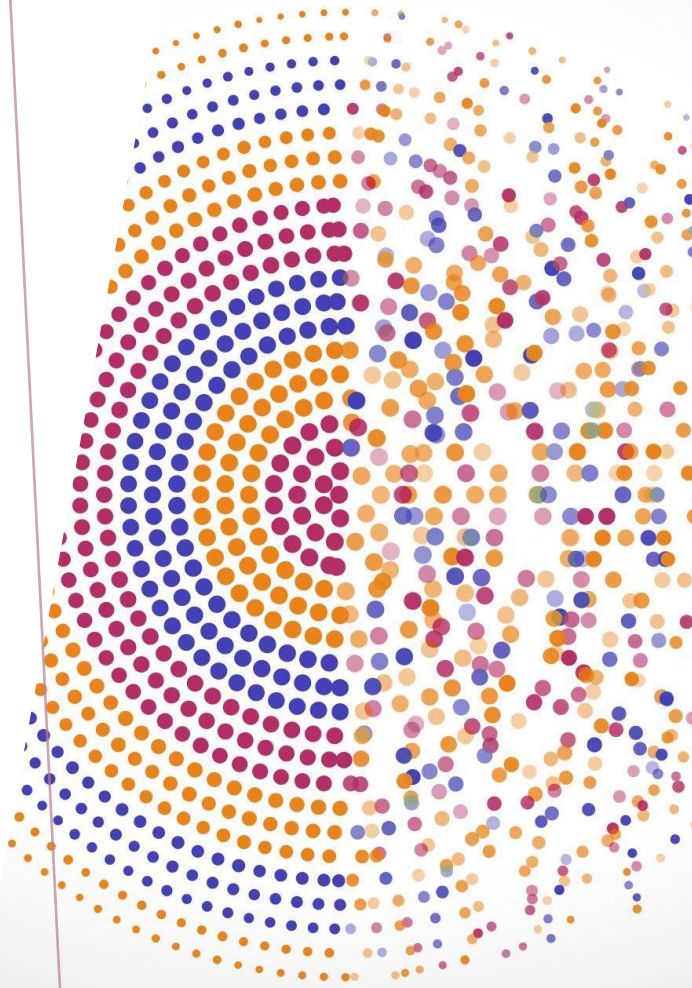
SECURE DATA HANDLING AND STORAGE: DATA ENCRYPTION AND SECURE DATA TRANSMISSION. SECURE DATA STORAGE AND ACCESS CONTROL. SECURE MULTI-PARTY COMPUTATION AND HOMOMORPHIC ENCRYPTION



DATA ENCRYPTION

- **Symmetric encryption:**
  - Uses one key to encrypt and decrypt
  - Stream and block ciphers
  - Initialization vectors and chaining
  - DES (Data Encryption Standard)
  - Blowfish and Twofish
  - RC5 and RC6
  - AES

SYMETRIC ENCRYPTION (CODE)

- https://github.com/anishLearnsToCode/DES
- https://www.schneier.com/academic/twofish/download/
- https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/
- https://www.geeksforgeeks.org/rc5-encryption-algorithm/
- https://www.educative.io/answers/how-rc6-encryption-algorithm-works
- https://onboardbase.com/blog/aes-encryption-decryption/

ASYMMETRIC ENCRYPTION

- **Asymmetric encryption:**
  - uses two keys: public and private
  - Methods:
    - Factoring prime numbers (the basis of the RSA algorithm)
    - Discrete logarithm
    - Diffie-Hellman Key Agreement Protocol
    - Elliptic Curve Cryptography
  - Slower than symmetric encryption and is also weaker per bit of key length

ASSYMETRIC ENCRYPTION (CODE)

- https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

- **Reading material:**
  - https://www.sciencedirect.com/science/article/pii/B9780124171428000054
  - https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
  - https://nordvpn.com/blog/block-cipher-vs-stream-cipher/

SECURE DATA TRANSMISSION

Transport Layer Security (TLS) ensures encrypted data transit

Secure file transfer protocols (e.g., SFTP, HTTPS)

Avoid unencrypted communication channels

SECURE DATA STORAGE

- Encrypt data at rest
- Use secure cloud storage providers with compliance certifications
- Implement regular data backups and disaster recovery plans
- Best Practices: Access control policies (e.g., Role-Based Access Control - RBAC)

ACCESS CONTROL

Principles of least privilege (PoLP)

Multi-factor authentication (MFA)

Audit and monitor access logs

ADVANCED CRYPTOGRAPHIC TECHNIQUES

- **Secure Multi-Party Computation (SMPC):**
  - Allows collaborative computation without revealing individual data inputs
  - Applications: Collaborative AI model training
- **Homomorphic Encryption:**
  - Perform computations on encrypted data without decryption
  - Applications: Secure AI inference and model evaluation