Miller-Rabin

Rajesh Pavuluru
991711828

Abstract

Contents

1 Introduction

when someone wants to use the RSA public key cryptosystem, they had to generate the private key which consists of two large prime numbers and a public key consists of the product of that two prime numbers, to do this we need to able to find large prime numbers which plays a significant role in securing our information. Miller Rabin is a fast way to test primality of the large numbers. This algorithm is also known as Rabin-miller primality test and this algorithm determines whether number is prime which is similar to other tests such as Fermat primality Test and Solovay-Strassen primality test. This test is relied on equality or set of equalities that hold the true for prime values, then checks whether they hold for the number, that we want to test for primality. This algorithm is most practical known primality testing algorithm and is used in different software libraries that rely on RSA encryption and best example is OpenSSL. Unlike other primality tests which proves that a number is prime, Miller Rabin proves that the number is composite.So this might be called compositeness test instead of primality test. The miller Rabin test detects all composites. For each composite number n, there may be at least 3/4 (Miller Rabin) of numbers a are witnesses of compositeness of n.

2 History

Miller-Rabin primality test was named,when Michael Rabin discovered a randomized polynomial-time algorithm in 1980 to test whether a number is prime, which was closely related to a deterministic algorithm studied by Gary Miller in 1976. Miller Rabin is relatively simple extension of Fermats littleTheorem that allows us to test for primality with a much higher probability than Fermats little theorem..This is still the most practical known primality test algorithm.

3 How Miller Rabin works

Before Miller Rabin, we know only two ways to prove that a number n is composite:

1. find a factorization n = ab, where a,b >1.
2. find a Fermat witness for n, i.e a number x satisfying $x^{n-1} \not\equiv 1(modn)$.

Miller-Rabin test is based on a different way to prove that a number is composite.

Suppose n is prime with n >2 and It follows that $n-1$ is even and we can write it as $2^s d$, where s and d are positive integers (d is odd). For each a in (Z/nZ)*, either

$$a^d \equiv 1(modn)$$

or

$$a^{2^r.d} \equiv -1(modn)$$

for some

$$0 \leq r \leq s-1$$

. To show that one of these must be true, according to Fermat's little theorem, that for a prime number n:

$$a^{n-1} \equiv 1(modn)$$

By the above statement, in the event that we continue taking square foundations of a^{n-1}, we will get either 1 or -1. In the event that we get -1 then the second equity holds and it is finished. On the off chance that we never get 1, then when we have taken out each force of 2, we are left with the first one.

The Miller-Rabin primality test depends on the contrapositive of the above statement. i.e, in the event that we can discover an a

$$a^{d} \not\equiv 1(modn)$$

or

$$a^{2^r.d} \not\equiv -1(modn)$$

for all

$$0 \leq r \leq s-1$$

., then n is not prime.

We call an a witness for the compositeness of n (now and then misleadingly called a solid witness, in spite of the fact that it is a sure confirmation of this). Generally a is known as a strong liar, and n is a solid plausible prime to base a. The expression "strong liar" alludes to the situation where n is composite yet all things considered the mathematical statements hold as they would for a prime.

4 Example

Lets take 221 is our number to be tested for primality

n=221

n-1 = 220 = $2^2 * 55$, s=2 , d=55

picking random a1 in range 0<$a1$<221,

a1=174

$a1^{2^0 d} modn = 174^{55} mod 221 = 471, n-1$

$a1^{2^1 d} modn = 174^{110} mod 221 = 220 = n-1$

Since $220 \equiv -1 modn$, either 221 is prime, or 174 is a strong liar for 221.

We will try another random a, a2 = 137:

$a2^{2^0 d} modn = 137^{55} mod 221 = 1881, n-1$

$a2^{2^1 d} modn = 137^{110} mod 221 = 2051, n-1$

Here a2 is a witness for the compositeness of n, and a1 was infact a strong liar

5 Algorithm

Input : n (n is the number to be tested for primality)
Output : whether n is prime or not

1. Let $n-1=2^s d$ where $d \epsilon N$ and $s \epsilon N$

   Choose a random integer a with $2 \leq a \leq n-2$

2. Compute
$$X \equiv a^d (mod n)$$

   If $X \equiv \pm 1 (mod n)$ Then end the algorithm with message "n is probably prime".

   If s=1 then end the algorithm with message "n is definitely not prime".

   Otherwise set r=1 and go to step 3

3. Compute
$$X \equiv a^{2^r d} (mod n)$$

   If $x \equiv 1 (mod n)$ then end the algorithm with message "n is definitely not prime".

   If $x \equiv -1 (mod n)$ then end the algorithm with message "n is probably prime".

   Otherwise set r=r+1 and go to step 4

4. If r=s-1, then go to step 5,otherwise go to step 3

5. Compute
$$X \equiv a^{2^{s-1} d} (mod n)$$

   If $x \not\equiv -1 (mod n)$ then terminate the algorithm with "n is definitely not prime".

   If $x \equiv -1 (mod n)$ then terminate the algorithm with "n is probably prime".

6 Advantages

- This Algorithm is used to test large numbers for primality.
- Due to its advantage in speed when compared to other primality tests, Miller Rabin test will be the test of choice for various cryptographic applications.
- When compared to Euler and Solovay-Strassen tests, Miller Rabin is more powerful and important aspect is that the probability of failure is reduced.
- According to the fermat test there are too many liars for all Carmichael numbers n, the error probability is close to 1, this disadvantage is avoided in Miller Rabin.

7 Disadvantages

- Inspite of the fact that the Miller-Rabin test is quick, there exist composite numbers n for which this test fails for 1/4 of all bases coprime to n.

8 Conclusion

In this paper we showed how to implement the Miller Rabin algorithm for Primality testing. we have seen that this algorithm might lies about the primality for 1/4 of bases coprime to a number, but there may be at least 3/4 of bases are witnesses of compositeness of n. Finally we recognized that its better to implement this algorithm for more than one base,before coming to the conclusion of primality of a particular number.

9 References

1. $en.wikipedia.org/wiki/Miller - Rabin\_primality\_test$
2. Richard A.Mollin,RSA and Public-Key cryptography
3. $Weisstein, EricW."Rabin-MillerStrongPseudoprimeTest."FromMathWorld$
4. $en.wikipedia.org/wiki/Primality\_test$
5. Introduction to Cryptography by Johannes Buchmann