Crypto V: Theory of Block Ciphers

Cryptographic Hardware for Embedded Systems
ECE 3170

Fall 2025

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading Assignment

- Please read Chapter 14 part 10 of the course textbook by Schneier

Confusion

- Hide the relationship between the plaintext, ciphertext and key
  - Consider an extreme case: a key dependent lookup table mapping 64 bits of plaintext to 64 bits of ciphertext
    - This would provide a very large search space
    - Problem: if the key has *n* bits, need $(2^n)*(2^{64}) = 2^{(n+64)}$ amount of memory
      - Note that 2^{40} = Terabyte (TB), and a single storage rack in a server farm can handle a few TB
    - Schneier says that this would provide sufficient security, but the course text was published in 1996; today there is agreement that a key size of at least 80 bits is needed
  - Modern block ciphers use much smaller tables (so-called “substitution boxes” or s-boxes)
    - Smaller size may allow brute-force attacks to succeed
    - In other words, the reduction in size helps make the block cipher computable with reduced memory but also helps the adversary

Table 12.6
S-Boxes

S-box 1:

14,	4,	13,	1,	2,	15,	11,	8,	3,	10,	6,	12,	5,	9,	0,	7,
0,	15,	7,	4,	14,	2,	13,	1,	10,	6,	12,	11,	9,	5,	3,	8,
4,	1,	14,	8,	13,	6,	2,	11,	15,	12,	9,	7,	3,	10,	5,	0,
15,	12,	8,	2,	4,	9,	1,	7,	5,	11,	3,	14,	10,	0,	6,	13,

S-box 2:

15,	1,	8,	14,	6,	11,	3,	4,	9,	7,	2,	13,	12,	0,	5,	10,
3,	13,	4,	7,	15,	2,	8,	14,	12,	0,	1,	10,	6,	9,	11,	5,
0,	14,	7,	11,	10,	4,	13,	1,	5,	8,	12,	6,	9,	3,	2,	15,
13,	8,	10,	1,	3,	15,	4,	2,	11,	6,	7,	12,	0,	5,	14,	9,

S-box 3:

10,	0,	9,	14,	6,	3,	15,	5,	1,	13,	12,	7,	11,	4,	2,	8,
13,	7,	0,	9,	3,	4,	6,	10,	2,	8,	5,	14,	12,	11,	15,	1,
13,	6,	4,	9,	8,	15,	3,	0,	11,	1,	2,	12,	5,	10,	14,	7,
1,	10,	13,	0,	6,	9,	8,	7,	4,	15,	14,	3,	11,	5,	2,	12,

S-box 4:

7,	13,	14,	3,	0,	6,	9,	10,	1,	2,	8,	5,	11,	12,	4,	15,
13,	8,	11,	5,	6,	15,	0,	3,	4,	7,	2,	12,	1,	10,	14,	9,

Diffusion

- Spread the influence of changing a few bits of plaintext or the key over as much of the ciphertext as possible
  - Helps hide statistical relationships

Combining Confusion and Diffusion

- Substitute (confuse) and permute (diffuse)
  - Product cipher
  - Substitution-permutation (SP) network
- Consider function ***f*** in DES
  - Diffusion: expansion permutation and P-box
    - Both are linear
  - Confusion: S-boxes
    - Nonlinear
  - All operations are fairly simple (fast) to compute
- Iterated block cipher
  - Two rounds of DES is not strong; five rounds must occur before all of the output bits are dependent on all of the input bits and all of the key bits
  - DES has 16 rounds

Feistel Networks

- Horst Feistel worked for IBM Research
- Take a block of length *n* and divide into two equal halves *L* and *R*
  - *n* must be even
- Define an iterated block cipher
- This function is reversible
- Therefore, a cipher based on a Feistel network is guaranteed to be invertible
- Note that reversibility is not dependent on f being reversible
- Further note that the same algorithm works for decryption

- L_i = R_{i-1}
- R_i = L_{i-1} XOR $f(R_{i-1}, K_i)$
  - where K_i is the subkey used in round *i* and *f* is the round function used

- L_{i-1} XOR $f(R_{i-1}, K_i)$ XOR $f(R_{i-1}, K_i)$ = L_{i-1}

Comments on DES

- If $C = E_k(P)$, then $C' = E_{k'}(P')$
  - where C', K' and P' are the bitwise complements of C, K and P
- Brute force attack complexity reduced by a factor of 2
- Simple relation:
  - If $E_k(P) = C$, then $E_{f(k)}(g(P,K)) = h(C,K)$
    - where f, g and h are simple functions, i.e., easy to compute
- A good block cipher has no simple relations

Weak Keys

- DES has been shown to have a few weak keys
- Not a practical problem: just avoid them in key generation
- Preferable to have all keys be equally strong

S-Box Design

- S-Box: a mapping from *m* bits to *n*
- Typically implemented as a look-up table
- Non-linear and non-degenerate, i.e., no way to compute the relation with a function
  - => must perform a look-up in memory!
- Boolean properties: balance of zeros and ones, no correlations between different bit combinations, avalanche effect
  - Avalanche: one bit of input should on average change approximately half of the output bits
- Provides strong resistance to cryptanalysis
  - In other words, forces the adversary to only use brute force attacks

Advanced Encryption Standard (AES)

- In 1997, NIST organized a public competition for a new cryptographic algorithm to replace DES
  - 15 algorithms were submitted from all over the world
  - The submissions were analyzed by NIST, the public, and especially by competing teams!
  - Workshops were held in 1998 and 1999, finally narrowing down to five submissions
  - Third and final workshop held in April 2000
  - In October 2000 NIST selected the algorithm of two cryptographers from Belgium, Vincent Rijmen and Joan Daemen, who names the algorithm Rijndael
  - NIST stated that all five candidates were excellent