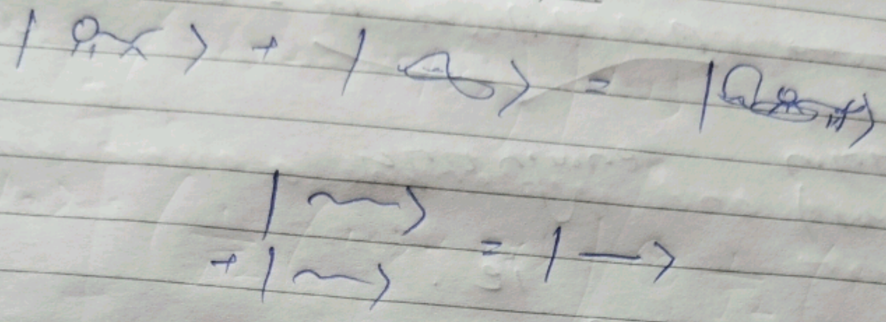
Date

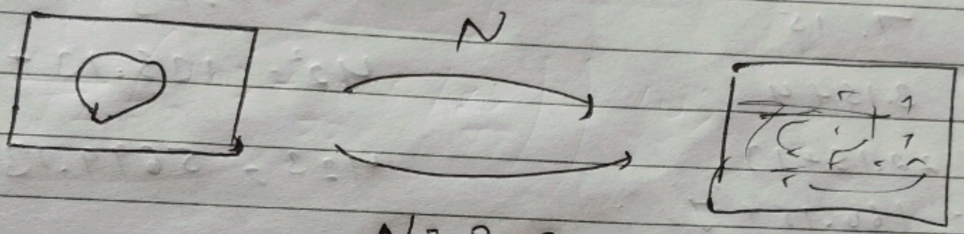
Page No.

DAY-16 TASK

Shor's Algorithm



RSA Encryption



N = ?.?

~~N = a.b~~

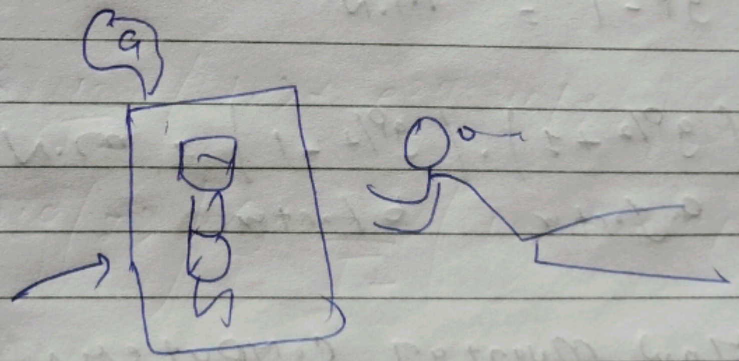
N = g.h

OR

N = a.b

g = a.c

gcd(N,g) = ?



Euclid's Algorithm

Shares a factor with N?

$g \longrightarrow g^{p/2} \pm 1$

unlikely likely!

Why $g^{P/2} \pm 1$?

$A, B \longrightarrow \underbrace{A.A.A.A \ldots A}$ = Something. B+1

(no common factors) enough time

ie.

$$A^P = M.B+1$$

Eg.

7, 15

$7^2 = 3.15+4$

$7^3 = 22.15+13$

$7^4 = 160.15+1$

42, 13

$42^2 = 135.13+9$

$42^3 = 5699.13+1$

N, g

$g^P = m.N+1$

$g^P - 1 = m.N$

$(g^{P/2}+1).(g^{P/2}-1) = m.N$

a. factor b. factor

How Quantum computers are fast!

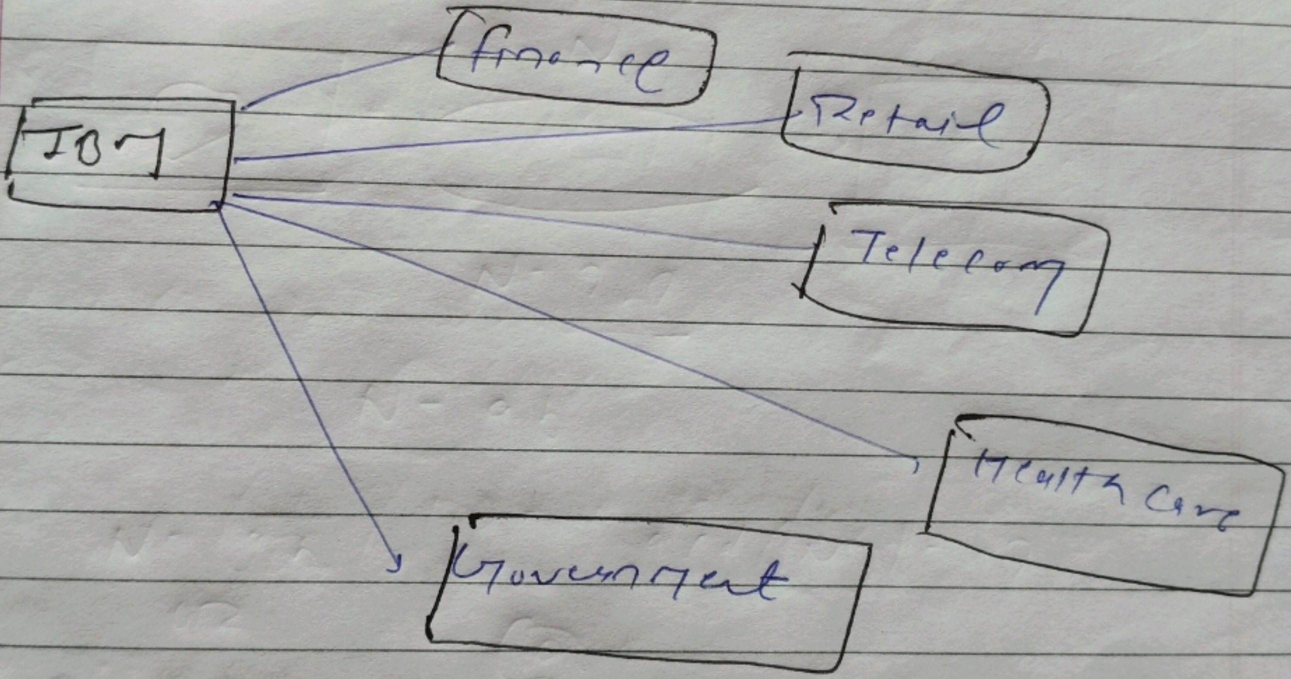
$$\boxed{|a\rangle + |b\rangle + |c\rangle \rightarrow \triangleright \boxed{f(x)} \triangleleft \rightarrow |f(b)\rangle}$$

NIST National Institude of Standards and Technology

IBM scientists co-developed all four quantum-safe encryption algorithms.

ML-KEN | ML-DSA | falcon | SPHINCS+

there are four algoritms.



Together, we can make the world quantum safe.

Crytographic Discovery

understand the quantum risks and quantum-safe Priorities

Date

Page No.

Identify

Cryptography footprint and Priorit
actions.

Initiate and implement a quantum-s
Program