Algorithm

1. Pick 2 large primes P, Q
2. Calculate modulus $N = P \cdot Q$
3. Compute ϕ, $\phi(N) = (P-1).(Q-1)$
4. Choose public exponent e such that,
   a) $1 < e < \phi(N)$
   b) $gcd(e, \phi) = 1$
5. Choose secret exponent d such that, $e.d \mod \phi(N) = 1$
6. Encode the message m with, $C = m^e \mod N$
7. Decode the ciphertext C with, $m = C^d \mod N$

Basically,

RSA = {
public key = [e, N]
private key = [d, N]

secret components = [P, Q, φ, d]
}

Basis for RSA [NP problem]

The process of multiplying 2 primes to get N is easy. However, getting back the primes P, Q from N is computationally very difficult.

> unless you have trillions of years of computation under your belt
> (or a Quantum Computer xD)

Choosing e

We need to choose e such that ϕ and e are coprime. In practice we take e as a prime number greater than 2 and lesser than ϕ.
This means that the factors of $e = \{1, e\}$

Now, in which case will $gcd(e, \phi) \neq 1$?

- when ϕ is a multiple of e $\left(gcd(e, \phi) = e \right)$

So, if ϕ is a multiple of e, pick new primes P, Q that will give you $gcd(e, \phi) = 1$

In practice e is taken as $2^{16} + 1$
$\therefore e = 65537$

What is ϕ ? (Euler's Totient Function)

A number p is prime if it is divisible by only 1 and itself, i.e. its factors $= \{1, p\}$

Two numbers, x and y, are coprime if they share no common factors except for 1.
i.e $gcd(x, y) = 1$

ϕ is a function of N that returns the number of numbers from 1 to N that are coprime with N.

$$\therefore \phi(N) = \left| \{ i : 1 \leq i < N \text{ and } gcd(i, N) = 1 \} \right|$$

Lemma -

if prime_factors$(N) = \{p, q\}$, i.e. $N = p \cdot q$
then,
$$\phi(N) = (p-1) \cdot (q-1)$$

Prove this!

RSA Encryption Algorithm 2

15 November 2021 09:40 AM

Bob wants to send a message to Alice

RSA Summary

Alice	unsafe channel	Bob
Safe		Safe
Generate: public key = [e, N]; private key = [d, N]	e, N	m = message, as an integer
Secret components: P, Q, $\phi(N)$, d		$c = m^e (\bmod N)$
$m = c^d (\bmod N)$	c	

Public-Key Cryptosystem

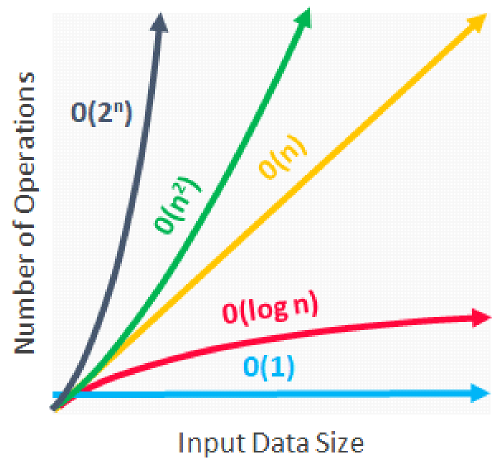
Practical Demonstration with small primes!

Alice	unsafe channel	Bob
P = 13 Q = 17 N = 221 ϕ = 192 d = 77 12·16 e = 5	[5, 221]	m = "B" ↓ 66 a → 97 A ↓ 65 B ↓ 66
d = 77 $c^d \bmod N$ $66 = 53^{77} \bmod 221$ ↓ "B"	53	$c = 66^5 \bmod 221$

RSA Encryption Algorithm 3

18 November 2021 09:39 AM

Time Complexity



The task we want to solve is,
is algorithm X faster than algorithm Y.
We can use the run-times of the two algorithms and determine which takes lesser time.

However, different systems will report different individual run times. This is why we introduce time complexity of an algorithm, which tells us how the run time scales with input size.

In Big-O notation, we consider the worst case scenario.

Orders of Time Complexity:

constant $O(1)$

logarithmic $O(\log n)$

polynomial $O(n^k)$

exponential $O(2^n)$

Examples:

(I) for i=1, i<=n, i=i+1

do something

(II) for i=1, i<=n, i=i+1
for j=1, j<=n, j=j+1

do something

(III) for i=1, i*i<=n, i=i+1

do something

In Big-O notation, we ignore constants and multiples.
(see the big picture)

RSA Encryption Algorithm 4

18 November 2021 01:07 PM

Extra stuff!

- Extended euclid algorithm to find d from phi and e

- Why rsa works - d is actually the modular inverse of e with phi. It exists only
If e and phi have no common factors.

- In practice, we use the charmicael function instead of euler's totient function

$$\lambda(n) = \operatorname{lcm}(p-1, q-1)$$

Further Reading:

Derivation of Lemma (Prerequisites for understanding this - Discrete mathematics, basic Group Theory)
https://scholar.rose-hulman.edu/cgi/viewcontent.cgi?article=1081&context=rhumj#:~:text=Euler's%20%CF%86%20(phi)%20Function%20counts,formula%20arises%20from%20this%20fact.

RSA Exhaustive Article
https://www.di-mgt.com.au/rsa_alg.html

Modular Inverse
https://www.geeksforgeeks.org/multiplicative-inverse-under-modulo-m/

RSA Encryption Algorithm

19 November 2021 06:24 PM

Extended Euclidean GCD

iteration 1

$top1 = \overset{\phi}{192}$ | $top2 = \overset{\phi}{192}$

$e = 5$ ✓ | let $d = 1$

$k = \left\lfloor \frac{192}{5} \right\rfloor = 38$ | $k = 38$

$192 - 38(5) = 192 - 190 = 2$ | $192 - 38(1) = 154$

iteration 2

$top1 = 5$ | $top2 = 1$

$e2 = 2$ | $d = 154$

$k = \left\lfloor \frac{5}{2} \right\rfloor = 2$ ⟶ $k = 2$

$5 - 2(2) = 1$ ← $e2$ | $1 - 2(154) = 1 - 308 = -307$

$-307 \bmod \phi$

$= -307 \bmod 192$

$$\begin{array}{r} -307 \\ +192 \\ \hline -115 \end{array} \qquad \begin{array}{r} -115 \\ +192 \\ \hline +77 \end{array}$$

$\boxed{d = 77}$