Page No. :

Date :

Name - Pawar mehul P

Roll No - 28

Class - MCA - 1

Subject - ION

Assignment - 1

Page No. : 1
Date :

① list All Symmetric key Algorithms
- AES (Advanced Encryption standard)
- DES (Data Encryption standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in-replacement for DES or IDEA)
- RC4 (Rivest ciphes 4)
- RC5 (Rivest ciphes 5)
- RC6 (Rivest ciphes 6)
- 3DES
- CAST5
- Camellia

2) list All Asymmetric key Algorithms
- RSA (Rivest-Shamis-Adlemen)
- DSA (Digital signature Algorithm)
- Diffie-Hellman key exchange
- X448 key exchange
- Elliptic curve cryptography
- ECC
- Ed448 signing
- X25519 key Exchange
- Ed25519 signing

③ list the algorithm for message digest
- MD5 (message Digest 5), MD2, MD4, MD6
- SHA-1 (Hash secure Hash Algorithm 1)
- HashClash
- Hash function security summary