Algorithm 1 get_strong_prime

```
Input: bit_length
Output: prime
get a prime p of 256bit
for Rabin_wit(pq_1) == false do
    get a random number q in range $2^{256} to 2^{257}$
    pq_1 = p*q+1
end for
for Rabin_wit(prime) == false do
    get a random number r in range $2^{512} to 2^{513}$
    result = pq_1 * r
end for
return prime
```