Fermat's Little Theorem and RSA Algorithm

Posted on **July 8, 2013**

RSA is a cryptographic algorithm that is used to send and receive messages. We use the Fermat's Little Theorem to prove that RSA works correctly and accurately. In other words, the decrypted message is indeed the original message from the sender. Mathematically we show that applying the encryption function and the decryption function successively produces the identity function.

To see how RSA works, see the previous post An Illustration of the RSA Algorithm.

RSA Algorithm

We first briefly describe the algorithm and then present the mathematical statement to validate.

Let $N = p \cdot q$ where p and q are two prime numbers. Let $\phi = (p-1) \cdot (q-1)$. Choose an integer e with $1 < e < N$ such that e and ϕ are relatively prime.

The public key consists of N and e where e is the encryption key. Once it is published, anyone can use it to encrypt messages to send to the creator of the public key. The following is the encryption function:

$$f(M) \equiv M^e \pmod{N}$$

where M is a positive integer and is the original message.

The private key is a positive integer d that satisfies:

$$d \cdot e \equiv 1 \pmod{\phi = (p-1) \cdot (q-1)}$$

In other words, d is the multiplicative inverse of e in the modular arithmetic of modulo ϕ. The above condition is equivalent to: $de - 1 = (p-1) \cdot (q-1) \cdot k$ for some integer k.

The number d is the decryption key that will be used to decode messages. So it should remain private.

Once the creator of the public key receives an encrypted message $C = f(M)$, he or she uses the following decryption function to obtain the original message M.

$$g(C) \equiv C^d \pmod{N}$$

The Mathematical Statement to Validate

What we prove is that the decryption function is to undo the encryption function. Specifically, we prove the following:

$$g(C) = g(f(M)) = (M^e)^d = M^{ed} \equiv M \ (\text{Mod } N) \tag{1}$$

In other words, applying the decryption function g to the encryption function f produces the original message.

Fermat's Little Theorem

In this section, we list out the tools we need to prove the correctness of RSA.

Theorem 1 (Fermat's Little Theorem)
If p is a prime number and a is an integer such that a and p are relatively prime, then

$a^{p-1} - 1$ is an integer multiple of p

or equivalently $a^{p-1} \equiv 1 \pmod{p}$.

For a proof of Fermat's little theorem, see this post.

Lemma 2 (Euclid's Lemma)
Let a, b and d be integers where $d \neq 0$. Then if d divides $a \cdot b$ (symbolically $d|a \cdot b$), then either $d|a$ or $d|b$.

Euclid's Lemma is needed to prove the following Lemma.

Lemma 3
Let M be an integer. Let p and q be prime numbers with $p \neq q$.

Then if $a \equiv M \pmod{p}$ and $a \equiv M \pmod{q}$, then $a \equiv M \pmod{p \cdot q}$.

Proof of Lemma 3
Suppose we have $a \equiv M \pmod{p}$ and $a \equiv M \pmod{q}$. Then for some integers i and j, we have:

$a = M + p \cdot i$ and $a = M + q \cdot j$.

Then $p \cdot i = q \cdot j$. This implies that p divides $q \cdot j$ ($p|q \cdot j$). By Euclid's lemma, we have either $p|q$ or $p|j$. Since p and q are distinct prime numbers, we cannot have $p|q$. So we have $p|j$ and that $j = p \cdot w$ for some integer w
.

Now, $a = M + q \cdot j = M + q \cdot p \cdot w$, implying that $a \equiv M \pmod{p \cdot q}$. ■

The Proof of (1)

We now prove the property (1) described above. We show that

$$(M^e)^d = M^{ed} \equiv M \ (\text{Mod } N = p \cdot q)$$

We first show that $M^{ed} \equiv M \ (\text{Mod } p)$ and $M^{ed} \equiv M \ (\text{Mod } q)$. Then the desired result follows from Lemma 3.

To show $M^{ed} \equiv M \ (\text{Mod } p)$, we consider two cases: $M \equiv 0 \ (\text{Mod } p)$ or $M \not\equiv 0 \ (\text{Mod } p)$.

Case 1. $M \equiv 0 \pmod{p}$. Then M is an integer multiple of p, say $M = p \cdot w$ where w is an integer. Then $M^{ed} = (p \cdot w)^{ed} = p \cdot p^{ed-1} \cdot w^{ed}$. So both M and M^{ed} are integer multiples of p. Thus $M^{ed} \equiv M \pmod{p}$.

Case 2. $M \not\equiv 0 \pmod{p}$. This means that p and M are relatively prime (having no common divisor other than 1). Thus we can use Fermat's Little Theorem. We have $M^{p-1} \equiv 1 \pmod{p}$.

From the way the decryption key d is defined above, we have $ed - 1 = (p-1) \cdot (q-1) \cdot k$ for some integer k. We then have:

$$\begin{aligned} M^{ed} &= M^{ed-1} \cdot M \\ &= M^{(p-1)\cdot(q-1)\cdot k} \cdot M \\ &= (M^{p-1})^{(q-1)\cdot k} \cdot M \\ &\equiv (1)^{(q-1)\cdot k} \cdot M \pmod{p} \; * \\ &\equiv M \pmod{p} \end{aligned}$$

At the step with *, we apply Fermat's Little Theorem. So we have $M^{ed} \equiv M \pmod{p}$.

The same reason reasoning can show that $M^{ed} \equiv M \pmod{q}$.

By Lemma 3, it follows that $M^{ed} \equiv M \pmod{N = p \cdot q}$. ■

Revised August 9, 2014.

SHARE THIS:

Twitter Facebook

Like

Be the first to like this.

RELATED

An Illustration of the RSA Algorithm
In "Applied"

Solving Linear Congruences
In "Basic"

Euler's phi function, part 2
In "Basic"

This entry was posted in **Applied**, **Prime Numbers** and tagged **Encryption**, **Euclid's Lemma**, **Fermat's Little Theorem**, **Mathematics**, **Number Theory**, **Prime Number**, **Public-key cryptography**, **Rivest-Shamir-Adleman**, **RSA**, **RSA Algorithm** by **Dan Ma**. Bookmark the **permalink [https://exploringnumbertheory.wordpress.com/2013/07/08/fermats-little-theorem-and-rsa-algorithm/]** .

3 THOUGHTS ON "FERMAT'S LITTLE THEOREM AND RSA ALGORITHM"

Pingback: Notes on Cryptology | Kıvanç's Pancake House

timclimber
on **July 25, 2015 at 12:04 am** said:

Great! Here is another article-explanation of RSA: http://yurichev.com/blog/RSA/

andrzej
on **May 10, 2017 at 3:04 am** said:

a=4, b=15, d=6; so d |a*b but neither d | a nor d | b;