ASSIGNMENT 10

Authors- Monica T., Niranjan P., Vasanthi R.

The first item in the textbook's bibliography is a paper by Agrawal, Kayal and Saxena, titled *Primes is in P*. That paper, published in 2004, and gives the first polytime deterministic algorithm for primality. Please write a one page explanation why OpenSSL, and other tools, still use the randomized Rabin-Miller instead of the deterministic polytime algorithm.

The tools like OpenSSL or algorithms like Diffie-Hellman, ElGamal and RSA requires requires large prime numbers to operate. One could try finding large prime numbers with brute force but it would not be efficient. There are various deterministic polytime algorithms to find if a number is prime or not. Eg- Rabin-Miller, Solovay and Strassen, Agrawal[04]. Agrawal [04] devised an algorithm which checks for primality of a number unlike Rabin-Miller which checks for non-composite of a number(not full proof in providing prime numbers). Thus the question arises, how come OpenSSL and other tools still use Rabin-Miller instead of deterministic polytime algorithm.

Rabin Miller uses

$$a^{(n-1)} = 1 \mathrm{mod}(n)$$

where n is the number whose primality is checked and a is the base , where $1<a<n$.
Even though Rabin-Miller is more simplified and an efficient algorithm with $O(n^4)$,(where as Agarwal [04] runs in $O(\log^{21/2} n)$). But Rabin-Miller has a problem that it sometimes passes composite as prime which are called Carmicheal numbers. The set of prime numbers and Carmicheal numbers is called pseudoprimes.
It has been shown though that the probability of error is less than equal to half.
And this could be further lessened by using multiple bases(a) to check the primality of n.

To solve the problem of finding large primes, we know by the Prime Number Theorem that there are about (n/log n) primes before a number n, which means that there are $2^n/n$ primes among n-bit integers, around 1 in n, which are fairly uniformly distributed. So we pick an integer at random from the given range and then apply Rabin-Miller algorithm to it.

In the paper titled "A polytime proof of correctness of the Rabin-Miller algorithm from Fermat's Little Theorem" by Grzegorz Hermanand Michael Soltys [2018], they try to prove the correctness of the Rabin-Miller algorithm from Fermat's little theorem. They give an explanation for the Carmicheal numbers and how they could be either a power of a smaller number Q, or a product of two relatively prime numbers Q and R.