Cryptanalysis
(암호분석)

Chapter 5 – Part 1

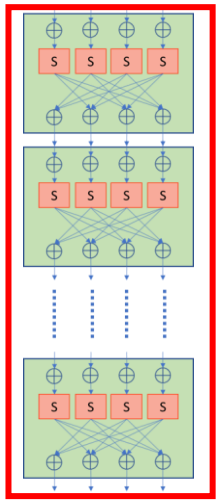
2020.4

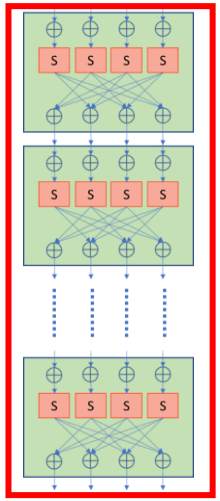
Contents

Chapter 5
- Part 1

- Generic Attack
- Brute force attack: Exhaustive key search
- Meet-in-the-Middle Attack
- TMTM: Time Memory Trade Off
- Slide Attack

Chapter 5
- Part 2





Cryptanalysis – 암호 분석(공격)

- 암호분석의 목표
  - 실용적 목표: 암호문과 관련된 **암호키**, **평문의 정보**를 획득
  - 이론적 목표: 암호 설계자의 주장에서 모순을 발견

- 안전성 분석의 고려사항
  - 공격 조건 (공격 시나리오, 모델)
  - 가용 자원 (공격자의 능력)
  - (가능한 경우만) 사용 환경의 특이 사항

공격자의 자원(resource)

- 공격에 필요한 기본 자원들
  - Computing Power
  - Memory
  - Data(Plaintext/Ciphertext/Key)
- 부가정보(구현정보)
  - Blackbox Cryptography
  - Greybox Cryptography
  - Whitebox Cryptography
- 새로운 자원의 도입
  - DNA/Molecular Computing
  - Quantum Computing

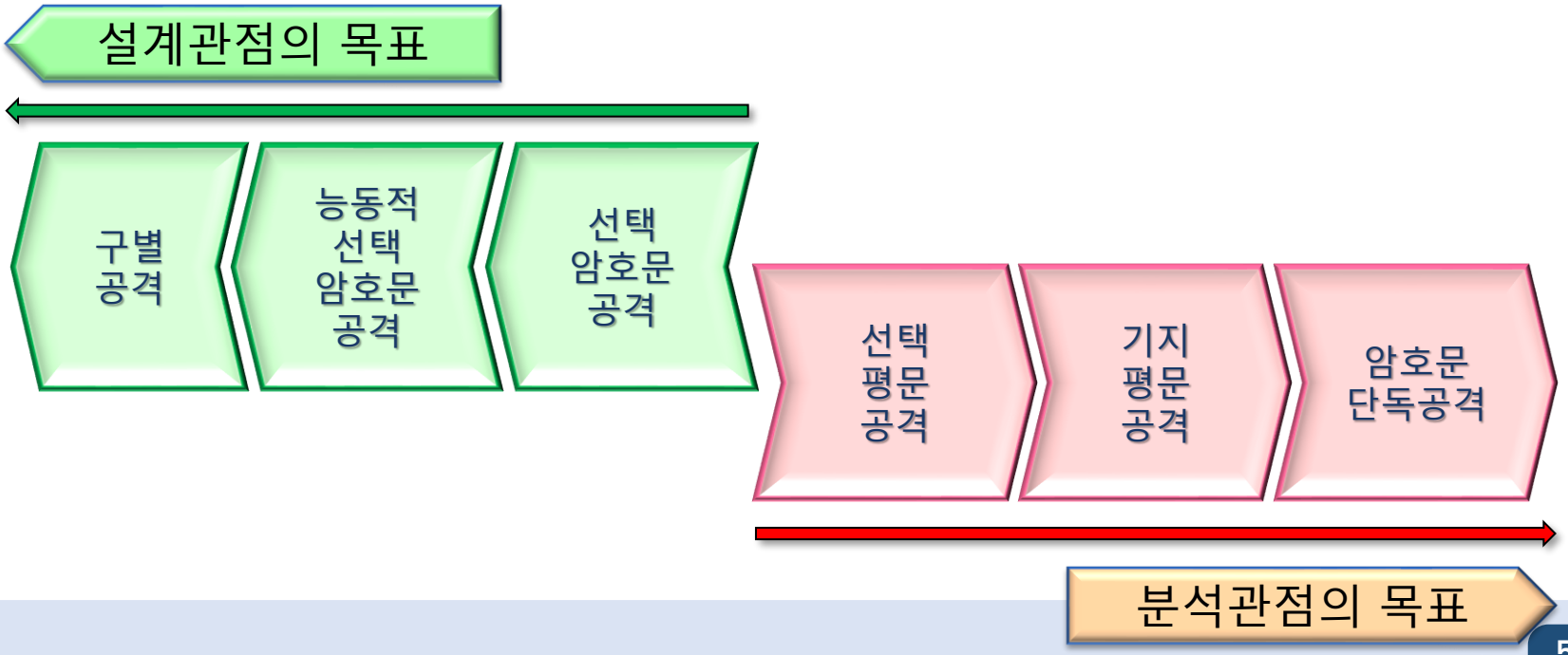
공격 모델

- Ciphertext Only Attack(암호문 단독 공격)
  - 암호문만으로 공격하는 방법 (+ 평문 정보 예상)
  - 예: 도청 등으로 수집한 암호문의 해독
- Known Plaintext Attack (기지평문 공격)
  - 획득한 평문과 암호문 쌍을 이용한 공격
  - 예: 헤더가 예측되는 암호문의 해독
- Chosen Plaintext Attack (선택평문 공격)
  - 공격자가 원하는 평문, 암호문 쌍을 얻을 수 있는 환경의 공격
  - 예: 획득한 암호장비를 이용한 암호문의 해독
- Chosen Ciphertext Attack (선택암호문 공격)
  - 공격자가 복호화 능력까지 갖는 환경에서의 공격
  - 예: 공격자가 암호문을 만들어 복호기에 넣어볼 수 있는 환경

예: A, B가 암호통신을 하는 경우, 공격자가 중간에 개입하여 A의 암호문을 가로채고 B에게 임의로 만든 암호문을 주면 B가 A에게 (공개채널 또는 평문으로) 잘못되었음을 알리면서 공격자가 보내준 암호문에 대응하는 평문을 보여준다.

공격과 방어

- 설계자 관점
  예상 공격 모델에 대한 안전성 보장을 목표로
- 공격자 관점
  가능한 적은 자원으로 공격하는 방법을 목표로



블록암호의 공격법

암호분석 과목:
- 암호키 전수조사(exhaustive key search)
- TMTO

- Generic Attack/Brute Force Attack
  - 블록암호의 공통적인 문제를 이용한 공격
  - TMTO, Biclique 등

- Key Recovery Attack (Using distinguisher)
  - 랜덤함수와 구별되는 특징으로부터 암호키를 찾는 공격기법
  - 차분분석(DC), 선형분석(LC) 등

Distinguisher 기반의 공격은
암호분석 과목에서 중요하게
다룰 부분임

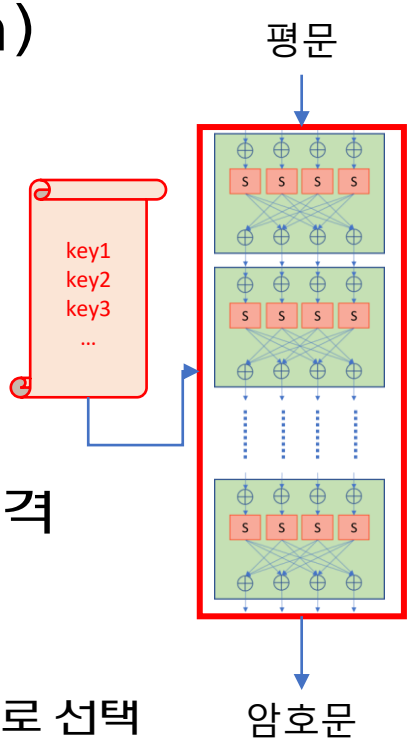
- Algebraic Attack
  - 대수적 구조를 이용한 키복구 공격
  - 연립 방정식을 구성하고 Solver(Groebner basis, PolyBori, SAT-solver)로 해를 찾는 방식

이번 과정에서 다루지 않음

Brute Force Attack (1)

- 암호키 전수조사 (Exhaustive key search)
  - 모든 키를 시도해보는 방법으로 공격
  - 암호키의 크기가 작은 경우만 가능

- 예: TC20의 공격 (기지평문 공격)
  - TC20: 블록크기=키크기=32비트
  - 주어진 평문, 암호문으로부터 암호키를 찾는 공격
  - 공격 알고리즘
    - 2^{32}가지 암호키 모두를 대입하여 평문을 암호화
    - 주어진 암호문과 같은 것이 나오면 올바른 암호키 후보로 선택
    - False alarm 확률: $1/2^{32}$ (잘못된 키가 암호키 후보가 될 확률)



Double Encryption

- 블록암호 안전성 문제
  - 암호키 전수조사가 가능하다면?

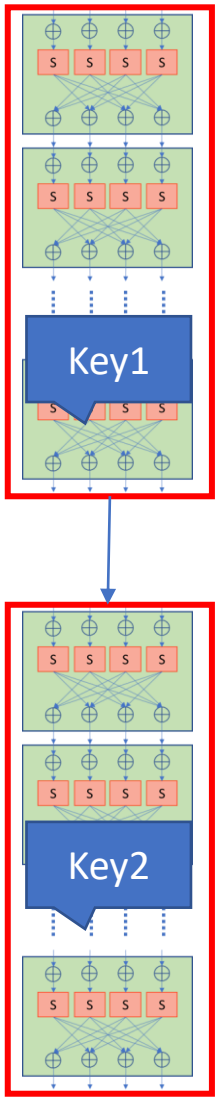
    → 암호키 크기를 늘이면 됨

DES의 56비트 암호키가 작다면,
2배로 늘이면 된다.

56비트 전수조사에 1초가 걸린다면,
112비트 전수조사에는23억년 걸린다.

- Double Encryption
  - 암호 알고리즘: C = E(P, key)
  - 강화된 알고리즘: C = E(E(P,key1), key2)
  - 블록 크기는 그대로, 암호키 크기는 2배로 강화

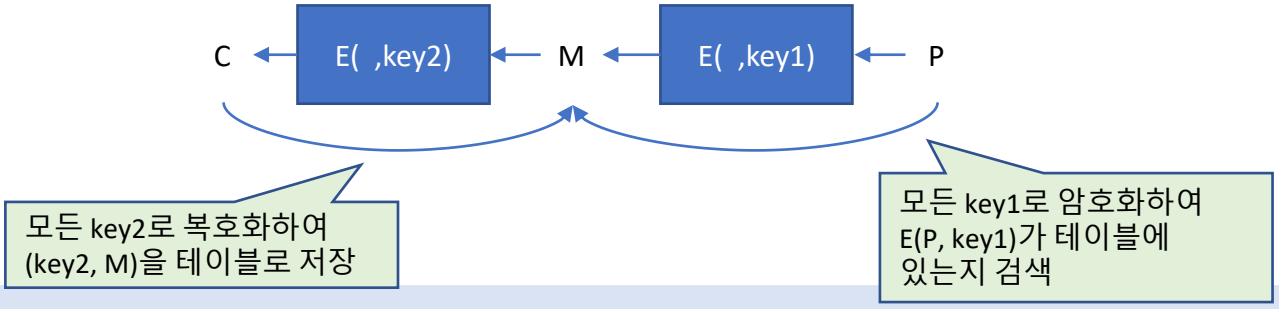
  → 키 전수조사 공격에 안전할까?



Brute Force Attack (2)

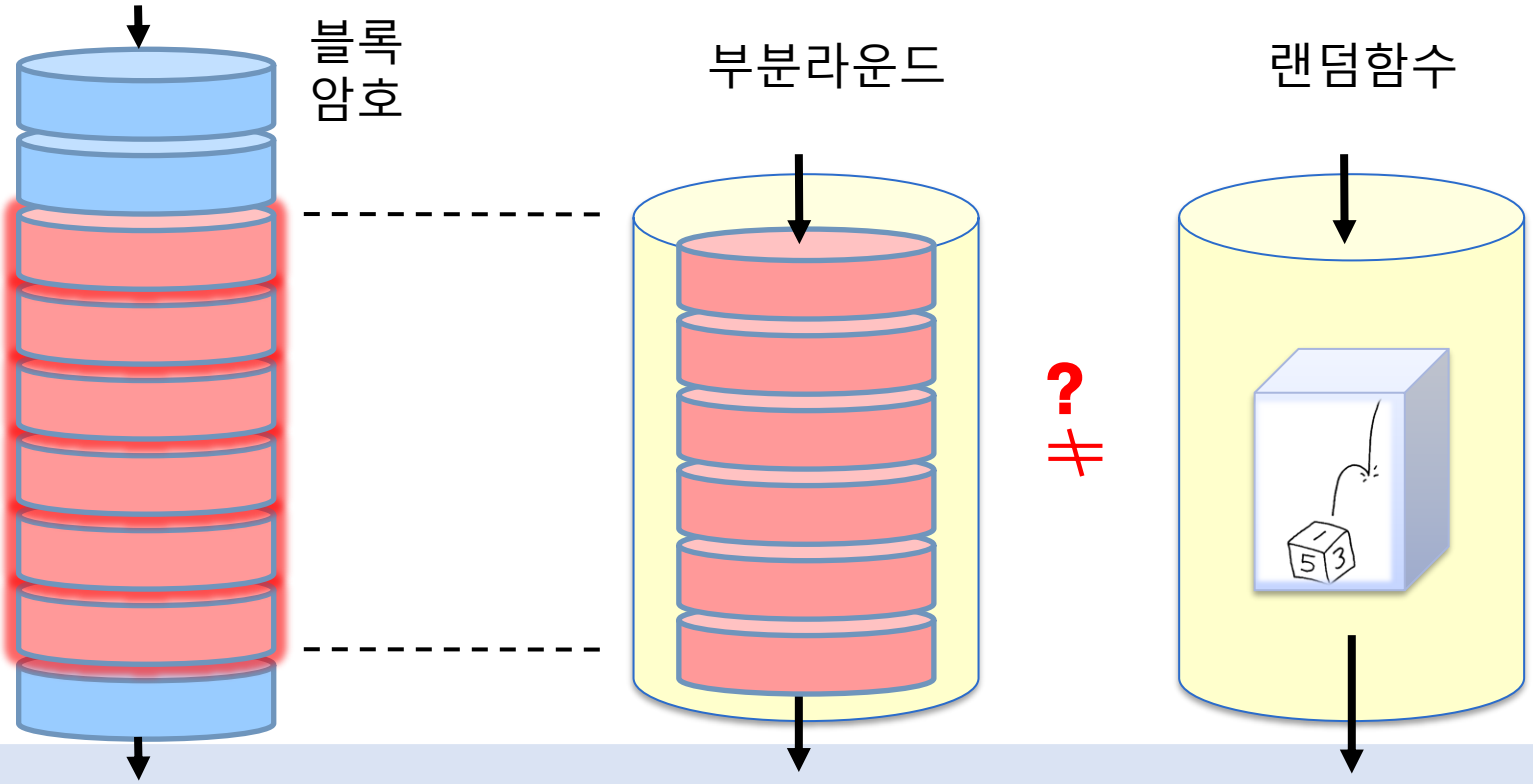
- Double Encryption의 안전성
  - C = E(P, key) 키 크기: 2^k → 공격량: 2^k 암호화 계산
  - C = E(E(P,key1), key2) 키 크기: 2^{2k} → 공격량: 2^{2k} 을 기대하지만 → MITM attack을 이용하면 2^{k+1} 로 공격이 가능함
  - 결론적으로 double encryption의 안전성은 강화되지 않음

- MITM(Meet-in-the-Middle) Attack 알고리즘
  - 주어진 평문(P)와 암호문(C)에 대하여, 암호키 key1, key2를 찾는 공격
  - 암호문 (C)를 가능한 모든 key2로 복호화하여 테이블에 저장한다.
  - 평문(P)를 가능한 모든 key1으로 암호화하여 저장해둔 테이블에서 찾는다.



Distinguisher를 이용한 공격

- 블록암호의 부분라운드와 랜덤함수를 구별하는 방법으로 암호키를 찾는 공격법



다음엔…

- Brute Force Attack
  - 키 전수조사 공격
  - Meet-In-The-Middle Attack

다음 시간에
Toy Cipher에 대한 공격을
Python으로 구현

- 랜덤함수와의 구분을 이용한 공격
  - DC
  - LC

Chapter 6,7에서
원리 및 구현