- Encryption / Cipher Systems
  - Caesar
  - Vigenere
  - Hill
  - Affine
  - DES (S-DES)
  - Cryptosystem Tuples (P, C, K, E, D)
  - Extended Euclidean Algorithm
- Public-Key Cryptosystem
  - Diffie Hellman (Key Exchange Protocol)
  - RSA
    - Ron Rivest
    - Adi Shamir
    - Len Adleman
- Hashing
  - 3 Properties of a Hash Function
    - Preimage
    - 2nd Preimage
    - Collision
  - MD5
    - Ron Rivest
  - SHA-1 → SHA-256
- Message Authentication
  - “Error” checking
- Passwords
  - Protection
    - Hashing
    - Salting
  - Cracking
    - Rainbow Tables
- Internet Security
  - SSL Handshake Protocol
- Attacks
  - Buffer Overflow
  - Code Injection
  - Privilege Escalation Attacks
  - Kali Linux