Cryptanalysis
(암호분석)

암호공격과 안전성 개념

2023.3

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)

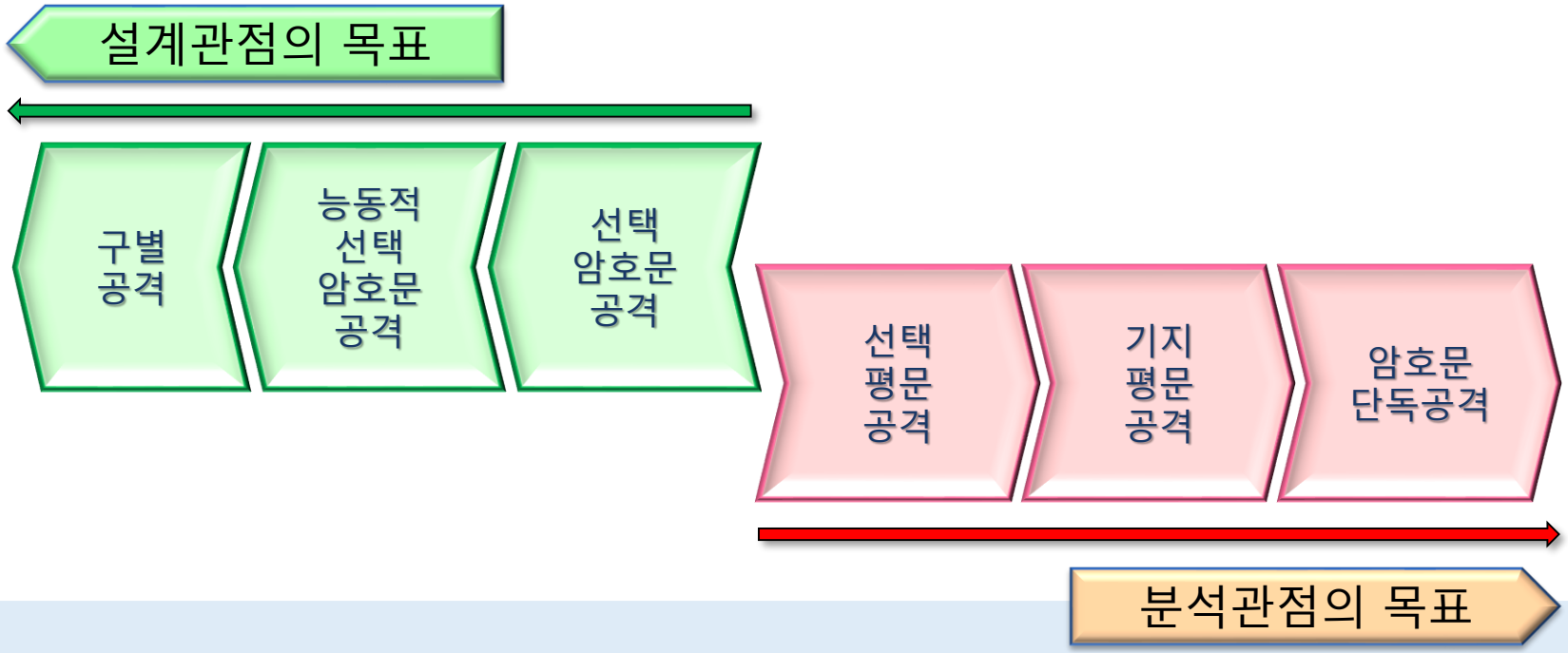
- 공격에 필요한 기본 자원들
  - Computing Power
  - Memory
  - Data(Plaintext/Ciphertext/Key)
- 부가정보(구현정보)
  - Blackbox Cryptography
  - Greybox Cryptography
  - Whitebox Cryptography
- 새로운 자원의 도입
  - DNA/Molecular Computing
  - Quantum Computing

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

공격과 방어

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

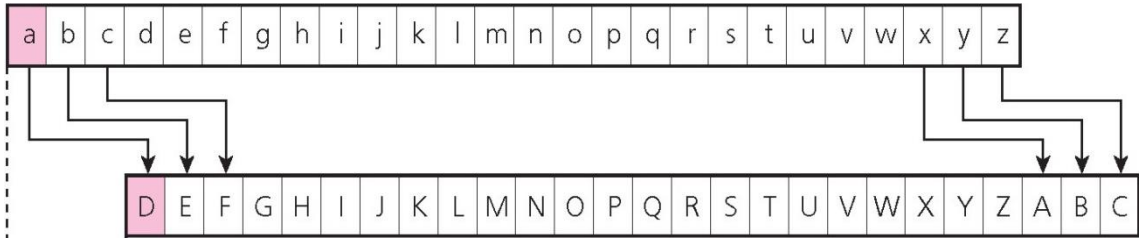


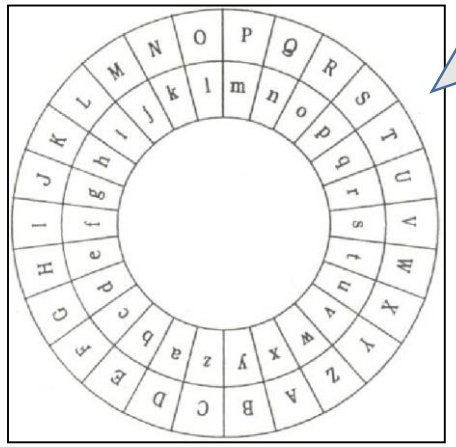
안전한 암호의 조건(1) – 암호키 공간

- 씨저 암호(Caesar Cipher)
  - 평문(P), 암호문(C), 암호키(K)의 관계

$$C = E_K(M) = M + K \bmod 26$$

K=3 인 경우

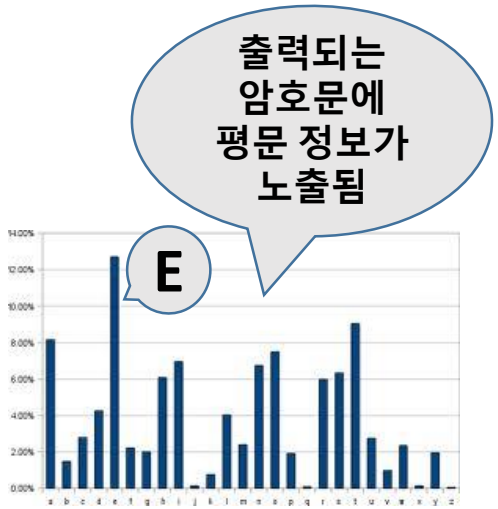




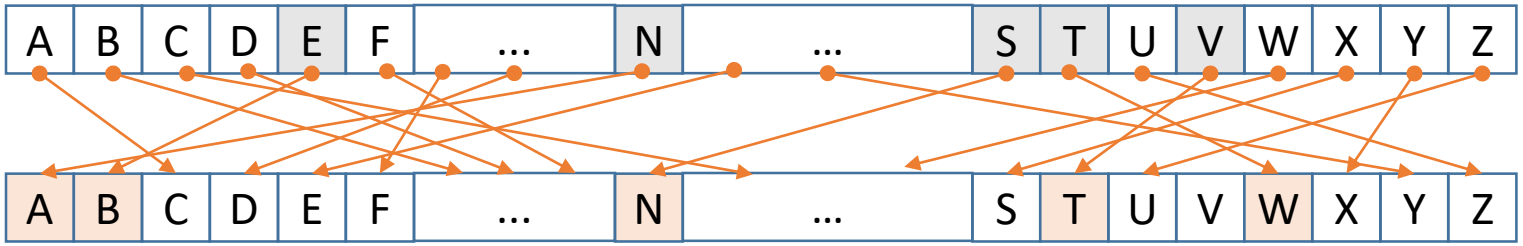
암호키의
종류(26가지)가
너무 적어
안전하지 않음

안전한 암호의 조건(2) – 평문/암호문의 관계

- 단순치환 암호
  - 암호키(=치환표): A~Z를 무작위로 섞는 방법
  - 암호키의 종류는 $26! \approx 4 \times 10^{26}$ 로 충분히 큼



E(seventeen) = nbtbawbba



안전한 비밀키 암호의 조건

- 안전한 암호화의 조건
  - 암호문은 **난수**와 구별할 수 없어야 한다.
    (평문을 추측할 수 있는 정보를 제공하지 않아야 한다)
  - 암호키는 공격자가 예측할 수 없어야 한다.
    (키 공간이 충분히 크고, **랜덤하게 선택**되어, 공격자가 키를 맞출 확률이 낮아야 한다)