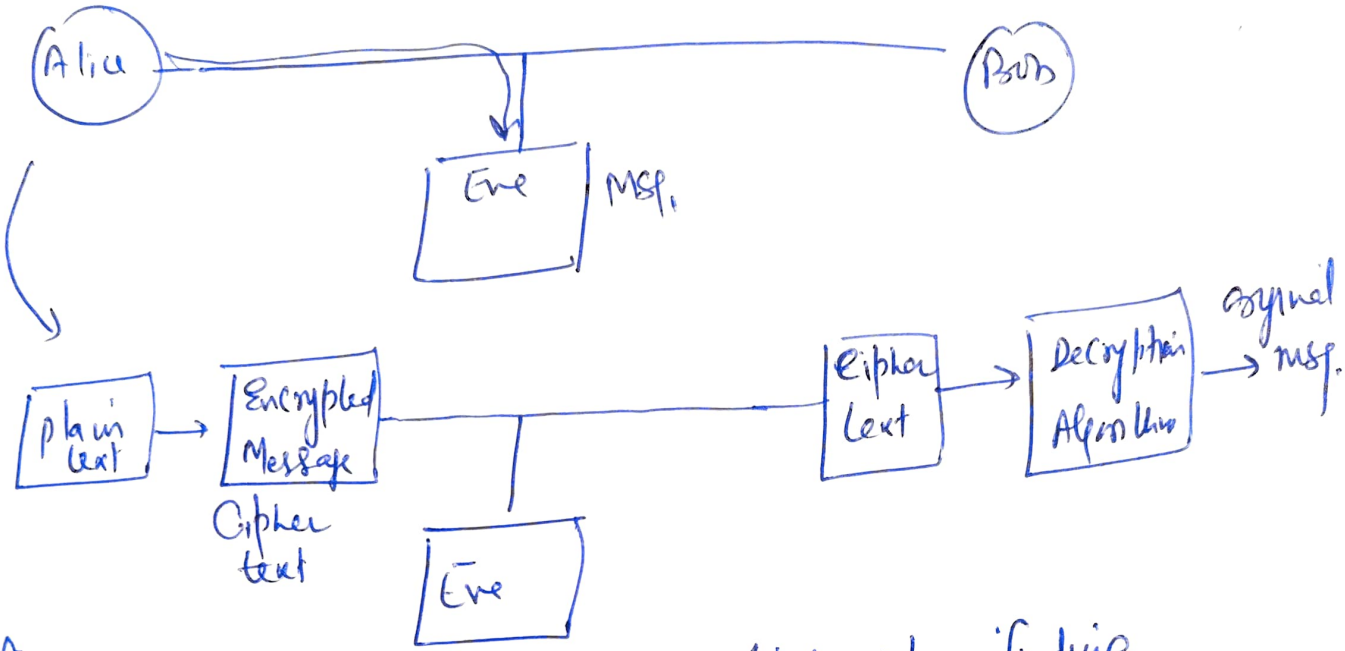
(Quantum Cryptography)

20 feb, 2024 ①

Classical Cryptography



RSA [take a large No.] } decryption after finding two prime No. of this large No.

MIT Shor's proposed an algorithm Shor's factoring Algorithm in 1994 in Polynomial time

Quantum Computer How many Qubit →

Post Quantum Cryptography

Advantage :- (1) Eve can't able to copy the qubit.

(2) If Eve try to take the message means Measurement take place, the qubit will be destroyed.

One time Pad protocol classical algorithm

Original msg. 0 1 1 0 1 1
Encrypted Key ⊕ 1 1 1 0 1 0
Encrypted msg. 1 0 0 0 0 1

Alice

Bob receive
Encrypted key ⊕ 1 0 0 0 0 1
Decrypted 1 1 1 0 1 0
0 1 1 0 1 1

A → Z
B → Y
C → X
D
)

AJAY

Quantum protocol BB84 protocol (used to generate encryption key)

1984
Bennett & Brassard

Step-1 Alice will toss a Coin n times H-0 T-1

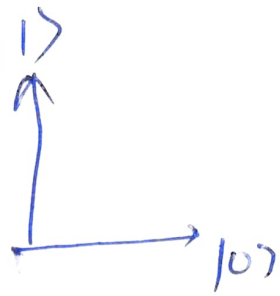
0 1 1 0 1 1 0 1 1 0 1 1 1 1 —

Alice will flip the Coin n times, Alice will decide the basis in which the qubit need to prepare.

H-0 — Computational basis
T → 1 Hadamard "

Computational basis $|0\rangle, |1\rangle$

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\rightarrow\rangle$ $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |\uparrow\rangle$



$|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = |\nearrow\rangle$

$|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = |\nwarrow\rangle$

H – 0 – Computational Basis
T – 1 – Hadamard "
$|\nwarrow\rangle$ denote 1 in Hadamard "
$|\nearrow\rangle$ " 0 " "

Alice qubit	1	2	3	4	5	6	7	8	9	10
Alice Random bits	0	1	1	0	1	1	1	0	1	0
Alice Random Bases	C	C	H	C	C	C	H	C	H	H
Alice Send	$\rightarrow\rangle$	$\uparrow\rangle$	$\nwarrow\rangle$	$\rightarrow\rangle$	$\uparrow\rangle$	$\nwarrow\rangle$	$\nwarrow\rangle$	$\rightarrow\rangle$	$\nwarrow\rangle$	$\nearrow\rangle$
Bob	H	C	H	H	C	H	C	C	H	C
	0,1 ✗	1 ✓	1 ✓	0,1 ✗	1 ✓	0,1 ✗	0,1 ✗	0 ✓	1 ✓	0,1 ✗

$|\langle 0|0\rangle|^2 = 1$ $\quad |\langle +|0\rangle|^2 = \left|\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right|^2 = \frac{1}{2}$

$|\langle 1|1\rangle|^2 = 1$ $\quad |\langle +|1\rangle|^2 = \frac{1}{2}$

$|\langle +|+\rangle|^2 = 1$ $\quad |\langle 0|+\rangle|^2 = \frac{1}{2}$

$|\langle -|-\rangle|^2 = 1$ $\quad |\langle 1|+\rangle|^2 = \frac{1}{2}$

Initially 1000 length key

After Bob Measurement & Basis Announcement } 500 length key

↓

250 length public key publically announced by Alice & Bob

↓

249 Matching, a fixed percentage of Error is Allowed.

Remaining 250 length are used as a encryption, decryption key

---