

Primality Testing:-

1st approach:-

Input: N, t

output:- decision whether N is prime or not.

for $i = 1$ to t .

$a \leftarrow \$ \{1, \dots, N-1\}$.

if $a^{N-1} \not\equiv 1 \pmod{N}$, then return "composite".

end for

return "prime".

$a \in \mathbb{Z}_N^*$
"a is called witness".

"if $\gcd(a, N) \neq 1$.
then a is a trivial
witness".

If Z_N^* has at least one witness, then there are at least $|Z_N^*|/2$ many witnesses.

What is the probability that the experiment returns "Composite".

At any trial, it returns composite, if either $\gcd(a, N) \neq 1 \pmod{N}$ or a is a witness.

Let A be the event that $\gcd(a, N) \neq 1$
 Let B " " " " " a is a witness

$$\begin{aligned} & \left. \begin{array}{l} \text{Let } A \text{ be the event that } \gcd(a, N) \neq 1 \\ \text{Let } B \text{ " " " " " } a \text{ is a witness} \end{array} \right\} \begin{aligned} & \text{Pr}[\text{ith trial returns composite}] \\ &= \text{Pr}[A \cup B] = \text{Pr}[A] + \text{Pr}[B] - \text{Pr}[A \cap B] \\ &\geq \text{Pr}[B] \\ &= \frac{|W|}{N-1} \geq \frac{|Z_N^*|}{2(N-1)} = c \end{aligned} \end{aligned}$$

$$\text{Pr}[\text{prime return}] = \prod_i \text{Pr}[\text{ith trial does not return composite}] \leq (1-c)^t$$

2nd Approach:-

Let N be an odd integer.

$N-1 = 2^r \cdot u$, where u is an odd integer and $r \geq 1$.

$a^{2^r \cdot u} \neq 1 \pmod N$. $\rightarrow$ Previous check.

for $i \in \{0, \dots, r-1\}$, we compute $a^{2^i \cdot u}$
 $(a^u, a^{2u}, a^{2^2 u}, \dots, a^{2^{r-1} \cdot u})$.

Let $a \in \mathbb{Z}_N^*$. a is called a strong witness if $a^u \neq \pm 1 \pmod N$ and $a^{2^i \cdot u} \neq -1 \pmod N$ for all $i \in \{1, \dots, r-1\}$.

In other words, if a is not a strong witness, then we have either of the following:-

$$\begin{aligned} - (a^u, a^{2u}, a^{2^2u}, \dots, a^{2^{r-1}u}) &= (\pm 1, 1, \dots, 1) \\ - (a^u, a^{2u}, a^{2^2u}, \dots, a^{2^{r-1}u}) &= (*, * \dots *, -1, 1, \dots, 1). \end{aligned}$$

Claim:- Let $a \in \mathbb{Z}_N^*$. If a is a witness, then a is a strong witness.

Let W be the set of witness,

Let SW " " " " strong witness.

$$|W| \leq |SW|$$

Lemma: Let N be an odd prime. Then there does not exist any strong witness.

Pf: Let $a \in \mathbb{Z}_N^*$ be any arbitrary integer.

Let $i \geq 0$ be the smallest index, $i \in \{0, \dots, r\}$. Such that $a^{2^i \cdot u} = 1 \pmod{N}$.

Such i exists

if $i = 0$, we are done!

$$a^{2^i \cdot u} \equiv 1 \pmod{N} \text{ for some } 0 < i \leq r-1$$

$$(a^{2^{i-1} \cdot u})^2 = a^{2^i \cdot u} \equiv 1 \pmod{N} \Rightarrow a^{2^{i-1} \cdot u} \equiv \pm 1 \pmod{N}.$$

Let N be a odd composite number which is not a prime power.

Lemma:- Let N be an odd number that is not a prime power. Then at least half of the elements of $\mathbb{Z}_N^*$ are strong witnesses.

Pf: Let "Bad" be the set of integers $a \in \mathbb{Z}_N^*$ which are not strong witnesses. We define a set Bad' . We will show

$$(i) \text{Bad} \subseteq \text{Bad}'$$

(ii) Bad' is a strict subgroup of $\mathbb{Z}_N^*$.

pf: For every $a \in \text{Bad}$. $-1 \in \text{Bad}$.

we compute $a^{2^i u} \bmod N$. $i \in \{0, \dots, r-1\}$.

Such that $a^{2^i u} \equiv -1 \bmod N$. Let k be the largest index.

$\text{Bad}' = \{a \in \mathbb{Z}_N^* : a^{2^k u} \equiv \pm 1 \bmod N\}$ for which $\exists a \in \text{Bad}$ such that $a^{2^k u} \equiv -1 \bmod N$.

Claim: $\text{Bad} \subseteq \text{Bad}'$

Let $a \in \text{Bad} \Rightarrow a^u = 1 \bmod N \mid a^{2^j u} = -1 \bmod N$ for some $j \in \{0, \dots, r-1\}$

$$a^{2^k u} = (a^u)^{2^k} = 1 \bmod N,$$

$$a^{2^k u} = (a^{2^j u})^{2^{k-j}}$$

Claim: Bad' is a subgroup of $\mathbb{Z}_N^*$.

$$-1 \in \text{Bad}'$$

$$a \in \text{Bad}' \Rightarrow a^{2^k \cdot u} \equiv \pm 1 \pmod{N}$$

$$b \in \text{Bad}' \Rightarrow b^{2^k \cdot u} \equiv \pm 1 \pmod{N}$$

$$(ab)^{2^k \cdot u} = a^{2^k \cdot u} \cdot b^{2^k \cdot u} \equiv \pm 1 \pmod{N}.$$

Claim: Bad' is a strict subgroup of $\mathbb{Z}_N^*$.

Pf: - Since N is not a prime power, N can be expressed as $N = N_1 \cdot N_2$ such that $\gcd(N_1, N_2) = 1$.

By applying CRT, any element $a \in \mathbb{Z}_N^*$ can be mapped to $a_1 \in \mathbb{Z}_{N_1}^*$ and $a_2 \in \mathbb{Z}_{N_2}^*$, i.e.:

$a \mapsto (a_1, a_2)$, where $a_1 \equiv a \pmod{N_1}$ and $a_2 \equiv a \pmod{N_2}$.

$1 \mapsto (+1, +1)$ Let $a \in \text{Bad}'$ such that $a^{2^k \cdot u} \equiv -1 \pmod{N}$.
 $-1 \mapsto (-1, -1)$.

$$a^{2^k \cdot u} = (a_1, a_2)^{2^k \cdot u} = (a_1^{2^k \cdot u}, a_2^{2^k \cdot u}).$$

So, if $a^{2^k \cdot u} \equiv -1 \pmod{N}$, then $a_1^{2^k \cdot u} \equiv -1 \pmod{N_1}$
 $a_2^{2^k \cdot u} \equiv -1 \pmod{N_2}$.

Consider an element $b \in \mathbb{Z}_N^*$ with $b = (a, 1)$

$$b^{2^k u} = (a, 1)^{2^k u} = (a^{2^k u}, 1) \\ = (-1, 1)$$

Thus $b \in \mathbb{Z}_N^*$ but $b \notin \text{Bad}'$. Hence, Bad' is a strict subgroup of $\mathbb{Z}_N^*$.

$$\text{Thus } |\text{Bad}'| \leq |\mathbb{Z}_N^*|/2.$$

$$\Rightarrow |\text{Bad}| \leq |\mathbb{Z}_N^*|/2$$

Miller Rabin Primality test.

Input:- N is an integer, t is a parameter.

Output:- Decision whether N is prime or not.

Check:- if N is even, return composite.

if N is a prime power, return "composite"

✓ Compute r and u such that $N-1 = 2^r \cdot u$.

for $i = 1$ to t .

$a \leftarrow \{1, \dots, N-1\}$

if $a^u \not\equiv \pm 1 \pmod{N}$ and $a^{2^j \cdot u} \not\equiv -1 \pmod{N}$ for all $j \in \{1, \dots, r-1\}$.

return composite.

end for

return "prime".

Hard problems:-

- (i) Factorization
- (ii) Computing discrete log.

GenModulus (1^n) ; n is called the security parameter.

- ✓ - Samples two n bit prime numbers p and q .
- Compute $N = p \cdot q$.
- output (N, p, q) .

Factorization Game:-

- Factor_{A, GenModulus} (n).
- 1. Run GenModulus (1^n) to obtain (N, p, q)
 - 2. A is given N and outputs $p', q' > 1$.
 - 3. output 1 if $p' \cdot q' = N$.

Defn: Factoring is hard relative to GenModulus.
if for all PPT adversary A ,
 $\exists$ a negligible fn $\text{negl}()$,
such that

$$\Pr \left[\text{Factor}_{A, \text{GenModulus}}(n) \right] \leq \text{negl}(n)$$

RSA problem:

Let $N = p \cdot q$, where p and q are two distinct n bit primes.
Let e be an integer such that $\gcd(e, \phi(N)) = 1$.

Then $f_e: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$ defined as $x \mapsto x^e \bmod N$ is a bijection.

$$x^e \equiv y^e \bmod N \quad \phi(N) \mid de - 1 \Rightarrow de - 1 = k \cdot \phi(N)$$

$$\Rightarrow x^{de} \equiv y^{de} \bmod N$$

$$\Rightarrow de = 1 + k \cdot \phi(N)$$

$$\Rightarrow x^{1+k \cdot \phi(N)} \equiv y^{1+k \cdot \phi(N)} \bmod N$$

$$\Rightarrow x \equiv y \bmod N$$

RSA Assumption:-

$\text{RSA-Inv}_A, \text{GenRSA}^{(n)}.$

1. Run $\text{GenRSA}(1^n)$ to obtain (N, e, d) .
2. Choose a uniform $y \in \mathbb{Z}_N^*$.
3. A is given (N, e, y) and outputs $x \in \mathbb{Z}_N^*$.
4. output 1 if $x^e \equiv y \pmod{N}$.

e is called
"public exponent"
 d is called
"private exponent"

$\text{GenRSA}(1^n)$.

outputs a modulus N
which is the product of
two n -bit primes and
two integers $e, d > 0$ such
that $ed \equiv 1 \pmod{\phi(N)}$.

Defn RSA problem is hard relative to GenRSA. if for.
all PPT adversary A , $\exists$ a negligible fn $\text{negl}(\cdot)$.
such that

$$Pr[RSA\text{-}Inv_{A, \text{GenRSA}}(n)] \leq \text{negl}(n).$$

How one can implement GenRSA.

GenRSA(1^n)

1. Run GenModulus(1^n) to obtain (N, p, q) .
2. Compute $\phi(N) = (p-1)(q-1)$
3. choose an integer e such that $\gcd(e, \phi(N)) = 1$.
4. Compute $d = e^{-1} \bmod \phi(N)$.
5. output (N, e, d) .

How does the hardness of RSA is related to factoring.

We are given y .

We need to find $y^d \bmod n$

d is called "trapdoor".

Conclusion:- If factorization is easy to solve, then RSA-Inv is also easy to solve.

If RSA-Inv is hard, then factorization is hard.