Primary Reference: https://github.com/ashutosh1206/Crypton
Note: Implement each and every attack yourself and then start solving challenges related to that attack

Tutorials

1. Introduction to Cryptography by Christof Paar

Blogs to follow:

1. Prof. Matthew Green's blog: https://blog.cryptographyengineering.com/
2. David Wong: https://www.cryptologie.net/
3. Grocid: https://grocid.net/
4. Hellman's blog: http://mslc.ctf.su/;
5. Shiho Midorikawa's blog: https://elliptic-shiho.github.io
6. Filippo Valsorda's blog: https://blog.filippo.io/
7. Tokyo Westerns writeups: http://westerns.tokyo/writeups/

Tools/Libraries

1. Pycryptodome
2. Xortool
3. Cribdrag
4. Sage → *Important*
5. neca (Only for a special case of Coppersmith's attack on 512-bit RSA)

Roadmap

1. **Stream Ciphers**
    a. Caesar Cipher, Substitution Cipher
    b. Single-Byte XOR, Single Character XOR
        i. Cryptopals challenges: challenges 1-4
    c. Repeated Key XOR
        i. Cryptopals challenges: challenges 5-6
    d. CTF Challenges:
    e. Transposition Ciphers
        i. Vigenere3D from Seccon'17
2. **Block Cipher implementation**
    a. Using pycryptodome: Install and read the documentation
    b. Padding in block ciphers

i. PKCS#7 padding

1. Implement padding: Cryptopals Challenge 9
2. PKCS#7 validation: Cryptopals Challenge 15

c. Different modes of encryption

i. ECB mode
ii. CBC mode
iii. CTR mode

d. AES implementation in python using pycryptodome

i. ECB mode implementation: Cryptopals challenge 7
ii. ECB mode detection: Cryptopals challenge 8
iii. CBC mode implementation: Cryptopals challenge 10
iv. CTR mode implementation: Cryptopals challenge 18

e. Block size detection

i. Refer to: https://masterpessimistaa.wordpress.com/2017/04/07/block-size-detection/
ii. Implement

f. CBC-IV detection

i. Refer to: https://github.com/ashutosh1206/Crypton/tree/master/Block-Cipher/CBC-IV-Detection
ii. Implementation

g. ECB Byte at a Time Attack

i. Refer to Crypton for attack description
ii. CTF Challenges

1. Cryptopals challenge 12
2. BabyCrypt: CSAW Quals 2017
3. Locked Dungeons: Swamp CTF 2018

h. CBC Bit Flipping Attack

i. CTF Challenges

1. Cryptopals challenge 16
2. CNVService: ACEBEAR CTF 2018
3. Locked Dungeons 2: Swamp CTF 2018
4. USSH 3.0: CTFZone 2018
5. Into the Darkness: HackIT CTF 2018

i. CTR Bit Flipping Attack

i. CTF Challenges

1. Cryptopals challenge 26

j. CTR fixed-nonce Statistical Attack

i. CTF Challenges

1. Cryptopals challenge 20
2. Stack Overflow: SHA2017 CTF

k. CBC Padding Oracle Attack

        i. https://blog.skullsecurity.org/2013/padding-oracle-attacks-in-depth
        ii. https://blog.skullsecurity.org/2013/a-padding-oracle-example
        iii. CTF Challenges:
            1. Cryptopals challenge 17
            2. Whistleblower: Midnight Sun CTF Quals 2018
            3. Yunny, Asis Quals 18
        iv. Tools:
            1. Feather duster Padding Oracle Module
    l. AES/DES Time-Space tradeoff related tasks
        i. Spaces - IJCTF’20
    m. DES Weak Keys
        i.

3. **Number Theory**
    a. Lecture 7, 11-14 from Christof Paar
    b. Number Theory (Implement all)
        i. Euclid’s GCD
        ii. Extended Euclid’s Algorithm
            1. Implementation
        iii. Modular Arithmetic
            1. Modular Inverse
        iv. Euler’s Totient Function
        v. Chinese Remainder Theorem
    c. Mathematical Structures / Abstract Algebra
        i. Groups, Cyclic Groups
        ii. Rings
        iii. Fields, Finite Fields
    d. Hensel’s Lifting
        i. Bro, do you even lift? Confidence 19
    e. Tonelli Shanks
    f. Homomorphism, Isomorphism

4. **RSA**
    a. RSA Encryption/Decryption
        i. Implement unpadded RSA
    b. Challenges on RSA + Number Theory
        i. Intro-Challenges: Crypton- 12 challenges
        ii. RSAbaby: Codegate CTF Prequels 2018
    c. Common Modulus Attack
        i. Implementation
        ii. CTF Challenges
            1. RSA-1s-Fun: InCTF International 2017
            2. Secret FS: HITCON Quals 2017
            3. Three set of challenges from Code Blue
    d. Factorization techniques (Read and implement all)

- - - i. Fermat’s factorization
    - ii. Pollard’s p-1 factorization
    - iii. William’s p+1 factorization
  - e. Blinding Attack
    - i.
  - f. Wiener’s Attack
    - i. CTF Challenges
      1. Multi-Layer RSA: InCTF International 2017
      2. Complex RSA: Backdoor CTF 2017
  - g. Variant of Wiener’s Attack
    - i. CTF Challenges
      1. Throwback: InCTF International 2018
      2. Gracias: ASIS CTF Finals 2017
  - h. Coppersmith’s Attack
    - i. CTF Challenges
      1. Stereotypes: Backdoor CTF 2017
      2. Bazik: Meepwn CTF Quals 2018
      3. baby-Alice-Bob: InCTF International 2018
      4. Really Suspicious Acronym, Confidence 19
  - i. Hastad’s Broadcast Attack
    - i. HBA on unpadded messages
      1. Trinity, Nox 19
    - ii. HBA on padded messages
      1. Multicast: Plaid CTF 2017
  - j. Franklin Reiter’s related message attack
    - i. CTF Challenges
      1. RSA Padding: N1CTF 2018
      2. RSA-2: b00t2root’18
  - k. Boneh Durfee Method
  - l. Chosen Ciphertext Attack
    - i. Due to homomorphic property of RSA
    - ii. LSB Decryption Oracle
      1. Mixed Cipher: TWCTF 2018
    - iii. CCA2 Attack
      1. Request-Auth: InCTF International 2018
  - m. ROCA
    - i. Weird Crypto, Fireshell 19
  - n. Coppersmith Shortpad Attack
    - i. Drypto, Plaid’19

5. **Diffie Hellman**
   - a. DH
     - i. Read and Understand
     - ii. Attacks

            1. Small Subgroup Confinement Attack: Cryptopals Challenge 57
            2. Cookiegen Challenge: InCTFi 2019
    b. ECDH
        i. Read and Understand
        ii. Attacks
            1. Invalid Curve Point Attack: Cryptopals Challenge 59
            2. ECDH: De1CTF 2020
            3. Nonce reuse

6. **Discrete Logarithm Problem**
    a. DLP
        i. Baby Step Giant Step Algorithm
            1. Implementation
            2. CTF Challenges:
                a. DLP: SEC-T CTF 2017
        ii. Pollard's Rho Method
            1. Implementation
        iii. Pollard's Kangaroo Method
            1. Implementation
        iv. Pohlig Hellman Method
            1. Implementation
    b. ECDLP
        i. Baby Step Giant Step Algorithm
            1. Implementation
        ii. Pollard's Rho Method
            1. Implementation
        iii. Pohlig hellman Attack
            1. implementation
        iv. MOV attack
    c. Man-in-the-middle attack

7. **Elliptic Curves**
    a. Implementation
        i. Point addition
        ii. Point Doubling
        iii. Point multiplication
        iv. Refer to: https://github.com/ashutosh1206/Crypton/tree/master/Elliptic-Curves
    b. Trustica Video series on Elliptic Curve Fundamentals
    c. Andrea Corbellini: A Gentle Introduction
    d. Attacks
        i. Smarts Attack
        ii. Singular Curves

8. **Message Authentication Code**
    a. CBC-MAC

        - i. Implementation
        - ii. Attacks
            - 1. Forgery Attack
    - b. N-MAC
        - i. Implementation
    - c. P-MAC
        - i. Implementation
    - d. One Time Mac

9. **Hashing Algorithms**
    - a. Identification of Hash type
    - b. Attacks
        - i. MD5 collision
        - ii. Hash-length extension attack
            - 1. Eternal Game, TamuCTF 2020
        - iii. HMAC-vulnerability
            - 1.

10. **Authenticated Encryption**
    - a. AEAD
        - i. AES-GCM
            - 1. Implementation
            - 2. Attacks
                - a. Forbidden Attack
                - b. Authentication Weakness in GCM
                - c. CTF challenges
                    - i. Forbidden, Volga Quals 17
                    - ii. GenuineCounterMode, HackIm 19
    - b. AE
        - i. Encrypt and MAC
        - ii. MAC then Encrypt
        - iii. Encrypt then MAC

11. **General**
    - a. PRNGs
    - b. Shamir’s Secret Sharing Scheme
    - c. Zlib Compression, GPG
        - i. Drinks, InsomniHack 19
        - ii. flatCrypt, CSAW Quals 19
    - d. Meet In The Middle
        - i. 2Fun, Nox 19
    - e. LFSR, LCG
        - i. Shifter (LFSR), Volga Qual 19
        - ii. LG (LCG), Volga Quals 19
        - iii. zer0lfsr , Zer0CTF 2019

Topics to be added:

- ❏ Digital Signatures