



# CRYPTOGRAPHY

## Securing Digital Communication

- SABARISH K.S (23CSR184)

# DESCRIPTION:

- Rise of Digital Communication
- Increased Reliance on Online Platforms
- Growing Volume of Sensitive Data
- Technological Advancements in Encryption
- Emergence of Cybersecurity Threats
- Need for Secure Data Transmission

# PROBLEM STATEMENT:

- High Incidence of Data Breaches
- Difficulty in Ensuring Data Privacy
- Impact on Personal and Organizational Security
- Legal and Ethical Concerns in Data Handling
- Need for Robust Cryptographic Solutions

# PROCESS:

- Data Encryption Request
- Key Generation
- Encryption Process
- Transmission of Encrypted Data
- Decryption Process
- Output Original Data



# CONCLUSION:

- Reduction in Data Breaches
- Improved Privacy Protection
- Trustworthy Digital Communication
- Protection of Sensitive Information
- Facilitated Secure Online Transactions

# FUTURE SCOPES:

- Improved Security with Quantum Cryptography
- Adaptive Encryption Algorithms
- Real-time Data Protection
- Cross-Platform Cryptographic Solutions
- Broader Implementation Across Industries



**THANK YOU!**