RSA Encryption

Johnny Lindbergh

May 2018

1 Prime Generation

Large prime numbers are generated using the Rabin-Miller primallity test:

Algorithm 1 Rabin-Miller

```
for i ← 1, n do
    choose random a ∈ {1, 2, 3, ..., p − 2}
    z ≡ a^r mod p
    if z ≢ 1 and z ≢ p − 1 then
        for j ← 1, u − 1 do
            z ≡ z^2 mod p
            if z = 1 then
                Return False
        if z ≠ p − 1 then
            Return False
Return True
```

2 Key Generation

Let $n = pq$ where $p, q \in \mathbb{P}$,

compute $\phi(n)$, where ϕ is Euler's totient function.

Choose $e \in \mathbb{Z}$ such that, $1 < e < \phi(n)$, $gcd(\phi(n), e) = 1$ e and $\phi(n)$ are coprime

Find $d = e^{-1} (\mathrm{mod} \phi(n))$

The public key exponent is e and the private key exponent is d