution to key distribution and he sparked interest among other mathematicians and scientists. Try as he might, Diffie and his partners Hellman and Merkle could not discover such a cipher. That discovery was made by another trio of researchers: Rivest, Shamir and Adleman.

Rivest, Shamir, and Adleman were a perfect team. Rivest is a computer scientist with an exemplary ability to apply new ideas in new places. He also kept up with the latest scientific papers, so he always had these zany new ideas for the one way function. Shamir, also a computer scientist, has a lightning intellect, and an ability to cast aside the technicalities and focus on the core of a problem. He as well as Rivest generated ideas for the one-way function. Adleman is a mathematician with extraordinary stamina, rigor and patience. He was largely responsible for spotting the flaws within the ideas of Rivest and Shamir, and he ensured that they did not follow false leads. Rivest and Shamir spent a year coming up with ideas, and Adleman spent a year shooting them down. It was very discouraging, but they knew that each failure steered them away from sterile math into more fertile mathematical ground. In April 1977, Rivest, Shamir, and Adleman spent Passover at the house of a student and consumed liberal quantities of Manischewitz wine before returning to their respective homes sometime around midnight. Rivest was unable to sleep, so he lay on his couch with a math textbook. He began to mull over the question that had been nagging him all year: Is it possible to find a one-way function that can be reversed only if the receiver has some special information? Suddenly, the mists began to clear and he had a revelation. He spent the rest of the night formalizing his idea, and by daybreak he had effectively written a complete mathematical paper. Rivest had a breakthrough, but it could not have come without the help of Shamir and Adleman. The system was later dubbed RSA, for **R**ivest, **S**hamir, and **A**dleman.

2 The RSA algorithm: an overview

We choose two primes p and q. We define $m := p \times q$, and we also choose a k such that k and $\phi(m)$ are relatively prime, $(k, \phi(m)) = 1$. The numbers p and q are kept private; m and k are public. Before encrypting a section of plain text, we first convert the text into numbers using ASCII. If our text is larger than m, we cut it into blocks that are each smaller than m. These blocks are labeled $a_1,\ a_2, \cdots a_r$. In theory, it could happen that some a_i and m are not relatively prime, $(a_i, m) \neq 1$, but this probability is so small when m and a_n are large, that we will ignore it here.

The following theorem may seem irrelevant, but it will tie in with RSA later on. The two paragraphs following the theorem will show why this theorem makes sense.

Theorem 2.1 *Suppose* $m \in \mathbb{N}$, *and* $(a, m) = 1$. *If* $k,\ \bar{k} \in \mathbb{Z}$ *are such that* $k \times \bar{k} \equiv 1 \pmod{\phi(m)}$, *then* $a^{k \times \bar{k}} \equiv a \pmod{m}$.

Proof: Since $k \times \bar{k} \equiv 1 \pmod{\phi(m)}$, $k \times \bar{k} = 1 + \phi(m) \times s$, where $s \in \mathbb{Z}$, $s \geq 0$. Now $a^{k \times \bar{k}} = a^{1+\phi(m) \times s} = a \times \left(a^{\phi(m)}\right)^r$. Since $a^{\phi(m)} \equiv 1 \pmod{m}$ (by Euler's congruence), it follows that $a^{k \times \bar{k}} \equiv a \times 1^r \equiv a \pmod{m}$. □

Since $(a_i, m) = 1$, for each $i \in \{1, 2, \cdots, r\}$, it follows that $\left(a_i^k, m\right) = 1$, for each $i \in \{1, 2, \cdots, r\}$. Furthermore, if we set $n := \phi(m)$, and $a_1,\ a_2,\ \cdots,\ a_r$ is a system of reduced residues $\pmod{m}$, then the numbers $a_1^k,\ a_2^k,\ \cdots,\ a_r^k$ are also relatively prime to m. The kth powers $a_1^k,\ a_2^k, \cdots$ a_r^k are all distinct, by the following argument: because $(k, \phi(m)) = 1$, there exists $\bar{k}$ so that $k \times \bar{k} \equiv 1 \pmod{\phi(m)}$; then if $a_i^k \equiv a_j^k \pmod{m}$ and $i \neq j$, Theorem 2.1 implies that $a_i \equiv a_i^{k \times \bar{k}} \equiv \left(a_i^k\right)^{\bar{k}} \equiv \left(a_j^k\right)^{\bar{k}} \equiv a_j^{k \times \bar{k}} \equiv a_j \pmod{m}$, which is impossible if $i \neq j$.

How does this relate to RSA? You, being supersmart, take block a_i and compute b_i such that $b_i \equiv a_i^k \pmod{m}$. We just proved that the b_i are distinct (assuming the a_i were distinct to start with). Send the distinct b_i to me. I know p and q, and therefore $\phi(m)$, and I compute $\bar{k}$ using the Euclidean algorithm. Then I solve the congruence for x_i, $x_i \equiv b_i^{\bar{k}}$. By Theorem 2.1, $x_i \equiv a_i$ (mod m), and since $a_i < m$, $x_i = a_i$.

This cryptosystem is hard to break, because if a person were to intercept the message, all they would know is the public keys: m and k. Theoretically, you could construct $\phi(m)$ from m, but this would involve factoring m into p and q. This is really hard if m is large, for as of yet there is no efficient way to factor really large numbers.

The RSA algorithm relies thus on finding large primes p and q. The next section addresses how this can be done.

3 Primality testing and Carmichael numbers.

By Fermat's Little Theorem, if, for some number a, we have $a^M \not\equiv a \pmod{M}$, then M is not a prime. (Note that it is a lot easier, i.e. faster, to raise a number a to a power, even when that power is large, than to check whether M can be factored.) To check whether a randomly picked number M is prime or composite, one could thus imagine doing experiments, trying all the numbers a between 0 and $M-1$ and checking whether $a^M \equiv a \pmod{M}$; if there is one a that fails this congruence test, then M is composite. This looks like a nice algorithm to prove that M is composite, but unfortunately it does not *detect* all composite M: it hits a snag at $M = 561 = 3 \times 11 \times 17$:

Theorem 3.1 $a^{561} \equiv a \pmod{561}$ *for* all a.

Proof: We shall prove that $a^{561} \equiv a \pmod{3}$, $\pmod{11}$ and $\pmod{17}$. For each of these we shall use Euler's congruence $a^{\phi(p)} \equiv 1 \pmod{p}$ for prime p.

We have, for arbitrary a,

$$a^{561} = \left(a^2\right)^{280} \times a \equiv 1 \times a \equiv a \ (\ \mathrm{mod}\ 3) \ ,$$

$$a^{561} = \left(a^{10}\right)^{56} \times a \equiv 1 \times a \equiv a \ (\ \mathrm{mod}\ 11) \ ,$$

$$a^{561} = \left(a^{16}\right)^{35} \times a \equiv 1 \times a \equiv a \ (\ \mathrm{mod}\ 17) \ .$$

Therefore, by the Chinese remainder theorem, $a^{561} \equiv a \pmod{561}$. □

Are there other numbers than 561 that have the same property? Being bold, we propose

Theorem 3.2 *A composite number M satisfies $a^M \equiv a \pmod{M}$ for all a if and only if M is odd, and every prime p dividing M satisfies the following two conditions:*

- $p^2 \not| M$,
- $\phi(p) | M-1$.

Proof:

- We start with the "only if" direction. Suppose M is composite such that $a^M \equiv a \pmod{M}$ for all a. We have $M = p_1 \times p_2 \times \cdots p_n$, where the p_i are primes. Choose a such that $a \equiv -1 \pmod{M}$. Then, because of the assumption on M, $a^M \equiv a \equiv -1 \pmod{M}$. If M were even, this would imply that $1 \equiv -1 \pmod{M}$, which is only possible if $M = 1$ or $M = 2$, neither of which are composite. Since we are given that M is composite, it follows that M cannot be even, i.e. it must be odd.
  Next we prove the first of the two necessary conditions. Suppose $p_i^{e_i+1}|M$. We want to show that then $e_i = 0$. Set $a = p_i^{e_i}$. Then, again by our assumption, $p_i^{e_i M} \equiv p_i^{e_i} \pmod{M}$. Consequently $M| \left(p_i^{e_i M} - p_i^{e_i}\right)$; since $p_i^{e_i+1}|M$, it follows that $p_i^{e_i+1}| \left(p_i^{e_i M} - p_i^{e_i}\right)$. Therefore $\frac{p_i^{e_i M} - p_i^{e_i}}{p_i^{e_i+1}} = \frac{p_i^{e_i(M-1)}-1}{p_i}$ is an integer, i.e. $p_i| \left(p_i^{e_i(M-1)} - 1\right)$. This is possible only if $p_i^{e_i(M-1)} - 1 = 0$, which implies $e_i = 0$, since $M \neq 1$. This proves the first of the two necessary conditions.
  For the second condition, we need to prove that $p_i - 1 | M-1$, $\forall i$. Suppose this is not

true. Then there exists $q \in \{1, \dots, p_i - 2\}$ and $k_i \geq 0$ so that $M - 1 = k_i(p_i - 1) + q$. By assumption, we have, for arbitrary a, that $M|(a^M - a)$. Since $p_i|M$, it follows that (substituting $k_i(p_i - 1) + q + 1$ for M) $p_i| \left(a^{k_i(p_i-1)+q+1} - a\right)$, or $a^{k_i(p_i-1)+q+1} \equiv a \pmod{p_i}$. Since $a^{p_i - 1} \equiv 1 \pmod{p_i}$, it follows that $a^{q+1} \equiv a \pmod{p_i}$. Because p_i is prime, this implies, if a is not a multiple of p_i, that $a^q \equiv 1 \pmod{p_i}$. To summarize, we have shown that if the second condition does not hold, then there exists a number $q \in \{1, \dots, p_i - 2\}$ so that $\forall a \in \{1, 2, \dots, p_i - 1\} \ : \ a^q \equiv 1 \pmod{p_i}$. By Theorem 2.26 in [1], this congruence can have at most q solutions because it is of degree q; since $q < p_i - 1$ and we derived that the congruence holds for the $p_i - 1$ elements of $\{1, 2, \dots, p_i - 1\}$, this is a contradiction. [Too many pigeons (= solutions) for the number of holes (= maximum number of solutions), or too few pigeons (= possible labels for the solutions) for the number of holes (= solutions waiting to be labeled)].

- Next we prove the "if" direction, that is, we assume that the composite number M is odd, and that it satisfies the two conditions. We can again factor M into its prime factors, $M = p_1 \times p_2 \times \cdots \times p_n$, where the p_i are all distinct because of the first condition. Because $p_i - 1|M - 1$, we also have, for each i, that there exists an integer k_i so that $M - 1 = k_i(p_i - 1)$. Take now an arbitrary a. Because $a^{p_i-1} \equiv 1 \pmod{p_i}$, we also have $\left(a^{p_i-1}\right)^{k_i} \equiv 1 \pmod{p_i}$, or $a^{M-1} \equiv 1 \pmod{p_i}$. This can be rewritten as $a^M - a \equiv 0 \pmod{p_i}$, which means that $p_i|a^M - a$. Because this is true for each i, and the p_i are all distinct, it follows that $\prod_{i=1}^n p_i \left| a^M - a \right.$, i.e. that $M|a^M - a$, which is again equivalent to saying that $a^M \equiv a$ (mod M). (This direction was a lot simpler!) □

The theorem we just proved is called Korselt's criterion for Carmichael numbers. "Carmichael numbers" are the numbers of which we were just speaking: numbers M that are composite but for which nevertheless $a^M \equiv a \pmod{M}$ for all a. They are named after R.O. Carmichael who first noted them in 1910. (561 is the smallest of them.)

If we use only Fermat's Little Theorem to detect primes, the Carmichael numbers can sneak in as well. Now that we are well acquainted with the Carmichael numbers, it is time to come up with a better test to decide whether a number is prime or composite. We have the following theorem:

Theorem 3.3 *If p is an odd prime, then* $(p - 1)! \equiv -1 \pmod{p}$.

Proof: If g is a primitive root, then the numbers $g, \ g^2, \ g^3, \dots, \ g^{p-1}$ are distinct $(\bmod\ p)$. On the other hand, $g \times g^2 \times g^3 \times \cdots \times g^{p-1} = g^{\frac{p(p-1)}{2}} \equiv 1 \times 2 \times \cdots \times (p - 1) = (p - 1)! \pmod{p}$. Since $g^{p-1} \equiv 1 \pmod{p}$, $g^{\frac{p-1}{2}} \equiv 1$ or $-1 \pmod{p}$. However, $g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ because g is a primitive root. Thus $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, and $g^{\frac{p(p-1)}{2}} \equiv (-1)^p \equiv -1 (\bmod\ p)$, since p is odd. □

(Note: we could prove this separately for $p = 2$ but that is highly irrelevant for primality testing.) This theorem *does* give a necessary *and* sufficient condition for primality, because we also have the following

Theorem 3.4 *If M is composite, $M > 4$, then* $(M - 1)! \equiv 0 \pmod{M}$.

Proof: If M is composite, then it can be written as a product of the type $M = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_r^{e_r}$, where the p_i are distinct primes. Let's first do the case where there are at least two different primes in this product, i.e. $r > 1$. Because $e_i \times p_i \leq p_i^{e_i} < M$, $(M-1)!$ contains all the numbers $p_1, 2p_1, 3p_1, \ldots, e_i p_i$ as factors, so that $p_i^{e_i} | (M-1)!$. Since this is true for any i, it follows that $(M-1)!$is divisible by the smallest common multiple of the $p_1^{e_1}, \cdots, p_r^{e_r}$, which is their product M. So $M|(M-1)!$, i.e. $(M-1)! \equiv 0 \pmod{M}$
Next, consider $r = 1$, i.e. $M = p^e$, with $e > 1$. If $p > 2$, then we still have $e \times p < p^e = M$, and we can use the same argument. If $p = 2$, then $e \times 2 < 2^e = M$ if $e > 2$, and the same argument still carries through. We thus have to exclude only the case $M = 2^2 = 4$. □.

Unfortunately, $(p-1)!$ is not exactly chump change. If p has, say, a hundred digits (RSA cryptosystems do use primes of this size!), then at least 90% of the factors in $(p-1)!$ have 99 digits, so that $(p-1)!$ will have more than $99 \times 90 = 8910$ digits ... This theorem (Wilson's Theorem) is therefore not of any practical interest for primality testing for RSA. We are thus still in the market for other primality tests.

Theorem 3.5 *Let p be an odd prime, then, for arbitrary a, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

(The Legendre symbol $\left(\frac{a}{p}\right)$ is defined in [1] in Definition 3.2)

Proof: If $\left(\frac{a}{p}\right) = 1$, then $x^2 \equiv a \pmod{p}$ has a solution, say, x_0. Then, by Fermat's congruence, $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$. If $\left(\frac{a}{p}\right) = -1$, then $x^2 \equiv a \pmod{p}$ has no solution. For each j such that $1 \leq j < p$, choose j' such that $j \times j' \equiv a \pmod{p}$. We know that $j \not\equiv j' \pmod{p}$. The combined contribution of j and j' to $(p-1)!$ is congruent to a, $\pmod{p}$. Since there are $\frac{p-1}{2}$ pairs j, j' , it follows that $a^{\frac{p-1}{2}} \equiv (p-1)! \pmod{p}$. Since (see above) $(p-1)! \equiv -1 \pmod{p}$, we have that $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

To use this for primality testing of a random number M, we could imagine again testing numbers a in $\mathbb{Z}/M\mathbb{Z}$; if one of them doesn't satisfy the condition, then M is composite. For instance, if we pick a to be a square, and $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{M}$, then M is composite. According to the article on the Solovay-Strassen primality test in[4], this test gives a necessary and sufficient condition: if M is composite, then for at least half the numbers in $\mathbb{Z}/M\mathbb{Z}$, $\left(\frac{a}{p}\right) \not\equiv a^{\frac{p-1}{2}} \pmod{M}$.

The following theorem gives yet another primality test:

Theorem 3.6 *Let p be an odd prime, and write $p - 1 = 2^k q$, with q odd. Take a arbitrary. Then either $a^q \equiv 1 \pmod{p}$, or there is an integer $m \in \{0, 1, 2, \ldots, k-1\}$ so that $a^{2^m q} \equiv -1 \pmod{p}$.*

Proof: If $a^q \equiv 1 \pmod{p}$, we don't have to prove anything. So, let's suppose $a^q \not\equiv 1 \pmod{p}$. Define $E = \{\ell; 1 \leq \ell \leq k \text{ such that } a^{2^\ell q} \equiv 1 \pmod{p}\}$. Because $k \in E$, $E \neq \emptyset$. E must have a smallest element ℓ_0, which has to be at least 2, since $1 \notin E$ by the assumption with which we started the proof. Set $n := \ell_0 - 1 \geq 1$. Since $n \notin E$, we have $a^{2^n q} \not\equiv 1 \pmod{p}$; on the other hand, since $n + 1 \in E$, $a^{2^{n+1} q} \equiv 1 \pmod{p}$, i.e. $\left(a^{2^n q}\right)^2 \equiv 1 \pmod{p}$. It follows that $a^{2^n q} \equiv -1$ (mod p). □

By the contrapositive, this gives us a criterion by which we know that a number is composite:

Corollary 3.7 *Let M be an odd integer; write $M-1=2^k q$, with q odd. If for some choice of a we have both $a^q \not\equiv 1 \pmod{M}$ and $a^{2^\ell q} \not\equiv -1 \pmod{M}$, $\forall \ell \in \{0,1,\ldots,k-1\}$, then M is composite.*

If M is an odd composite number, then there are at least 75% of the numbers in $\{1,\ldots,M-1\}$ that establish, by the this test, that M is composite [2]. If we randomly choose 100 different a and none of them indicate that the M is composite, then the chance of M being nevertheless composite is approximately $.75^{100} \cong 3^{-13}$. In practice, a composite M is usually unmasked within a few tries.

Let's try it for a Carmichael number. In [2] the case 561 is discussed in detail, so let's do another one here. We take $6601 = 7 \times 23 \times 41$. We have $6600 = 2^3 \times 825$, so $k=3$, $q=825$. Even the simplest try for a already exposes 6601 for the composite number it is, since $2^{825} \equiv 2738$ (mod 6601), $2^{2\times 825} \equiv 4509 \pmod{6601}$, and $2^{4\times 825} \equiv 1 \pmod{6601}$.

Here, it is easy and possible to unmask 6601 as a composite number, unlike with the primality test using Fermat's Little Theorem. In fact, this test was most widely used to find out if a large number was prime until 1999, with the advent of the AKS Test. This test was the first completely efficient primality test that ran in polynomial time.

References

[1] I. Niven, H. Zuckerman and H. Montgomery, *An Introduction to The Theory of Numbers* John Wiley & Sons, 1991 (5th edition).

[2] J. Silverman, *A Friendly Introduction to Number Theory*, Prentice Hall (Upper Saddle River, NJ) 1997.

[3] S. Singh, *The Code Book* Random House (New York) 1999.

[4] `www.Wikipedia.com`

[5] `www.mathworld.com`