2024/07/04, 2024 보안 기초 세미나

암호학과 네트워크 보안

- 1장 보안 개요, 4장 암호수학 -

김 혜 정(hyejeong@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

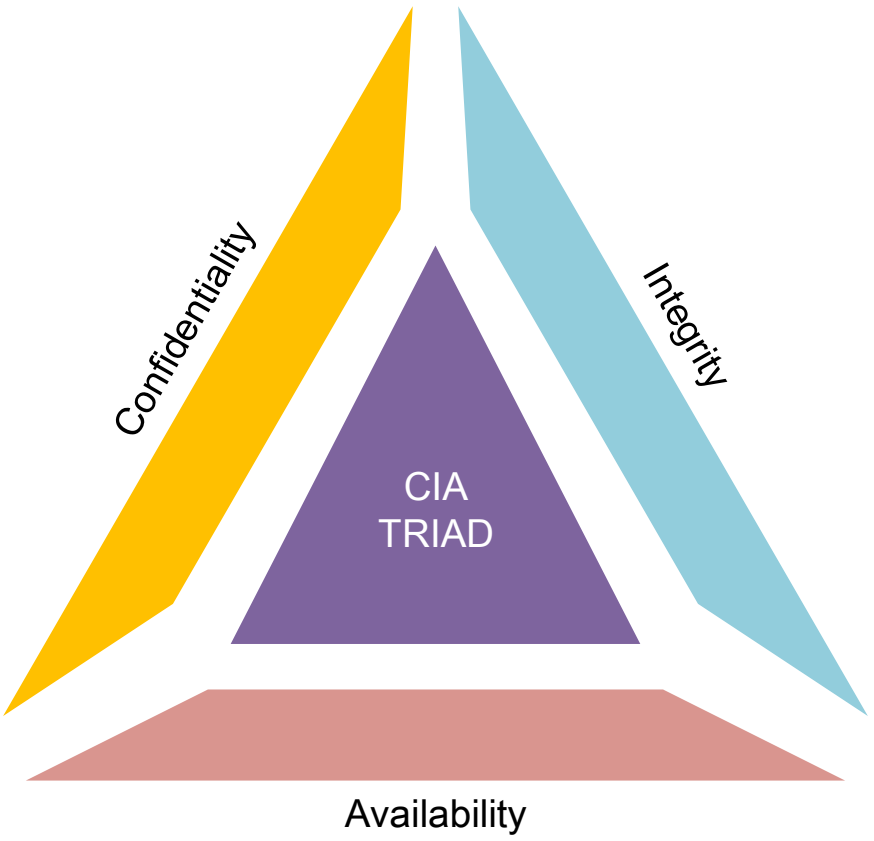
목 차

- 보안 개요
- 암호 수학
  - 대수 구조
  - $GF(2^n)$체

목 차

보안 개요

- 보안 목표
  - CIA Triad
    - 기밀성(Confidentiality)
      - 인가된 사용자만 정보 자산에 접근할 수 있는 원칙
    - 무결성(Integrity)
      - 인가된 사용자 이외에 정보를 변경되지 않도록 하는 원칙
    - 가용성(Availability)
      - 사용자가 필요 시 언제든 정보에 접근할 수 있도록 하는 원칙



보안 개요

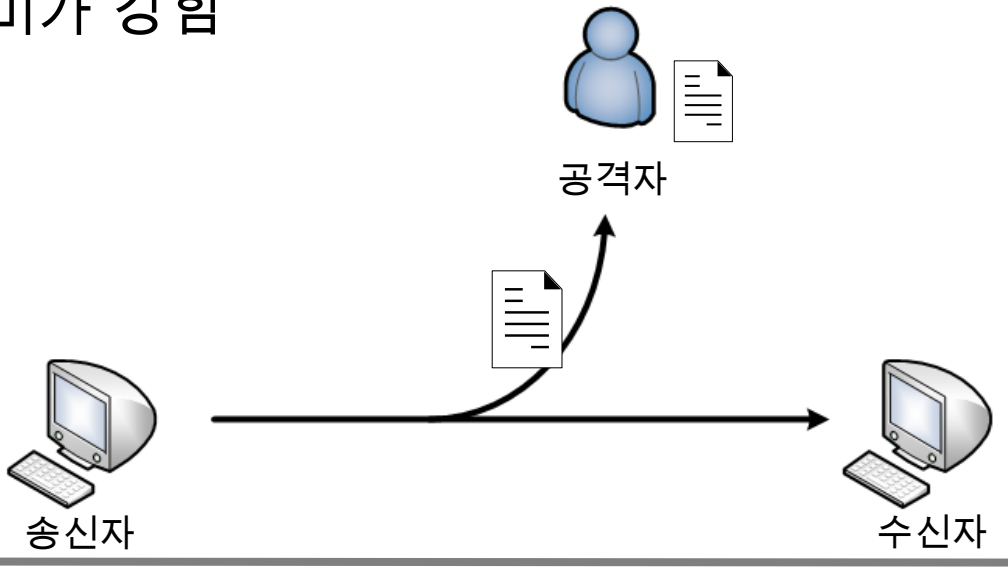
- 보안 목표
  - 침해된 예시
    - 기밀성이 침해된 경우
      - 암호화되지 않은 데이터를 전달할 때, 제 3자가 해당 데이터 패킷을 가로채 도청 또는 분석할 경우
    - 무결성이 침해된 경우
      - 공격자가 이메일 서버에 침입하여 발신자의 이메일 주소를 위조하고 보내고자 하는 이메일의 내용을 조작하여 수신자에게 전달한 경우
    - 가용성이 침해된 경우
      - 특정 웹 사이트가 DDoS 공격을 받아 서버가 다운되어 고객들이 사이트에 접속하지 못하는 경우

보안 개요

- 공격(Attack)
  - 악의적이거나 권한이 없이 정보의 안전성을 침해하려는 행위
  - 소극적 공격(Passive Attack)
    - 시스템으로부터 정보를 획득하려는 시도로, 시스템 자원에는 영향을 끼치지 않는 공격
      - 공격자가 데이터를 단순히 읽기만 하여 특별한 로그나 알림이 발생하지 않아 공격 탐지가 어려움
      - 기밀성을 위협
  - 적극적 공격(Active Attack)
    - 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격
      - 데이터를 변경, 비정상적인 패턴의 공격은 로그 및 경고가 발생하거나 네트워크 트래픽에서 이상을 감지할 수 있어 공격탐지가 비교적 쉬움
      - 무결성, 가용성을 위협

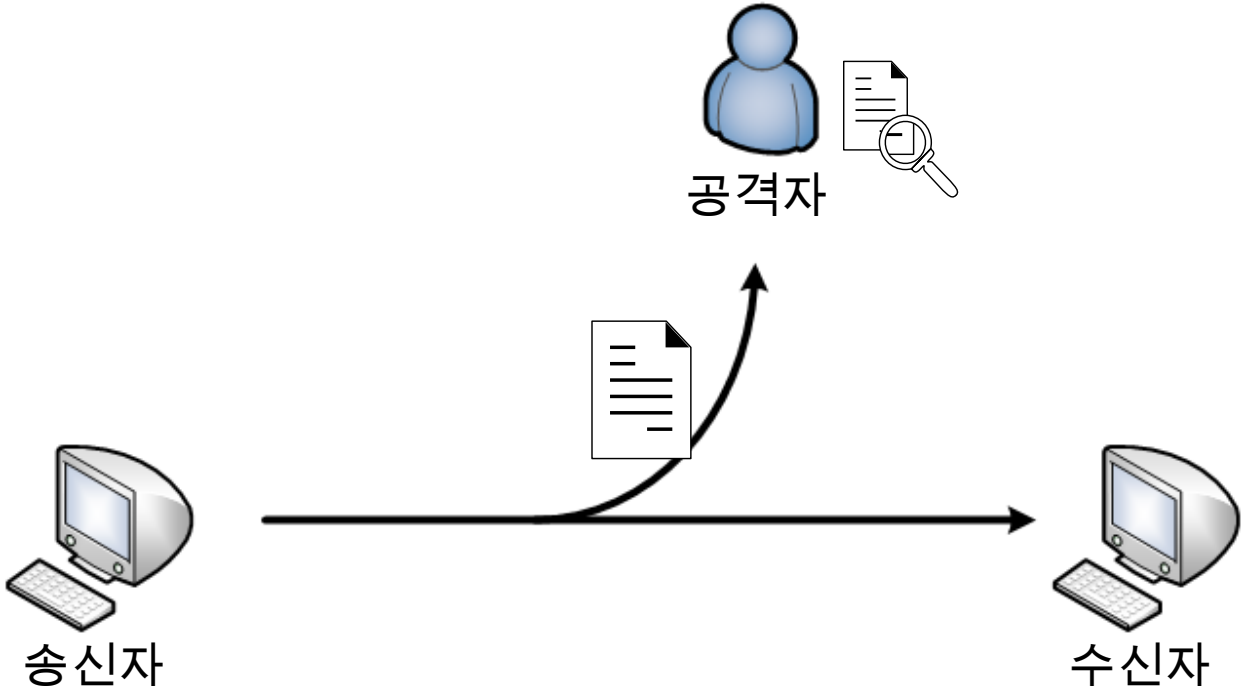
보안 개요

- 공격(Attack)
  - 소극적 공격(Passive Attack) (1/2)
    - 스니핑(Sniffing)
      - 네트워크 상 정보를 몰래 엿듣는 행위
      - 스누핑보다는 도청의 의미가 강함
    - 스누핑(Snooping)
      - 네트워크 상 정보를 감시, 분석하는 행위
      - 도청을 한 후, 분석하는 의미가 강함



보안 개요

- 공격(Attack)
  - 소극적 공격(Passive Attack) (2/2)
    - 트래픽 분석(Traffic Analysis)
      - 암호화된 트래픽을 분석하여 기타 정보를 획득하는 행위
        - 기타 정보: 송수신자, 패킷 크기 등의 메타 데이터 또는 반복적이거나 특이한 패턴

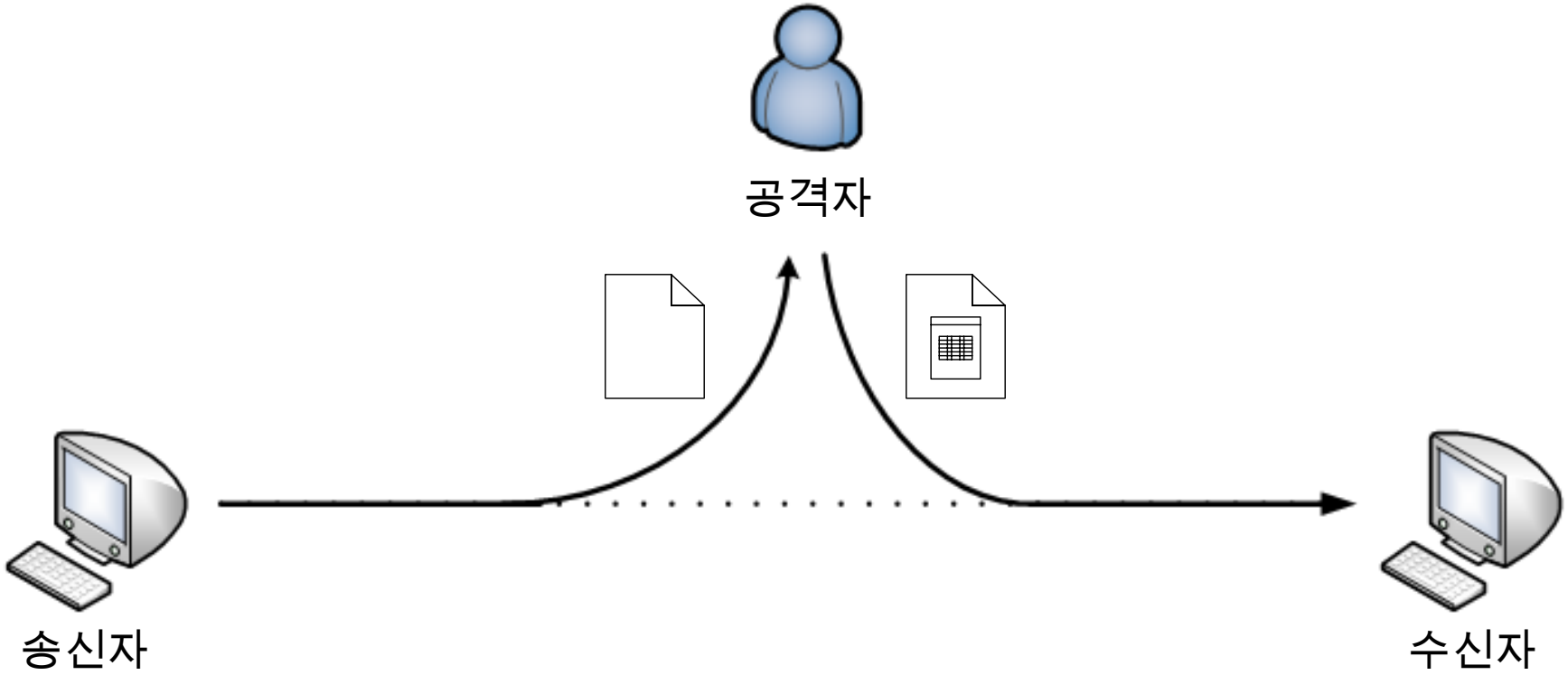


보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack)
    - 스푸핑(Spoofing)
      - 네트워크 상에서 시스템을 속여 정보를 가져가는 행위
      - 유형
        - ARP(Address Resolution Protocol) 스푸핑
          - 근거리 통신망 하에서 주소 결정 프로토콜 메시지를 이용하여 상대방의 데이터 패킷을 중간에 가로채는 중간자 공격
        - IP(Internet Protocol) 스푸핑
          - 타인의 IP를 강탈해 권한을 획득하려는 공격
        - DNS(Domain Name System) 스푸핑
          - DNS 서버를 장악하여 사용자가 의도치 않은 주소로 접속하게 만드는 공격

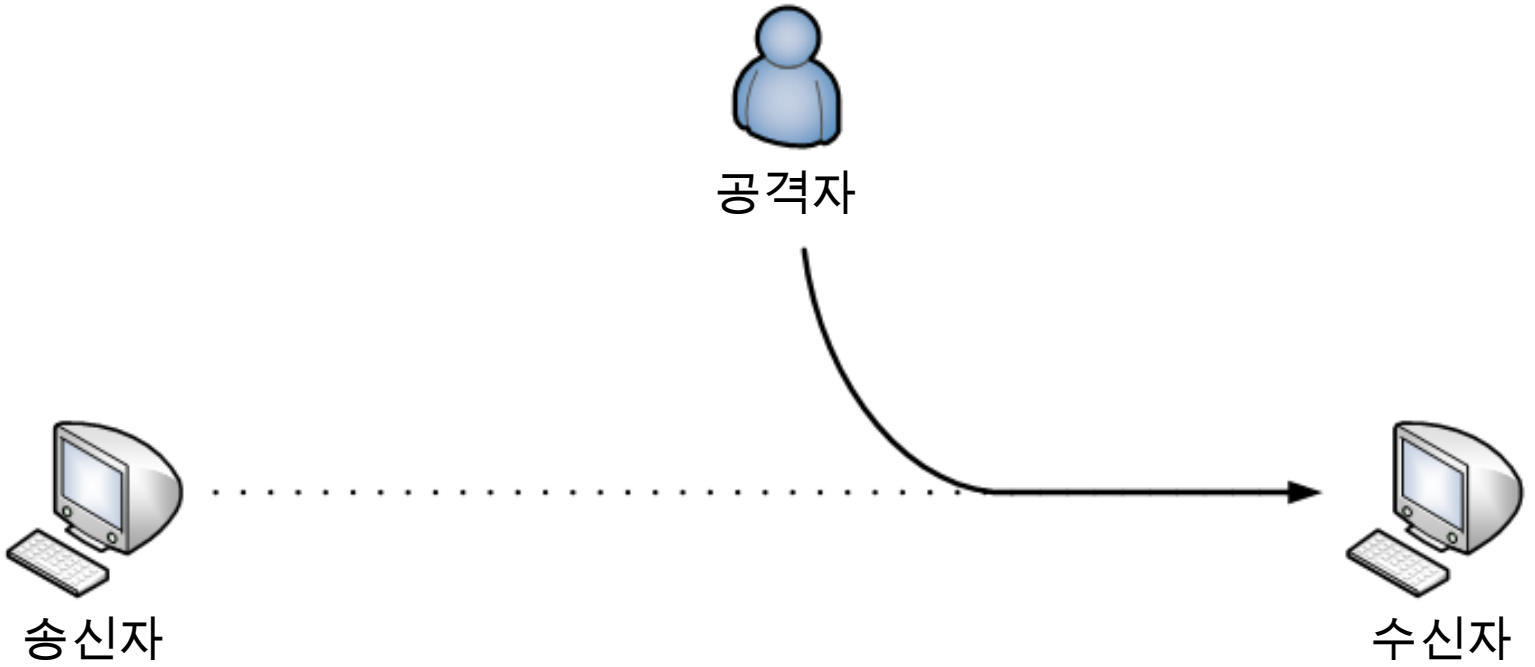
보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 무결성(1/4)
    - 메시지 변조(Modification)
      - 사용자의 허가없이 데이터의 내용을 수정하는 공격
        - e.g., Scapy를 사용하여 프로토콜의 패킷을 위조



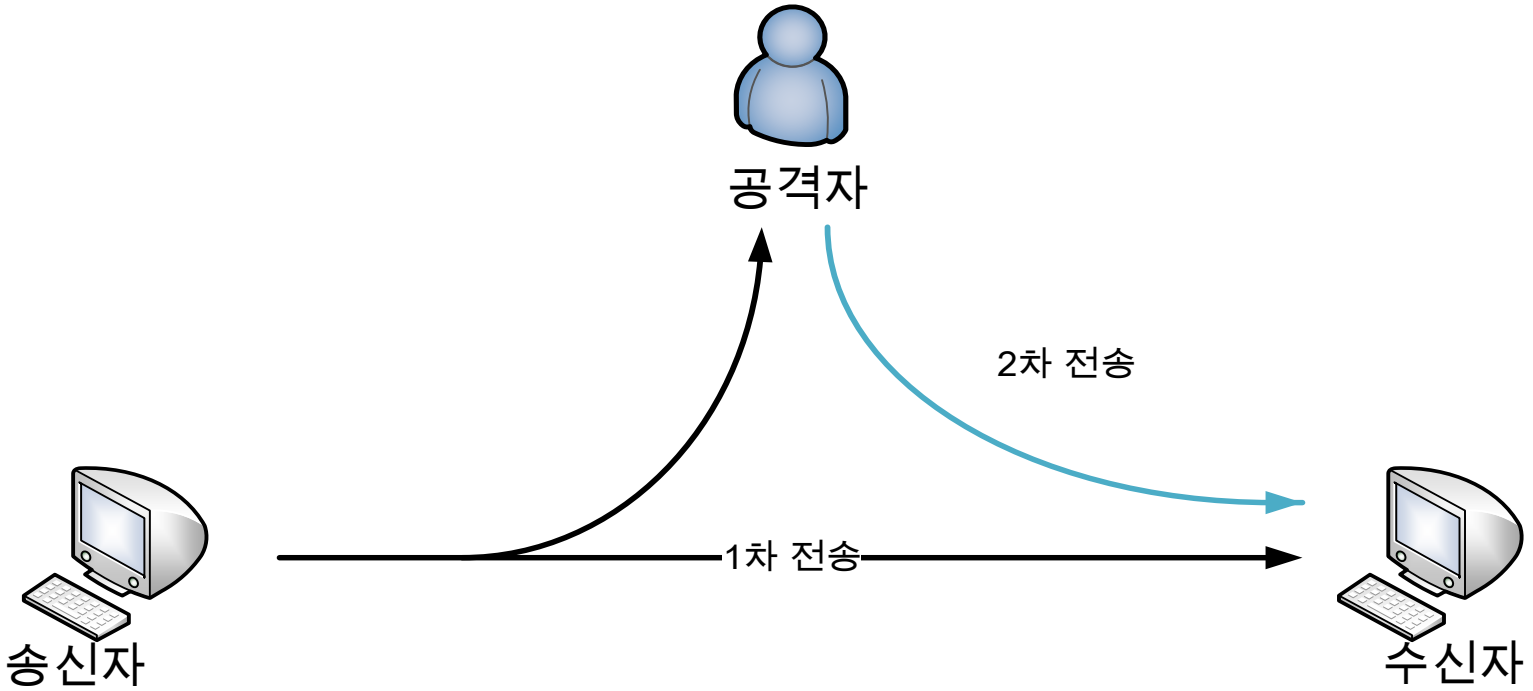
보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 무결성(2/4)
    - 가장(Masquerading)
      - 타인 또는 시스템으로 가장하여 불법적으로 접근하는 공격
        - e.g., 공격자가 송신자인 척 가장하여 악성코드를 송신하는 것



보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 무결성(3/4)
    - 재전송(Replay)
      - 이전에 전송된 데이터를 가로채서 다시 전송하는 공격
        - e.g., 전송되었던 TCP 요청을 한 번 더 보내어 시퀀스 넘버를 사용한 패킷 순서에 혼동을 주는 것



보안 개요

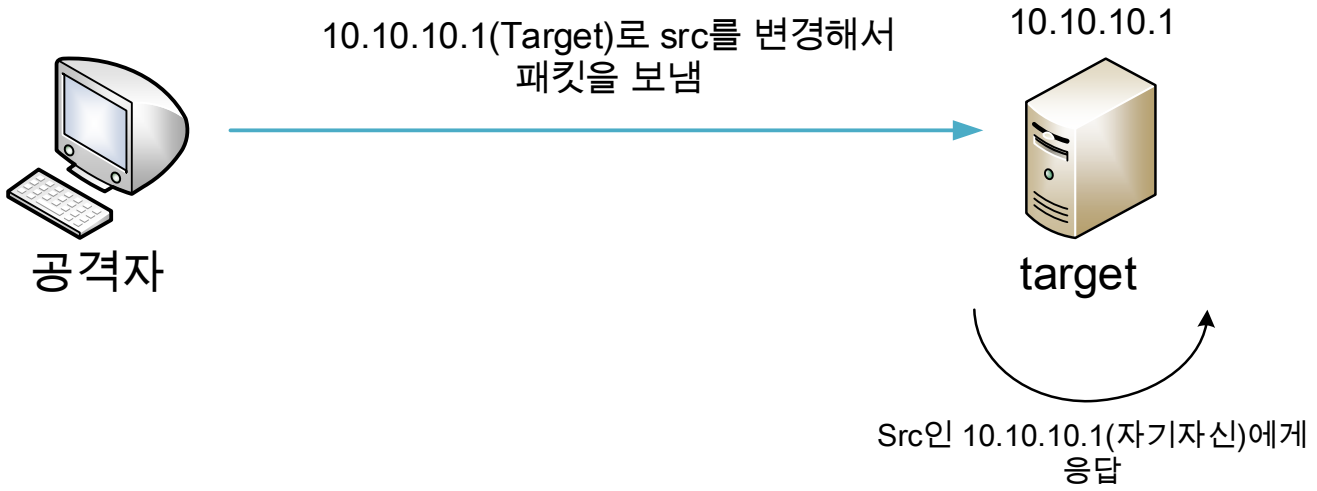
- 공격(Attack)
  - 적극적 공격(Active Attack) – 무결성(4/4)
    - 부인(Repudiation)
      - 공격자가 자신이 공격했다는 사실을 숨기거나 책임을 회피하려는 시도
      - 발신자 부인(Sender Repudiation)
        - 발신자가 메시지를 보냈다는 것을 부인하는 공격
        - 수신자는 메시지의 진위 여부를 확인할 수 있는 방법 필요
          - e.g., 사용자가 인터넷에서 파일을 다운로드했지만 추후에 해당 사실을 부정
      - 수신자 부인(Receiver Repudiation)
        - 수신자가 메시지를 받았음을 부인하는 공격
        - 발신자는 메시지가 성공적으로 전달되었음을 증명
          - e.g., 사용자(발신자)가 온라인 쇼핑에서 결제를 한 후, 쇼핑몰(수신자)에서 결제를 하지 않았다고 주장

보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 가용성(1/4)
    - 서비스 거부(DoS, Denial of Service) 및 분산 서비스 거부(DDoS, Distrubuted DoS)
      - 시스템에 과도한 부하를 발생시켜 정당한 사용자가 해당 서비스를 이용할 수 없도록 만드는 공격
      - DoS와 DDoS의 차이점
        - DoS: 단일 장치에서 악의적 트래픽을 보냄으로써 목표 달성
        - DDoS: 다수의 감염된 컴퓨터를 이용해 목표를 달성

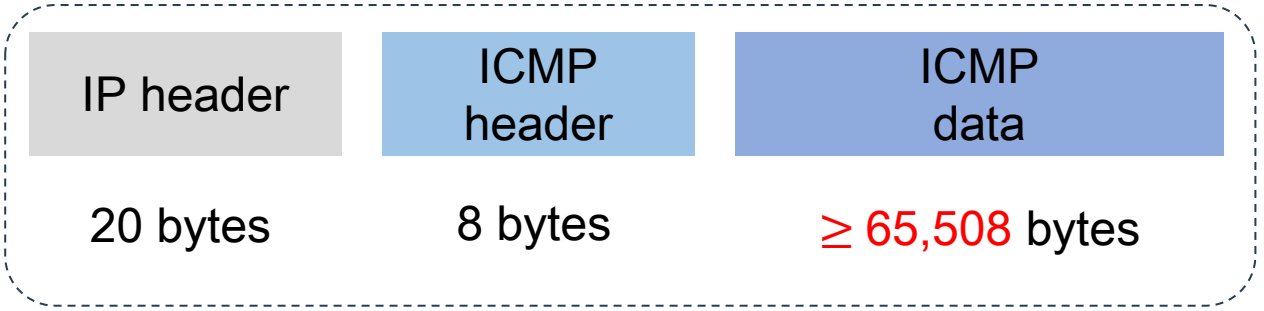
보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 가용성(2/4)
    - 서비스 거부 공격(DoS)의 종류
      - Land Attack(Local Area Network Denial Attack)
        - 출발지 IP 주소와 목적지 IP주소 값을 똑같이 만들어서 공격 대상에게 전달
          - e.g., 출발지 IP 주소와 목적지 IP 주소가 동일한 경우, 패킷을 차단



보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 가용성(3/4)
    - 서비스 거부 공격(DoS)의 종류
      - Ping of Death 공격
        - 규정 크기 이상의 ICMP 패킷으로 시스템을 마비시키는 공격
          - e.g., 브로드캐스트나 멀티캐스트 주소로 들어오는 ICMP 에코 요청에 대해 응답하지 않음

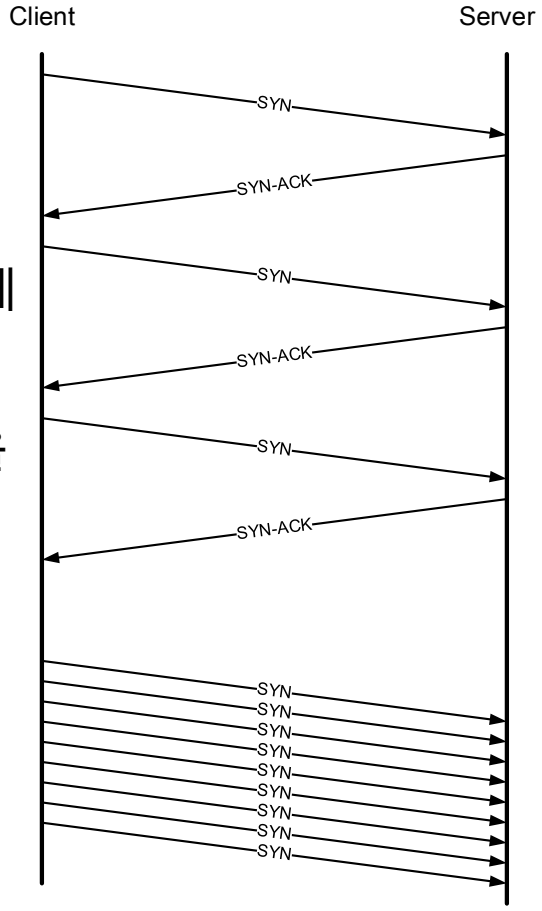


*MTU(Maximum Transmission Unit)
네트워크를 통해 전송될 수 있는 최대 패킷 크기. 일반적으로 이더넷의 MTU는 1500 바이트

* Ping
URL이나 IP를 지정하면 대상에게 에코를 요청하는 데이터를 전송하고 상대의 에코 응답을 기다리는 형태로 동작

보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 가용성(4/4)
    - 서비스 거부 공격(DoS)의 종류
      - SYN Flooding 공격
        - TCP 패킷의 SYN 비트를 이용한 공격 방법으로 대량의 요청을 전송해 대상의 시스템을 Flooding하게 만드는 공격
        - 악의적인 SYN만 보냄으로써 서버의 SYN Backlog을 가득 채워 신규 연결을 받지 못함
          - e.g., SYN-ACK 패킷을 전달할 때, ISN (Initial Sequence Number)에 Cookie 값을 넣어 전송



보안 개요

- 공격에 대한 대응방안(1/2)
  - 스니핑
    - VPN(Virtual Private Network)으로 데이터 전달
  - 스누핑
    - 암호화된 채널로의 전달
  - 트래픽 분석
    - 패킷 패딩 방식 사용
  - 스푸핑
    - ARP 스푸핑: 포트 보안 (Port Security) 사용
    - IP 스푸핑: IDS/IPS 시스템 (Intrusion Detection/Prevention Systems) 설치
    - DNS 스푸핑: DNSSEC (DNS Security Extensions) 사용

보안 개요

- 공격에 대한 대응방안(1/2)
  - 메시지 변조
    - MAC(Message Authentication Code) 사용
  - 가장
    - 생체 인식 인증, 지식 기반 인증 사용
  - 재전송
    - 타임스탬프나 고유한 난수 부여하여 전송
  - 부인
    - 디지털 서명, 로그 유지
  - DoS
    - Anycast 네트워크 확산하여 공격 완화

보안 개요

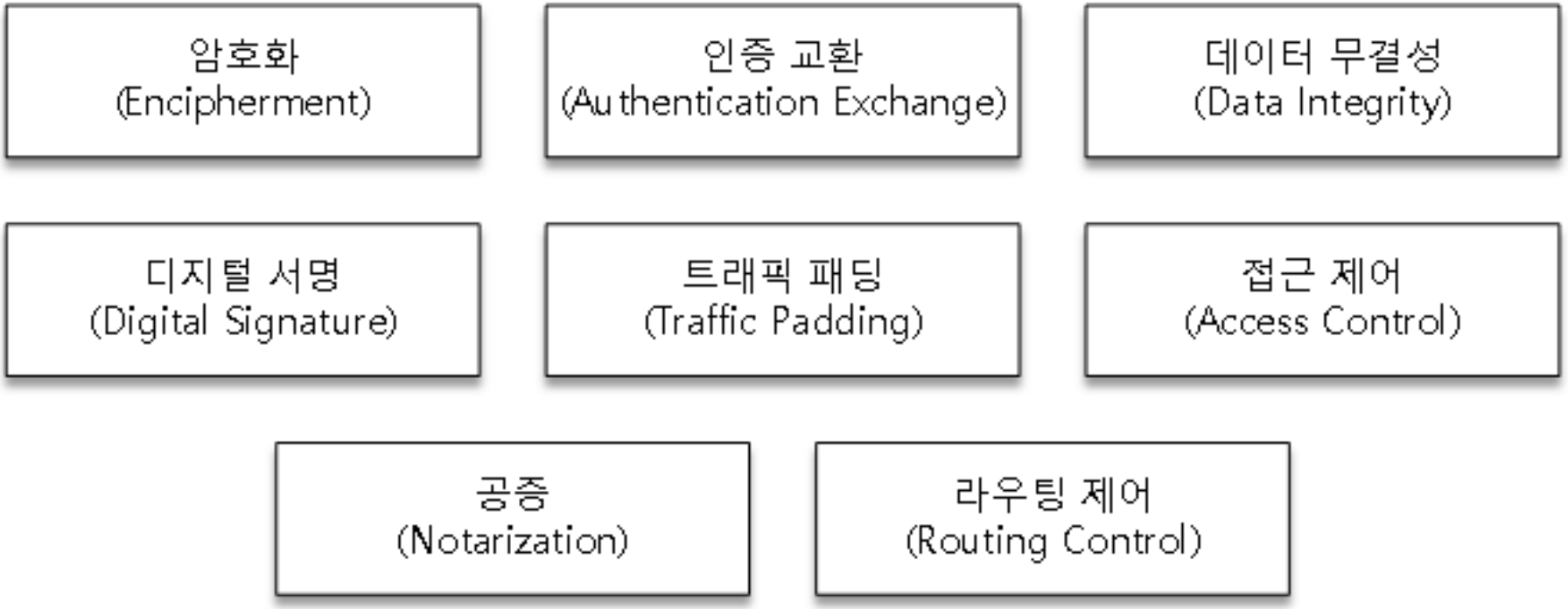
- 보안 서비스
  - 시스템이나 데이터의 보안을 유지하기 위해 제공되는 기능이나 작업

보안 서비스	정의
데이터 기밀성	노출 공격으로부터 데이터를 보호하기 위해 고안
데이터 무결성	데이터의 변경, 삽입, 삭제, 추가를 허가되지 않은 상태로 유지
인증	사용자의 신원 또는 데이터 출처의 신원을 확인
부인 방지	데이터의 송수신자가 나중에 해당 행위를 부인할 수 없도록 함
접근 제어	시스템 자원에 대한 접근 권한 제어

<출처: ITU-T, “X.800:Layer Two Security Service and Mechanisms for LAN”, 2019.>

보안 개요

- 보안 매커니즘 (1/4)
  - 보안 서비스를 구현하기 위해 사용되는 도구, 기술, 절차



<출처: ITU-T, “X.800:Layer Two Security Service and Mechanisms for LAN”, 2019.>

보안 개요

- 보안 매커니즘 (2/4)
  - 암호화(Encipherment)
    - 승인된 당사자만 정보를 확인할 수 있도록 데이터를 변환하는 방법
      - e.g., 대칭키, 비대칭키
  - 데이터 무결성(Data Integrity)
    - 데이터에 추가된 검사값을 이용하여 데이터의 무결성을 수신자가 확인하는 방법
      - e.g., 체크섬, MAC
  - 디지털 서명(Digital Signature)
    - 데이터에 암호학적으로 서명하고, 그 서명을 암호학적으로 검증할 수 있는 방법
      - e.g., 공인 인증서

보안 개요

- 보안 매커니즘 (3/4)
  - 트래픽 패딩(Traffic Padding)
    - 트래픽의 패턴을 숨기기 위해 가짜 데이터를 삽입하는 방법
      - e.g., 패킷 패딩
  - 라우팅 제어(Routing Control)
    - 제 3자가 도청하지 못하도록 송수신자 사이에 다른 가용 경로를 선택하고 지속적으로 변화시키는 방법
      - e.g., IP 테이블
  - 공증(Notarization)
    - 신뢰할 수 있는 제 3자를 선택하여 정보의 진위성을 증명하는 방법
      - e.g., PKI(Public Key Infrastructure)

보안 개요

- 보안 매커니즘 (4/4)
  - 접근 제어(Access Control)
    - 적절한 권한을 가진 인가자만이 특정 시스템이나 정보에 접근할 수 있도록 통제하는 방법
      - e.g. ACL(Access Control List), RBAC(Role Based Access Control), ABAC(Attribute Based Access Control)
  - 인증 교환(Authentication Exchange)
    - 통신 주체가 자신의 신원을 상대방에게 증명하고 인증 받는 방법
      - e.g., PPP PAP(Password Authentication Protocol)

보안 개요

- 암호
  - 비밀을 유지하기 위하여 당사자끼리만 알 수 있도록 꾸민 약속 기호 또는 알고리즘
  - 종류(1/3)
    - 대칭-키 암호화 (Symmetric-key Encipherment)
      - 동일한 키를 사용하여 데이터를 암복호화하는 방식
      - 두 가지 방식으로 나뉨
        - Stream 방식: 평문을 비트 단위로 분할하여 암호화
        - Block 방식: 평문을 블록단위로 분할하여 암호화
      - 키를 교환해야한다는 문제와 사람이 증가할수록 키 관리가 어려워짐
      - e.g., DES(Data Enctyption Standard), RC4(Rcon's Code 4)

보안 개요

- 암호
  - 종류(2/3)
    - 비대칭-키 암호화 (Asymmetric-key Encipherment)
      - 서로 다른 키를 사용하여 암·복호화하는 방식
      - 두 개의 키, 개인키와 공개키가 쌍을 이룬 형태
        - 개인 키(Private Key): 외부에 절대 노출되어서는 안되는 키
        - 공개 키(Public Key): 공개적으로 개방되어있는 키
      - 비밀 키 교환 문제를 해결
      - e.g., RSA(Rivest Shamir Adleman), DSA(Digital Signature Algorothm)
    - 해싱(Hashing)
      - 다양한 길이의 메시지를 해시함수(Hash Function)로 고정된 길이의 메시지로 압축
      - 해싱 완료시, 해시 값을 통해 본래 문자열을 알 수 없으며 변조 여부만 확인 가능
      - 동일 문자열은 동일 해시 알고리즘을 사용 시 반드시 동일한 해시 값을 출력

보안 개요

- 암호
  - 종류(3/3)
    - 혼합형 암호 체계
      - 대칭키와 비대칭키 암호의 각각의 장점을 결합한 암호화 방식
      - 공개키는 키 캡슐화에 사용되고, 개인키는 데이터 캡슐화에 사용
      - e.g., SSL(Secure Socket Layer)

보안 개요

- 암호
  - 대칭키와 비대칭키의 효과
    - 대칭 키
      - 알고리즘 구현이 간단하고 처리 속도가 빨라 데이터 전송, 파일이나 데이터베이스 암호화에 주로 쓰임
      - 키 길이가 짧고, 연산의 복잡성이 낮아 쉽게 해독될 수 있음
    - 비대칭 키
      - 연산의 복잡성이 높아 안전성이 강해 공인인증기관에서 서명이나 인증서 발급 시 사용
      - 키 길이가 길고, 복잡한 수학적 연산을 이용하여 구현되므로 처리 시간이 김

보안 개요

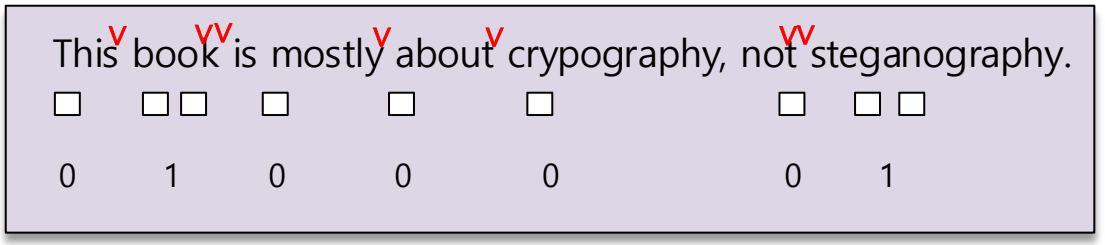
- 암호
  - 암호화와 해싱의 차이
    - 암호화: 수신자와 송신자 사이의 암호화와 복호화 두 단계가 존재하며 ‘데이터 노출 최소화’가 목표
    - 해싱: 암호화된 텍스트의 해시 값을 검사해 ‘데이터 변조가 없었는지 자체의 무결함의 증명하는 것’이 목표

보안 개요

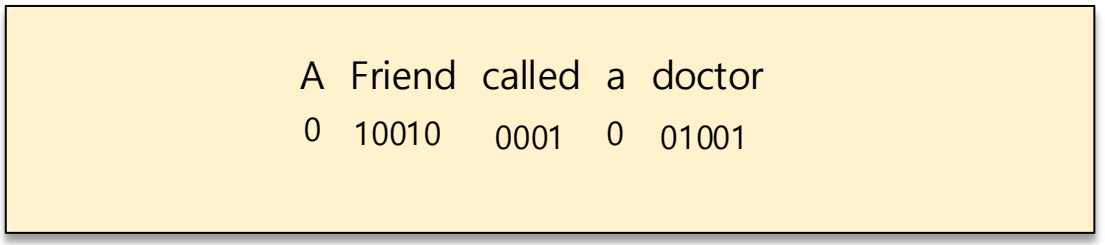
- 스테가노그래피(Steganography)(1/3)
  - 암호의 일종으로, 메시지 자체를 다른 것으로 덮어서 감추는 것
  - 역사적 사용
    - 메시지를 나무 조각에 새긴 뒤 밀랍에 담금
    - 메시지 행간, 종이의 뒷면에 비밀 메시지를 적음
      - 일정 각도의 빛에 노출될 때 메시지가 드러나도록 함
      - e.g., 양파주스, 암모니아 소금
    - 무의미한 메시지 안에 비밀 메시지를 숨기는 널 암호 (Null Cipher)

보안 개요

- 스테가노그래피(Steganography)(2/3)
  - 현대의 사용 (1/2)
    - 텍스트 커버(Text Cover)
      - 텍스트를 이용하여 데이터를 숨기는 것
        1. 이진수 0은 한 칸, 이진수 1은 두 칸 띄어쓰기
           - e.g., ASCII(0100001) 'A'

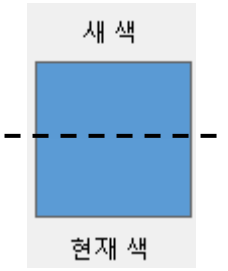


        2. 임의의 사전을 생성하고 패턴을 정해둔 뒤, 텍스트 커버를 이용하기
           - e.g., ASCII(01001000 01001001) 'Hi'



보안 개요

- 스테가노그래피(Steganography) (3/3)
  - 현대의 사용 (2/2)
    - 이미지 커버(Image Cover)
      - 컬러 이미지 안에 데이터를 숨기는 것
      - 디지털 이미지는 RGB, 3바이트의 픽셀로 구성됨
        - e.g., ASCII(01001101) 'M'



RGB

픽셀 1	10101010	11001100	11110000
픽셀 2	10010010	10101010	11001100
픽셀 3	11100011	10010010	10111010

픽셀 1	10101010	11001100	11110000
픽셀 2	10010010	10101010	11001100
픽셀 3	11100011	10010010	10111010

<새 색>

<현재 색>

목 차

- 보안 개요
- 암호 수학
  - 대수 구조
  - $GF(2^n)$체

암호 수학

- 대수 구조(Algebraic Structure)
  - 집합과 그 집합에 포함된 원소들에 적용되는 연산구조

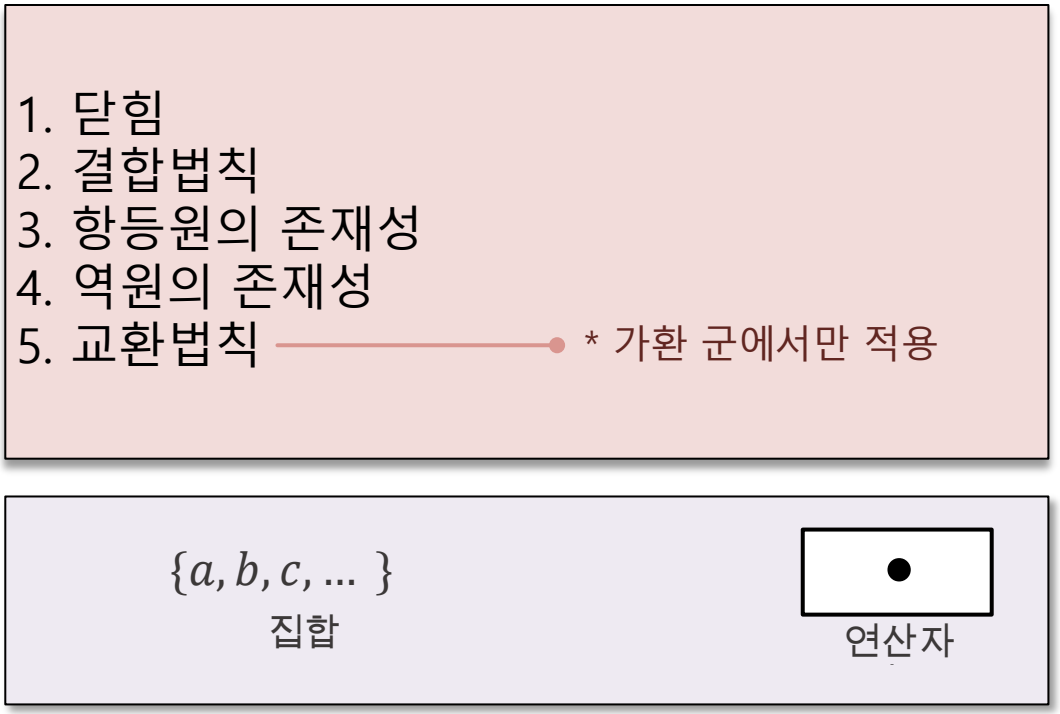
  - 일반적인 대수 구조
    - 군(G, Group)
    - 환(Ring)
    - 체(Field)

대수 구조

- 군(G, Group)
  - 정의
    - 네 개의 성질을 만족하는 연산 "•"이 정의된 원소들의 집합
      $G = < G', \bullet >$
  - 성질
    - 닫힘
      - a와 b가 G의 원소인 경우, $c = a \bullet b$ 또한 G의 원소
    - 결합법칙
      - a, b, c가 G의 원소인 경우 $(a \bullet b) \bullet c = a \bullet (b \bullet c)$를 만족
    - 항등원의 존재성
      - G의 임의의 원소 a에 대해, $e \bullet a = a \bullet e = a$를 만족하는 항등원 (Identity Element) e가 존재
    - 역원의 존재성
      - G의 원소 a에 대해, $a \bullet a' = a' \bullet a = e$를 만족하는 a의 역원(Inverse) a' 존재

대수 구조

- 군(G, Group)
  - 가환 군(Commutative Group)
    - 군의 네 개 성질에 교환법칙을 추가로 만족하는 집합
    - 성질



* 교환법칙
연산자 두 개의 순서를 바꾸어도 결과는 동일

대수 구조

- 군(G, Group)
  - 예제) 군 $G = < Z_n, + >$은 가환군임을 증명
    - 폐쇄성 만족
      - Z_n은 정수 집합이며, 연산 $+$는 모듈로 n에서의 덧셈
        즉, $a + b \; mod \; n$으로 정의

        $Z_n \in a, b$

        $0 \leq a, b < n$

        $0 \leq a + b < 2n$

        $0 \leq (a + b) \; mod \; n < n$
    - 결합법칙 만족
      - e.g., $(4 + 3) + 2 = 4 + (3 + 2)$
    - 교환법칙 만족
      - e.g., 5+2 = 2+5
    - 항등원 0
    - 모든 원소는 덧셈에 대한 역원을 가짐

대수 구조

- 군(G, Group)
  - 군의 종류
    - 유한 군(Finite Group)
      - 유한개의 원소를 갖는 군
    - 무한 군(Infinite Group)
      - 무한개의 원소를 갖는 군

대수 구조

- 군(G, Group)
  - 라그랑지 정리(Lagrange's Theorem)
    - G가 군이고 H가 G의 부분 군일 때, 각 위수를 $|G|$,$|H|$로 표현한다면 $|H|$는 $|G|$를 나눌 수 있음
      - 군의 위수 : 군에 있는 원소의 개수
    - e.g., $|G| = 6$이면 부분군들의 위수는
      $|H_1| = 1, |H_2| = 2, |H_3| = 3, |H_4| = 6$

대수 구조

- 군(G, Group)
  - 부분 군(H, Subgroup)
    - G = <S, •>가 군이고, T가 S의 공집합이 아닌 부분 집합이라고 할 때, 군 $H = < T, \bullet >$ 는 G의 부분 군
    - 부분 군의 기본 조건
      - 닫힘성
        - $H \in a, b$에 대해 $a \bullet b \in H$
      - 항등원의 존재성
        - H는 G의 항등원 포함
      - 역원의 존재성
        - 임의의 $a \in H$에 대해, $a^{-1} \in H$ (a^{-1}는 a의 G에서의 역원)

대수 구조

- 군(G, Group)
  - 부분 군(H, Subgroup)
    - 예제) 군 $H = < Z_{10}, + >$ 가 군 $G = < Z_{12}, + >$ 의 부분 군인가?
      - 라그랑지 정리를 위배함
        - 라그랑지 정리에 의해 군 G의 부분 군이 가지는 위수는 각 1, 2, 4, 6, 12개만 가능하다는 사실을 알 수 있음
      - 군 H는 $mod\ 10$의 연산을, 군 G는 $mod\ 12$의 연산을 말하기 때문

대수 구조

- 군(G, Group)
  - 순환 부분 군(Cyclic Subgroup)
    - 만약 군의 부분 군이 어떤 원소의 멱승(power)을 사용하여 생성된다면 부분 군을 순환 부분 군이라고 함
      - 멱승 : 원소에서 군의 연산을 반복적으로 적용한 것

$$a^n \rightarrow a \cdot a \cdot a \cdots a \ (n\text{번})$$

      - 군 $G \in a$, 부분군 $\mathrm{H} = \{a^n | n \in Z\}$
        이때 a를 생성원(Generater)이 하며 $< a >$ 라고 표기
  - 순환 군
    - 한 원소로 생성될 수 있는 군

$$< a > = \{a^n | n \in Z\} = \{\ldots, a^{-2}, a^{-1}, 1, a^1, a^2, \ldots\} \leq G$$

대수 구조

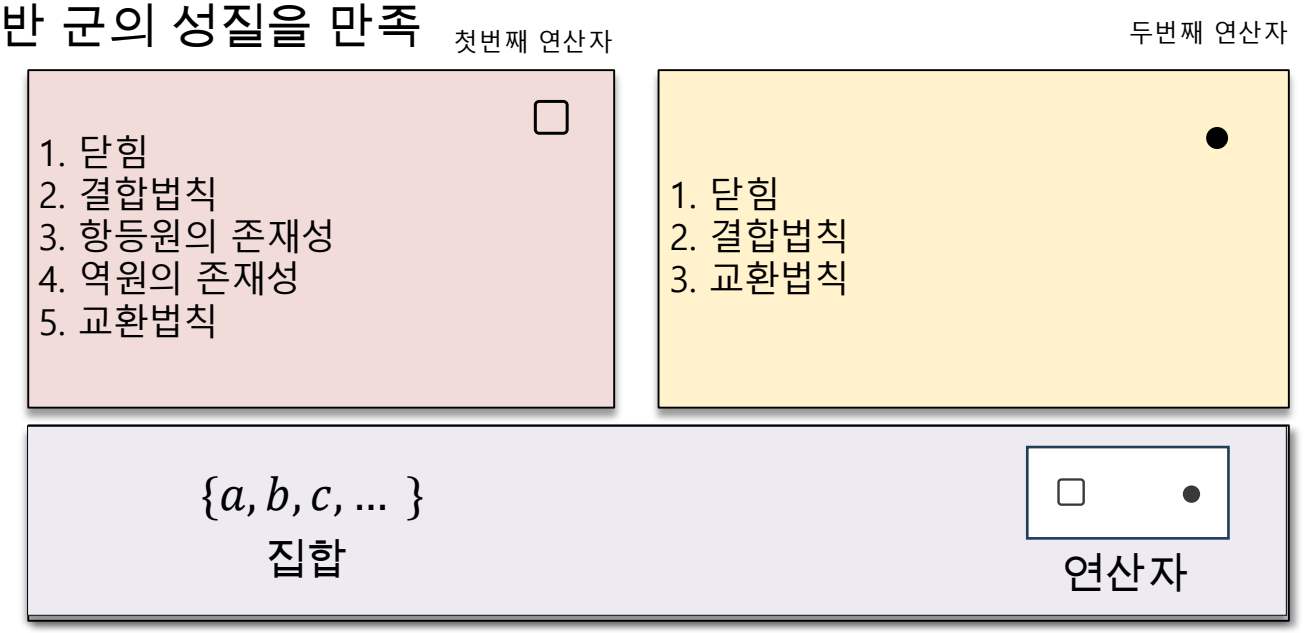
- 군(G, Group)
  - 예제)
    - 군 $G = < Z_{10}{}^{*}, \times >$ 로부터 세 개의 순환 부분 군이 생성
      - $H_1 = < \{1\}, \times >$, $H_2 = < \{1,9\}, \times >$, $H_3 = G$
      - H_1은 항등원만을 원소로 갖는 군
        $1^0 \ mod \ 10 = 1$ (중지: 이런 과정 반복)
      - H_3은 3으로부터 생성된 순환 부분 군
        $3^0 \ mod \ 10 = 1$
        $3^1 \ mod \ 10 = 3$
        $3^2 \ mod \ 10 = 9$
        $3^3 \ mod \ 10 = 7$ (중지: 이런 과정 반복)

대수 구조

- 군(G, Group)
  - 예제)
    - 군 $G = < Z_{10}{}^{*}, \times >$ 로부터 세 개의 순환 부분 군이 생성
      - $H_1 = < \{1\}, \times >$, $H_2 = < \{1,9\}, \times >$, $H_3 = G$
      - H_3은 7로부터 생성된 순환 부분 군
        $7^0 \ mod \ 10 = 1$
        $7^1 \ mod \ 10 = 7$
        $7^2 \ mod \ 10 = 9$
        $7^3 \ mod \ 10 = 3$ (중지: 해당 과정 반복)
      - H_2는 9로부터 생성된 순환 부분 군
        $9^0 \ mod \ 10 = 1$
        $9^1 \ mod \ 10 = 9$ (중지: 해당 과정 반복)

대수 구조

- 환(Ring)
  - 정의
    - 집합 R'에 두 연산 ▢, • 이 정의된 대수구조 $R = < R', ▢, • >$
  - 성질
    - 첫 번째 연산 $< R', ▢>$은 가환 군의 성질을 만족
    - 두 번째 연산 $< R', \cdot>$은 반 군의 성질을 만족



대수 구조

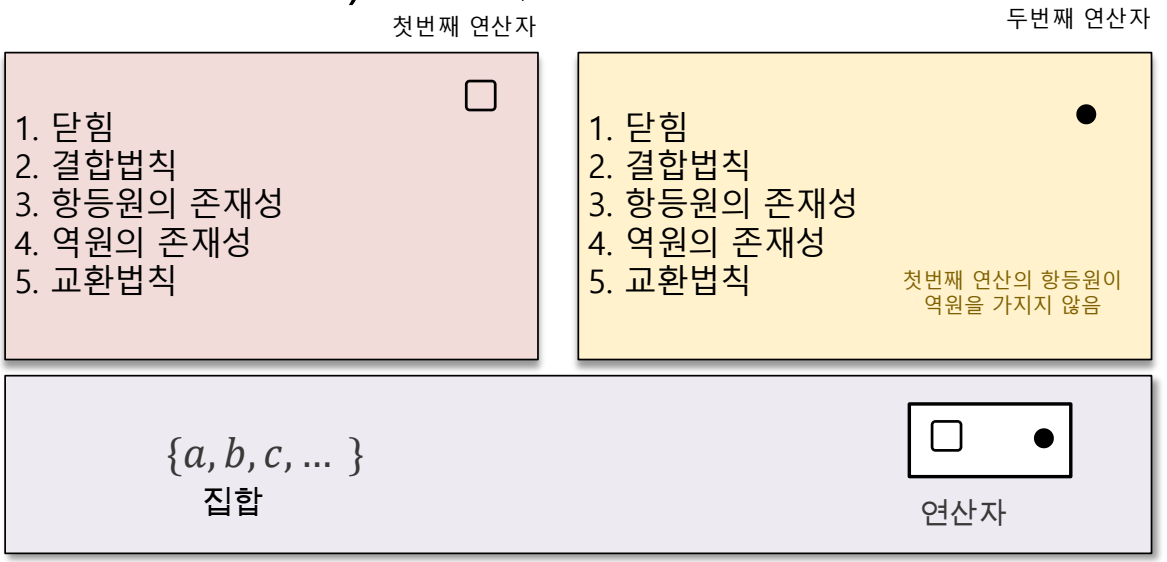
- 환(Ring)
  - 특징
    - 두 번째 항등원은 역원이 없을 수도 있음
      - 첫 번째 연산은 $+, -$만이 들어갈 수 있으며 두 번째 연산은 $\times$만 들어갈 수 있음
      - 예제)
        - 덧셈과 곱셈의 두 연산이 정의된 집합 Z_n은 가환 환일 때, 첫 번째 연산은 덧셈과 뺄셈을 모두 사용할 수 있으나 두 번째 연산은 나눗셈이 아닌 곱셈만이 들어갈 수 있다

          → 나눗셈은 집합 밖의 원소를 만들어 냄

          $5 \div 2 = 2.5$

대수 구조

- 체(Field)
  - 정의
    - 곱셈에 대한 교환법칙이 성립하는 나눗셈 환, $F = < F', \square, \bullet >$
  - 성질
    - 첫 번째 연산은 가환 군의 성질을 만족
    - 두 번째 연산에서 첫 번째 연산의 항등원이 역원을 갖지 않음
      - e.g., 첫 번째 연산(덧셈의 항등원 0): 덧셈, 두 번째 연산: 곱셈



대수 구조

- 체(Field)
  - 유한 체(Finite Field)
    - 유한개의 원소를 가진 체
      - 갈로아 체(Galois Field): $GF(p^n)$는 p^n개의 원소를 갖는 유한 체 (p는 소수, n은 양의 정수)

$\{0, 1\}$ $\quad + \quad \times$

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

a	0	1
$-a$	1	0

a	0	1
a^{-1}	$\cdot$	1

$GF(2)$

대수 구조

- 요약
  - 군(Group)
    - 집합과 이항 연산으로 구성된 대수적 구조
    - 폐쇄성, 결합법칙, 항등원, 역원을 만족
      (가환 군은 교환법칙까지 만족)
  - 환(Ring)
    - 집합과 두 이항 연산이 정의된 대수적 구조
    - 덧셈에서는 군을 형성하지만, 곱셈에서는 항상 역원이 아닌 경우가 있음
  - 체(Field)
    - 두 연산을 가진 대수적 구조
    - 모든 원소가 덧셈과 곱셈에 역원을 가짐

목 차

- 보안 개요
- 암호 수학
  - 대수 구조
  - $GF(2^n)$체

$GF(2^n)$체

- 개요
  - 암호학에선 사칙연산$(+\ -\times\div)$이 모두 필요함
    즉, 암호학에서는 체를 사용

대수 구조	들어갈 수 있는 연산자 유형	들어갈 수 있는 정수 집합의 유형
군	$(+\ -)\ or\ (\times\div)$	$Z_n\ or\ Z_n{}^*$
환	$(+\ -)\ and\ (\times)$	Z
체	$(+\ -)\ and\ (\times\div)$	$Z_p{}^*$

$GF(2^n)$체

- 한계점
  - 2^n보다 작은 가장 큰 소수 p를 이용해서 Z_p에 정의된 $GF(p)$를 사용
    - 단, p로부터 $2^n - 1$까지의 정수를 사용할 수 없기 때문에 비효율적
  - 원소의 개수가 2^n인 $GF(2^n)$체를 사용
    - 이 집합의 원소들이 비트 형태로 표현되기 때문에 네 개의 연산들이 적용될 수 없음
      - e.g., $n = 3$

XOR	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

AND	00	01	10	11
00	00	00	00	00
01	00	01	00	11
10	00	00	10	10
11	00	01	10	11

$GF(2^n)$체

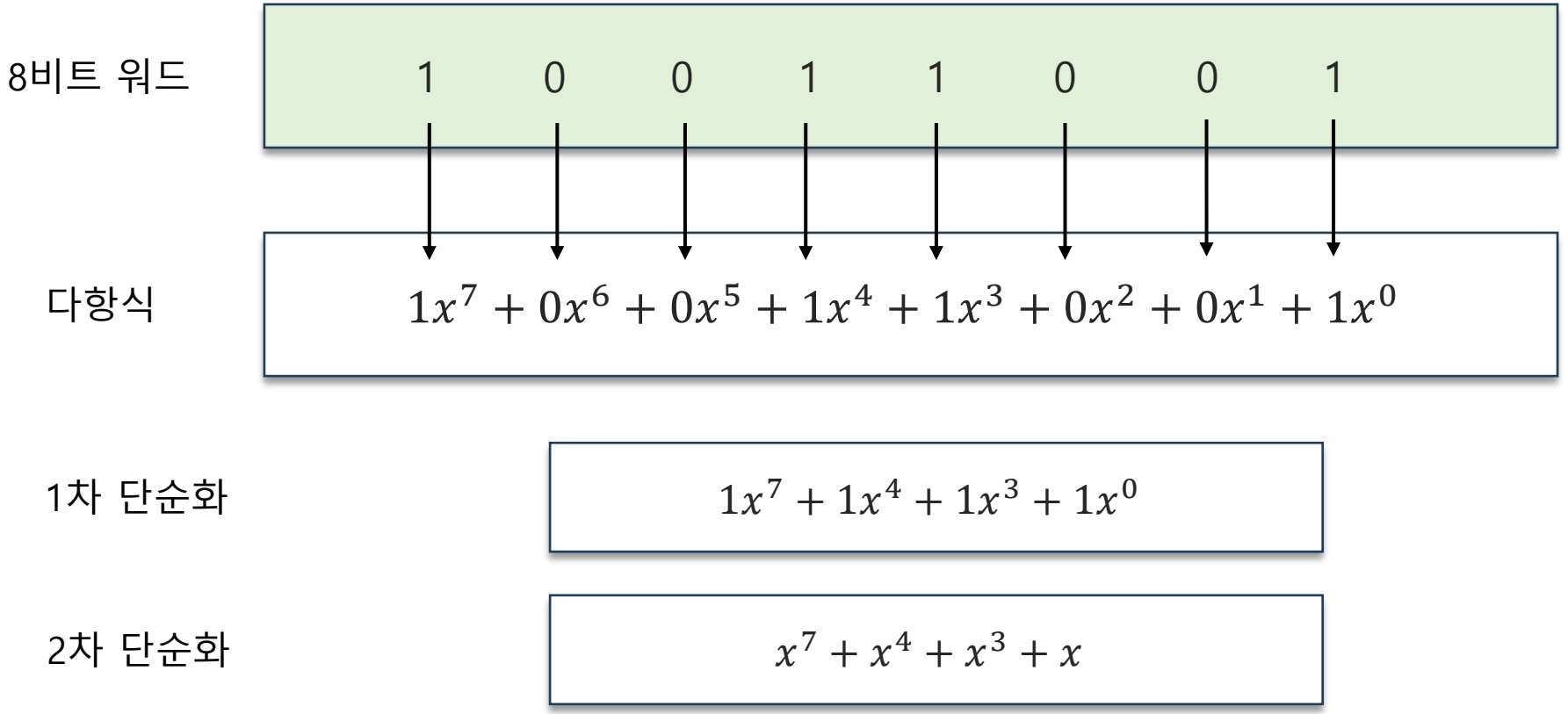
- 다항식(Polynomial)
  - n비트 워드들을 차수 $n-1$의 다항식 형태로 표현

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$$

  - 규칙
    - x의 지수승은 n비트 워드에서 비트들의 위치를 정의
      - 가장 오른쪽에 있는 비트를 최하위 비트, 가장 왼쪽에 있는 비트를 최상위 비트
    - 항의 계수는 비트들의 값으로써 정의
      - 비트는 $0, 1$뿐이므로 다항식의 계수들은 0 혹은 1

$GF(2^n)$체

- 다항식(Polynomial)
  - e.g., 8비트 워드(10011001) 표현



$GF(2^n)$체

- 다항식(Polynomial)
  - 연산
    - n비트 워드를 표현하는 다항식들은 두 개의 체 $GF(2)$와 $GF(2^n)$을 사용
  - 모듈로
    - 두 다항식의 덧셈은 결코 그 집합에 속하지 않는 다항식을 생성하지 않음
    - 두 다항식의 곱셈은 $n-1$ 보다 큰 차수를 가지는 다항식을 생성할 수 있음
      - 모듈로 논리에 따라 모듈로 다항식으로 나누고 나머지를 취함

$GF(2^n)$체

- 다항식(Polynomial)
  - 기약 다항식(Irreducible Polynomial)
    - 어떤 다항식 $P(x)$가 다른 다항식들로 나누어지지 않는 경우
      즉, $P(x)$를 나누는 다항식이 1과 $P(x)$ 외에는 없는 경우

차수	기약 다항식
1	$(x+1), (x)$
2	(x^2+x+1)
3	$(x^3+x^2+x+1), (x^3+\mathrm{x}+1)$
4	$(x^4+x^3+x^2+x+1), (x^4+x^3+x+1), (x^4+x+1)$
5	$(x^5+x^4+x^3+x^2+x+1), (x^5+x^3+x^2+x+1), (x^5+x^4+x^3+x+1),$ $(x^5+x^4+x^3+x^2+1), (x^5+x^4+x^2+x+1)$

$GF(2^n)$체

- 다항식(Polynomial)
  - 덧셈
    - 기호 $\oplus$는 다항식의 덧셈을 의미(XOR 연산)

$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0$$
$$0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 \quad \oplus$$
$$\text{----------}$$
$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0$$
$$\rightarrow \quad x^5 + x^3 + x + 1$$

    - 덧셈에 대한 항등원 0
    - 덧셈에 대한 역원
      - $GF(2)$에서 계수를 가지는 다항식의 덧셈에 대한 역원은 그 자신

$GF(2^n)$체

- 다항식(Polynomial)
  - 곱셈
    - 계수들의 곱셈은 $GF(2)$에서 이뤄짐
    - x^i와 x^j를 곱한 결과는 x^{i+j}
    - 곱셈은 $n-1$ 보다 큰 차수를 가지는 항을 생성할 수 있음
      - e.g., $x^8+x^4+x^3+x+1$을 가지는 $GF(2^8)$에서 (x^5+x^2+x) $(x^7+x^4+x^3+x^2+x)$

$$x^5(x^7+x^4+x^3+x^2+x)+x^2(x^7+x^4+x^3+x^2+x)+x(x^7+x^4+x^3+x^2+x)$$
$$= x^{12}+\cancel{x^9}+\cancel{x^8}+x^7+\cancel{x^6}+\cancel{x^4}+\cancel{x^9}+\cancel{x^6}+x^5+\cancel{x^4}+\cancel{x^3}+\cancel{x^8}+\cancel{x^5}+\cancel{x^4}+\cancel{x^3}+x^2$$
$$= x^{12}+x^7+x^2$$

$$(x^{12}+x^7+x^2)\ mod\ (x^8+x^4+x^3+x+1) = x^5+x^3+x^2+x$$

    - 곱셈에 대한 항등원 1
    - 곱셈에 대한 역원

      두 다항식을 곱한 결과에 모듈로를 취했을 때 나머지 구함

$GF(2^n)$체

- 요약
  - 기본 개념
    - $GF(p^n)$는 p^n개의 원소를 갖는 유한 체
    - 원소는 $\{000, 001, 010, \ldots, 111\}$과 같이 2진수로 표현
  - 덧셈 연산
    - 비트별 XOR 연산으로 수행
  - 곱셈 연산
    - 두 다항식을 곱하면 차수가 커질 수 있음
    - 결과 다항식을 기약 다항식으로 나누고, 나머지를 취해 차수를 줄임
      - 기약 다항식 : 다른 다항식으로 나눌 수 없는 다항식

Thanks!

김 혜 정(hyejeong@pel.sejong.ac.kr)