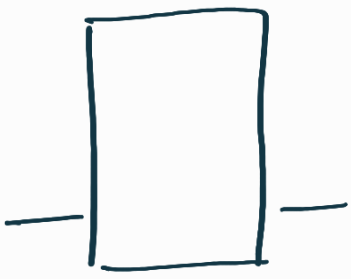


Black box computes an unknown periodic function $f(x)$

Find the period

classically : hard problem

However Quantum: easy ★

Let N be a positive integer ($N \geq 2$)

. Modulo N multiplication

Let $G_N = \{ a : \gcd(a,N) = 1 \text{ and } 1 \leq a < N \}$

a & N are relatively prime

G_N is a group under Multiplication Modulo N

$|G_N|$ = order of group = $\phi(N)$ = Euler's totient function

if $N = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ = prime number decomp. of N

$$\phi(N) = p_1^{n_1-1}(p_1-1) \cdot p_2^{n-1}(p_2-1) \cdots\cdots$$

• Order of a is smallest number m such that $a^m \equiv 1 \pmod N$

→ from Group Theory

→ m divides $\phi(N)$

→ if a is relatively prime to N then $a^{\phi(N)} \equiv 1 \pmod N$

→ $f(x) \equiv a^x \pmod N$

$f: \mathbb{Z} \longrightarrow G_N$

$\boxed{f(m) = 1} \Rightarrow f(x) = f(x+m)$

$a^x = a^x \cdot \underbrace{a^m}_{1} = a^{x+m}$

Period of $f(x)$ is m = the order of a

Problem: Given N find the prime factors of N.

Simplest case: $N = pq$ = product of two primes

Question: N is known. Find p (or q).

Classically: very hard.

Example: Try every prime number between $2, \dots, \sqrt{N}$

Shor's Algorithm:

Pick a random a.

Find the period of $f(x) = a^x \pmod N$

m: we know $m \mid \phi(N) = (p-1)(q-1)$

(period)

$= pq - p - q + 1$

$= N - (p+q) + 1$

Find a few more such orders

$a \to m$

$a' \to m'$

$a'' \to m''$

} find least common multiple } get $\phi(N)$

You now know $N = pq$

$N + 1 - \phi(N) = p + q$

} find p and q

---

* RSA public key crytosystem

Rivest, Shamir, Adelman

if a is relatively prime to N

$$a^{\phi(N)} \equiv 1 \pmod N$$

$$\to a^{\phi(N)+1} \equiv a \pmod N$$

If you know the prime factors of N, then you can find $\phi(N)$

$$N = pq \longrightarrow \phi(N) = (p-1)(q-1)$$

find x that divides $\phi(N)+1$

" y such that $xy = \phi(N)+1$

$$a^{xy} \equiv a \pmod{N}$$

$$(a^x)^y \equiv a \pmod{N}$$

$$f: a \longrightarrow a^x$$

$$g: b \longrightarrow b^y$$

f and g are inverses of each other

$$g(f(a)) \equiv a \pmod{N}$$

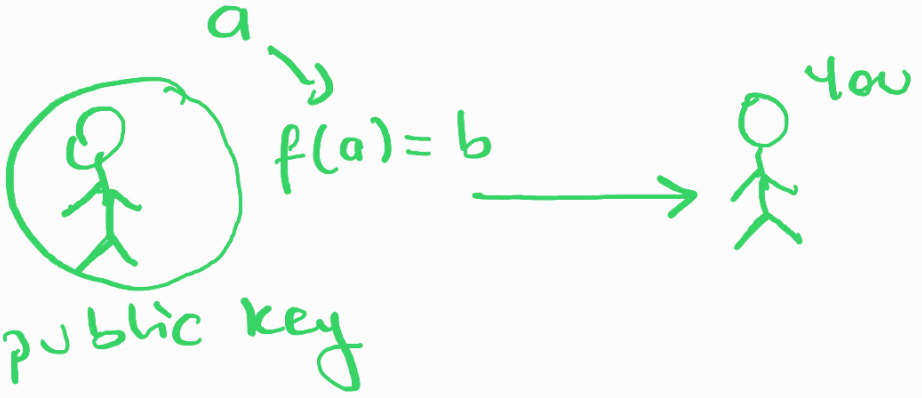
$$f(g(b)) \equiv b \pmod{N}$$

$f: a \longrightarrow b = a^x \pmod{N}$ encoding function (key = x, N)

$g: b \longrightarrow a = b^y \pmod{N}$ decoding function (key = y, N)

Public key: x, N

Private key: y, N, p, q } since factorization is difficult, knowing public key doesn't give you any info about the private key.



RSA cryptosystem

✱ Entanglement

$|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\chi\rangle_B$: product state

entangle if it is not a product state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

For two qubits A, B

$$|\psi\rangle_{AB} = \sum_{i,j=0}^{1} c_{ij} |i\rangle_A \otimes |j\rangle_B$$

$$C = \begin{bmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{bmatrix}$$

$|\psi\rangle$ is entangled $\Leftrightarrow$ $\det c \neq 0$

$|\psi\rangle$ is product $\Leftrightarrow$ $\det c = 0$

Let A and B be any systems

$\mathcal{H}_A$ = Hilbert space of A = n dimensional

$\mathcal{H}_B$ = Hilbert space of B = M dimensional

Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

$|\psi\rangle_{AB}$ = a state of the composite system A, B

→ Let $|\alpha_1\rangle, \dots, |\alpha_N\rangle$ be an orthonormal basis (o.c.b) of $\mathcal{H}_A$

" " $|\beta_1\rangle, \dots, |\beta_M\rangle$ " " "

" " of $\mathcal{H}_B$

↓

Expand $|\psi\rangle = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} |\alpha_i\rangle \otimes |\beta_j\rangle$

$C = \begin{bmatrix} c_{11} & \cdots & c_{1m} \\ \vdots & & \\ c_{n1} & \cdots & c_{nm} \end{bmatrix}$ is an $n \times m$ Matrix

Singular value decomposition of C

$C = UDV$

- $n \times n$ unitary
- $n \times m$ diagonal
- $m \times m$ unitary

$D = \begin{bmatrix} x & & 0 & \\ & x & & 0 \\ 0 & & \ddots & \\ & & & x \end{bmatrix}$ only the D_{ii} entries can be non-zero

$C = UDV$

$C^\dagger = V^\dagger D^\dagger U^\dagger$

$CC^\dagger = U \underbrace{DD^\dagger}_{\text{diagonal } n \times n} U^\dagger$ U diagonalizes $CC^\dagger$

V " $C^\dagger C$

Expand

$$|\psi\rangle = \sum_{i=1}^{N} \sum_{j=1}^{M} c_{ij} |\alpha_i\rangle \otimes |\beta_j\rangle$$

$$= \sum_{i,j,k,l} U_{ik} D_{kl} V_{lj} |\alpha_i\rangle \otimes |\beta_j\rangle$$

Define $|\tilde{\alpha}_k\rangle = \sum_i U_{ik} |\alpha_i\rangle$

$|\tilde{\alpha}_1\rangle, \ldots, |\tilde{\alpha}_N\rangle$ a new orb for $\mathcal{H}_A$.

Define $|\tilde{\beta}_l\rangle = \sum_j V_{lj} |\beta_j\rangle$

$|\tilde{\beta}_1\rangle, \ldots, |\tilde{\beta}_M\rangle$ is a new orb for $\mathcal{H}_B$

$$|\psi\rangle = \sum_{k,l} \underbrace{D_{kl}}_{d_k \delta_{k0}} |\tilde{\alpha}_k\rangle \otimes |\tilde{\beta}_l\rangle$$

$$|\psi\rangle = \sum_k d_k |\tilde{\alpha}_k\rangle \otimes |\tilde{\beta}_k\rangle$$

Schmidt decomposition