UNIT:-5

Device Independant - QKD

```
                    ┌─────────┐
                    │  START  │
                    └─────────┘
                         │
                         ▼
              ┌──────────────────────┐
              │ Prepare untrusted    │
              │ devices (black box)  │
              └──────────────────────┘
                         │
                         ▼
              ┌──────────────────────────┐
              │ Setup entanglement source│
              │ (trusted or untrusted)   │
              └──────────────────────────┘
                         │
                         ▼
              ┌──────────────────────┐
              │ Distribute           │
              │ entangled photons    │
              └──────────────────────┘
                         │
                         ▼
              ┌──────────────────────────┐
              │ Randomly choose          │
              │ Measurement setting x, y │
              └──────────────────────────┘
                         │
                         ▼
              ┌──────────────────────────┐
              │ Perform measurements     │
              │ and record outcomes a, b │
              └──────────────────────────┘
                         │
                         ▼
              ┌──────────────────────┐
              │ Publicly announce x, y│
              │ (NOT a, b)           │
              └──────────────────────┘
                         │
                         ▼
              ┌──────────────┐    ┌─Bell test rounds
              │ Seperate rounds├──►│ Key generation rounds
              └──────────────┘
                         │
                         ▼
              ┌──────────────────────┐
              │ Compute CHSH parameters│
              └──────────────────────┘
```

S < threshold   S > threshold
(No violation)   (Bell violation)

| Abort | | Extract Raw key bits |

QBER Estimation (sample)

→ Quantum bit error rate

$$QBER = \frac{\text{No of Incorrect bits}}{\text{Total no of received bits}}$$

| QBER too high | | Continue (QBER correction) |

= low (error correction) | Abort | | Classical error correction |

% of Mismatches bits b/w Alice & bob

after qw transm

Privacy amplification (hasing)

Authenticate Message
(MAC or PQC signatures)

< 36%

device trust

Final secure DI-QKD key

```
                    ┌─────────┐
                    │  END    │
                    └─────────┘
```