Cognizant Class 1

28 February 2020 16:40

- Substitution Ciphers
  - Monoalphabetical Cipher
  - Polyaplhabetic caesar cipher
  - Using a key to shift alphabet
  - Columnar transposition
- Cryptography & Cryptanalysis
- Hieroglyphs
- Steganography
- Security services of crypt..
  - Confidentiality
  - Data integrity
  - Authentication
  - Non-repudiation
- Cryptography Primitives
  - Encryption
  - Hash function
  - Message auth. Codes
  - Digital signatures
- Types of cryptosystems
  - Symmetric key encryption
    - Block cipher
    - Stream cipher
  - Assymetric: public key, private key
- DES
  - 64 bit block
  - 56 bit key
  - 16 round feistel network
- AES
- RC4
  - Stream cipher
  - Variable length key
  - Pseudo random bit generator
- RSA
- Hashing
  - MD5
- Cryptanalysis
  - Attacks: Passive, Active
- Tokenization
- Dictionary attack
  - Rainbow Table
- Man in Middle Attack
- Timing Attack

- Implementing feistel network
- Implement 3des
- Implement aes
- Search the .txt doc for email ids and phone numbers and encrypt(use regular
- Pdf doc with email ids and phone numbers , redact it
- U have n no of keys encrypt, send on a socket and decrypt (simulate man-in-t attack)
- Encrypt data in linux and go to windows and try to decrypt it (try android)

Feistel cipher algorithm

- Create a list of all the Plain Text characters.
- Convert the Plain Text to Ascii and then 8-bit binary format.
- Divide the binary Plain Text string into two halves: left half (L1)an
- Generate a random binary keys (K1 and K2) of length equal to the for the two rounds.
- First Round of Encryption

  a. Generate function f1 using R1 and K1 as follows:

  ```
  f1= xor(R1, K1)
  ```

  b. Now the new left half(L2) and right half(R2) after round 1 are a

  ```
  R2= xor(f1, L1)
  L2=R1
  ```

- Second Round of Encryption

  a. Generate function f2 using R2 and K2 as follows:

  ```
  f2= xor(R2, K2)
  ```

  b. Now the new left half(L2) and right half(R2) after round 1 are a

  ```
  R3= xor(f2, L2)
  L3=R2
  ```

- Concatenation of R3 to L3 is the Cipher Text
- Same algorithm is used for decryption to retrieve the Plain Text fr