Justin Ciocoi

Oct 3, 2023

CSCI 360 Class Notes

Cryptography and Cryptanalysis

AES

Overview

- 3 possible key sizes
    - 128/192/256 bytes
- Number of rounds varies based on key size
    - 10/12/14 rounds of AES respectively
- AES is *byte-oriented* whereas DES was *bit-oriented*
- Each round of AES consists of 4 layers
    - **Byte Substitution Layer**
        - Consists of 16 S-boxes which are:
            - *Identical*
            - The only *non-linear* elements of AES
            - *Bijective*, i.e., there exists a *one-to-one* mapping of input-output pairs
                - This means the S-box can be uniquely reversed
    - **Diffusion Layer**
    - Introduces *diffusion* in AES
        - Shift Rows Sublayer
            - 16-byte matrix
                - 1st row left alone
                - 2nd row circularly shifted left *once*

        - 3rd row circularly shifted left *twice*
        - 4th row circularly shifted left *thrice*
    - Mix Columns Sublayer
        - Each 4 byte column of the 4x4 matrix is treated as a vector and multiplied by a fixed 4x4 matrix
        - All arithmetic here is performed in GF(256)
        - This introduces diffusion as *every* output bit depends on *every* input bit
- **Key Addition Layer**
    - Very simple layer
    - For 16 byte state matrix *C* and 16-byte subkey *k*, the output of this round is:
        - $C \oplus k_i$
    - The subkey for *each* round is generated in the key schedule

- **Key Schedule**
    - *Number of subkeys* is equal to the *number of rounds +1*
    - Each round uses 32-bit *word-oriented* key schedule
    - Start with an initial *128-bit* key that is split into 4 *32-bit* words
    - Round Key 0 is $W[0] - W[3]$
    - For next round key ($W[4] - W[7]$)
        - $W[4] = (g * W[3]) \oplus W[0]$
        - $W[5] = W[1] \oplus W[4]$
        - $W[6] = W[2] \oplus W[5]$
        - $W[7] = W[3] \oplus W[6]$
    - g is a non linear function with 3 layers
        - The first layer is a linear shift to the left of the four words that are a part of the key
        - Next, each word will be passed through the same S-boxes used earlier in AES
        - Finally, the *8-bit* round coefficient, $RC[i]$, is XORed ($\oplus$) with the leftmost S-box output

DESX

- DES with AES' included key whitening

AES Decryption

- Since AES is not based on a Feistel network, its layers must be inverted in order for decryption to occur