RSA

$n \in \mathbb{N}$ & $n = pq$ where p & q are both prime numbers, chosen to be large, $p \neq q$

Chose $0 < e < n$ s.t. $\gcd(e, \phi(n)) = \gcd(e, (p-1)(q-1)) = 1$

Private key (p, q) & (n, e) is the public key.

Encryption: $\mathcal{E} : \mathbb{Z}_n \to \mathbb{Z}_n$ $\quad m \mapsto m^e$

Decryption: $\mathcal{D} : \mathbb{Z}_n \to \mathbb{Z}_n$ $\quad c \mapsto c^d$

where $d = e^{-1} \bmod \phi(n)$, $\phi(n) = (p-1)(q-1)$

$\left[\mathbb{Z}_n = \mathbb{Z}_{(p-1)(q-1)} \text{ \& } e \in U(\mathbb{Z}_{(p-1)(q-1)}) \right]$

$\exists\, s, t \in \mathbb{Z}$ s.t. $se + t\phi(n) = 1 \Rightarrow se \equiv 1 \bmod \phi(n)$

- $\mathcal{D}\mathcal{E}(m) = (m^e)^d = m^{ed}$ $(= m?)$ $\quad m^{se} = m^{1 - t\phi(n)} \equiv m \bmod n$

If $\gcd(m, n) = 1$, then $m^{\phi(n)} \equiv 1 \bmod n$ (Euler) $\quad |U(\mathbb{Z}_n)| = \phi(n)$

Suppose $\gcd(m, n) \neq 1$

Then $\gcd(m, n) = p$ or q.

$\boxed{\text{Assume } \gcd(m, n) = q}$ Then $m^{\phi(n)} \equiv 0 \equiv m \pmod q$

$\Rightarrow q \mid m$

Then $\gcd(m, p) = 1$. Then $m^{\phi(n)} = (m^{p-1})^{q-1} \equiv 1^{q-1} \equiv 1 \pmod p$

$|U(\mathbb{Z}_p)| = p - 1$

$$\boxed{m^{ed} = m^{1 - t\phi(n)} = m \cdot (m^{\phi(n)})^{-t} = 0 \bmod q \qquad = m \cdot 1 = m \bmod p}$$

~~$m^{\phi(n)}$~~ So, $m^{ed} \equiv m \bmod p$, $m^{ed} = m \bmod q$ $\}$

$\Rightarrow \quad m^{ed} \equiv m \mod pq := n$

[$p \mid m^{ed} - m$ & $q \mid m^{ed} - m$ & $p \neq q$ both primes.
$\rightarrow pq \mid m^{ed} - m$]

$\mathcal{D}(\mathcal{E}(m)) = m \quad \forall \; m \in \mathbb{Z}_n$

E.g., Plain text GRAPH

$\mathcal{A} = \{A = 0, \ldots, Z = 25, \_ = 26, ? = 27, ! = 28, , = 29,$
$: = 30, " = 31, ¿ = 32\}$

$n = 33 = 3 \times 11$ Chose $e = 3$ which is coprime to $20 = \phi(33) = \phi(3)\phi(11) = 2 \times 10$

$\mathcal{E}(G) = 6^3 = 18 \mod 33 = S$
$\mathcal{E}(R) = 17^3 = 29 \mod 33 = ,$
$\mathcal{E}(A) = 0 = A$
$\mathcal{E}(P) = 15^3 = 9 \mod 33 = J$
$\mathcal{E}(H) = 7^3 = 13 \mod 33 = N$
$\mathcal{E}(GRAPH) = S , A J N$

$\boxed{3^{-1} = 7 \mod \phi(n) = 20}$

$\mathcal{D}(m) = m^7$
$\mathcal{D}(S) = 18^7 = 6 \pmod{33} = G$
$\mathcal{D}(,) = 29^7 = 17 = R$
$\mathcal{D}(A) = 0 = A$

$\phi(J) = 9^7 = 15 = P$
$\phi(N) = 13^7 = 7 = H$

$\phi(S, AJN) = \underline{GRAPH.}$

<u>Cryptanalysis</u> : (n, e) is in public domain.

But computing $\phi(n)$ (& p & q) is difficult when $n = pq$ with p, q large.

If we know p, q we know $\underline{n}$

If we know n & $\phi(n)$, then we can find $\underline{p, q.}$

Observe p & q are roots of $(x-p)(x-q)$

$$x^2 - (p+q)x + pq$$

$$= \underline{x^2 - (n - \phi(n) + 1) + n}$$

$n - \phi(n) = pq - (p-1)(q-1)$
$= (p+q) - 1$

we can find p & q if we know $\underline{n \text{ \& } \phi(n).}$

<u>Quadradic residue</u>

Suppose $n \in \mathbb{N}$ & $a \in \mathbb{Z}$ s.t.

$\gcd(a, n) = 1$

Then a is a quadradic residue modulo n if the eq^n $x^2 \equiv a \mod n$ has a sol^n.

(looking for a sol^n is $\mathbb{Z}/n$)

If a is not a quadratic residue modulo n then it is called a non-quadratic residue modulo n.

E.g., $x^2 \equiv 0 \mod n$, $x^2 \equiv 1 \mod n$ have sol'ns

$x^2 \equiv 2 \pmod 3$ has no sol'n.

2 is ~~not a quad~~ non-quadratic modulo 3.

check: $x^2 \equiv 3 \mod 4$