# Unit 1 (Book – STALLING)

1. Euclidian Algorithm (5 Marks)
2. Calculate GCD (5 Marks)
3. Numerical on GCD (5 Marks)
4. Modulus questions (5 Marks)
5. Fermat theorem (5 Marks)
6. Euler theorem (5 Marks)
7. Pseudo Random Number (10 Marks) (5-6 QUESTIONS ON IT) - STALLING
   1. PRNG
   2. TRNG
   3. TRF

# Unit 2 (Book – Kahate n Stalling)

1. Basic Security Systems
2. Basic Security Services
3. Basic Security Model
4. CIAAN
5. Mono alphabetics Cipher Numerical and Theory *(GFG FOR NUMERICAL)*
6. Ceaser Cipher Numerical and Theory *(GFG FOR NUMERICAL)*
7. Playfair Cipher Numerical and Theory *(GFG FOR NUMERICAL)*
8. Hill Cipher Numerical and Theory *(GFG FOR NUMERICAL)*

# Unit 3 (Book - Stalling)

1. Difference between Symmetric and Asymmetric
2. Diff between Block and Stream Cipher
3. Difference between public and private key cryptography
4. Principles of public key cryptosystems
5. AES
6. DES
7. RC4
8. El-Gamal
9. Diffie Hellman *(Numerical)*
10. Hash Function
11. Hardware Stream Cipher – *(Stinson Book chapter 2)*
12. Modes of operation / Algorithmic Modes
    1. Explain
    2. Mode which works on stream cipher
    3. Mode which works on block cipher
13. SHA-512
14. MD5

# Unit 4

1. Digital Signature
2. RSA *(Numerical)*
3. ECC
4. ECC vs RSA

# Unit 5 (Book – William Stalling)

1. Zero Knowledge Protocol – MOST IMP
2. Key management
   1. Application
   2. Drawback
   3. Types
   4. Methods of Key Distribution
3. Cryptocurrency
   1. Anything can come e.g., BITCOIN
4. E-Commerce Cash Payment
5. Different methods of receiving anonymous cash on E-Commerce
6. Cryptology in Contact Tracing Applications
7. Issue related to Quantum Cryptanalysis

# Unit 6

1. What is post quantum cryptology
2. Code based cryptosystem
3. McEliece Cryptosystem
4. Lamport signature scheme
   1. Numerical on Lamport