Principles of Cybersecurity Midterm

Contents

[Security Mindset (cont’) | Classic Crypto 2](#_Toc117019334)

[Cryptography 2](#_Toc117019335)

[Symmetric Key Crypto 3](#_Toc117019336)

# TODO

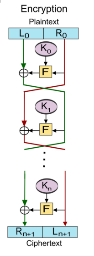
* Comparison between block and stream ciphers
* Comparison between linear and nonlinear cryptography

# Security Mindset (cont.’) | Classic Crypto

## Cryptography

* A cryptosystem consists of:
  + Key(s)
  + Encryption mechanism
  + Decryption mechanism
* **Symmetric key** in crypto is the concept where the same key for encrypting and decrypting is used
* Kerckhoffs’ principle states that the keys of a cryptosystem should be hidden but the mechanisms should be public. This is because algorithms never stay secret forever and it’s better to discover weaknesses beforehand.
* Different type of cryptos could be:
  + Codebook
  + One time pad (OTP)
    - One time pad is having the same length as the result text. Each character of the Onetime pad and the plain text is then XORed to get the cipher text
  + Stream cipher
  + Block cipher
* Caesar cipher builds on the algorithm to shift the alphabet

# Symmetric Key Crypto

* Stream cipher
  + Stream cipher is a generalized OTP
  + The key is stretched into a long **keystream**
  + Used to be the most populate of crypto
  + A5/1
    - Based on shift registers in the hardware
    - **How it works**
    - Uses 3 shift registers
    - Each iteration the formula majority is performed on three bits (Maj (x8, y10, 10)
    - A key is used as an initial fill for the registers
    - This was a very slow method
    - Now days the encryption is done within software due to fast processors
  + RC4
    - Based on changing lookup table
    - A table that contains **permutation** of the bytes between 0 and 255
* Block cipher
  + Works on larger chunks of data at the time
  + The plaintext and ciphertext contains **fixed-size blocks** bits
  + Iterated using a round function
    - The algorithm consists of a key and the output of the previous round
  + Example of block cipher is **Feistel Cipher**
* DES
  + Attacks by exhaustive key search
  + 56-bit key which nowadays are too small
  + Systems like 3-DES did improve the system to increase the key length. But this doesn’t always help due to attacks like in-the-middle attacks
* AES (Advanced Encryption Standard)
  + Variable key lengths
  + **Block size:** 128 bits, **key length:** 128,192 or 256 bits
  + Can be effectively implemented in an 8bit and 32bit CPU
  + Requires only one key
  + **Avalanche effect**; one small difference in the plaintext results in a big change in the cipher text
  + In short, the algorithm works by performing certain types of operation in multiple rounds on the plain text. The rounds usually are (10-14)
  + See online exactly how the encryption works
* TEA (Tiny encryption algorithm)
  + 64-bit block, 128 bits key
  + Has a weak round function so many rounds are required (32)
  + Uses a Magic number

## Overview of Linear Cryptanalysis

* Typical nonlinear functions are s-box which is the primary contribution of security of block ciphers
* Multiple blocks by chaining the blocks together
* ECB
  + Encrypt block independently
  + Use the same key repeatedly on different types of blocks
  + If a attacker can intercept the message it can be subject of Cut and Paste where the attacker mix the order of the messages
  + For example, because if we encrypt a block and the key and block is the same for two. If will result in for example an image leaving trace behind

A picture containing text

Description automatically generated

* CBC
  + Chain blocks together
  + Uses a initialization vector
  + Cut and paste could still be possible
* CTR
  + Block ciphers acts like a stream cipher
  + Popular for random access
  + Increases the initialization vector by one for each trip (no blocks are chained together)
* CIA
  + Confidentiality ©
    - No one is supposed to read what data or information is sent unless he is authorized
  + Integrity (I)
    - The ability to ensure that data is an accurate and unchanged representation of the original secure information
  + Availability (A)
    - The information concerned is always readily accessible to the authorized viewer
* Data integrity
  + Encryption provides confidentiality but does not provide integrity
  + The MAC address is often used for integrity
  + The MAC address serves as a checksum for the data
  + If a message has for example in CTR been changed the finale message (MAC) will not be the same. Therefore, the receiver can verify with the last message if it has been tampered with