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

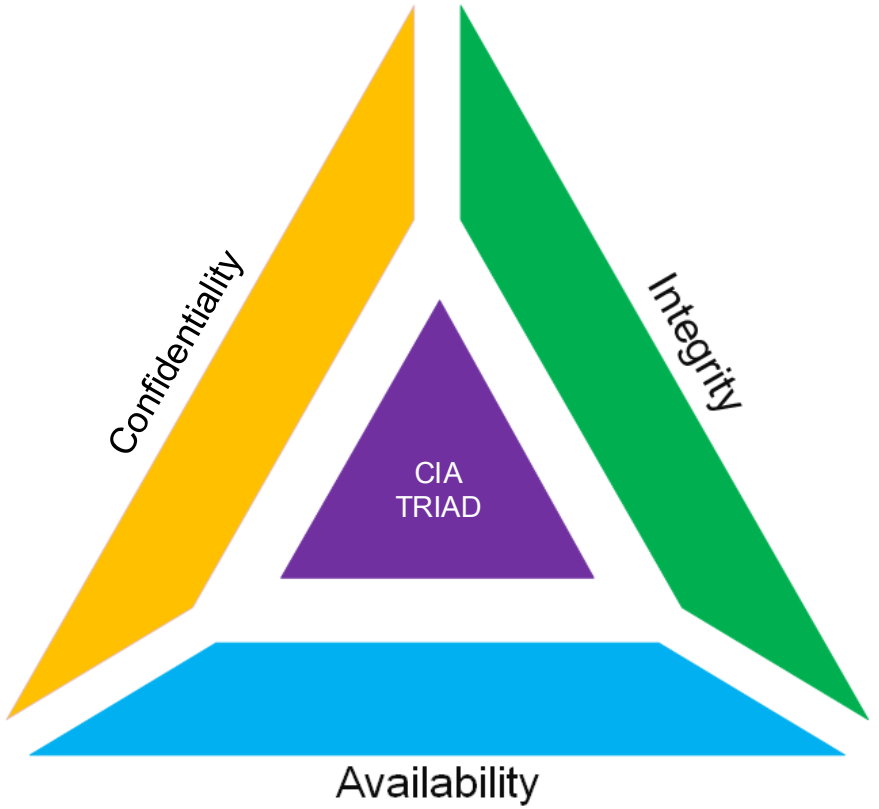
목 차

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

목 차

보안 개요

- 정의
  - 정보를 안전하게 보호하기 위해 지켜야할 보안 목표
    - 보안 목표
      - 기밀성(Confidentiality)
        - 무자격자의 정보 접근 방지
      - 무결성(Integrity)
        - 권한 있는 자만 정보 변경 가능
      - 가용성(Availability)
        - 권한 있는 자의 정보 접근 보장



보안 개요

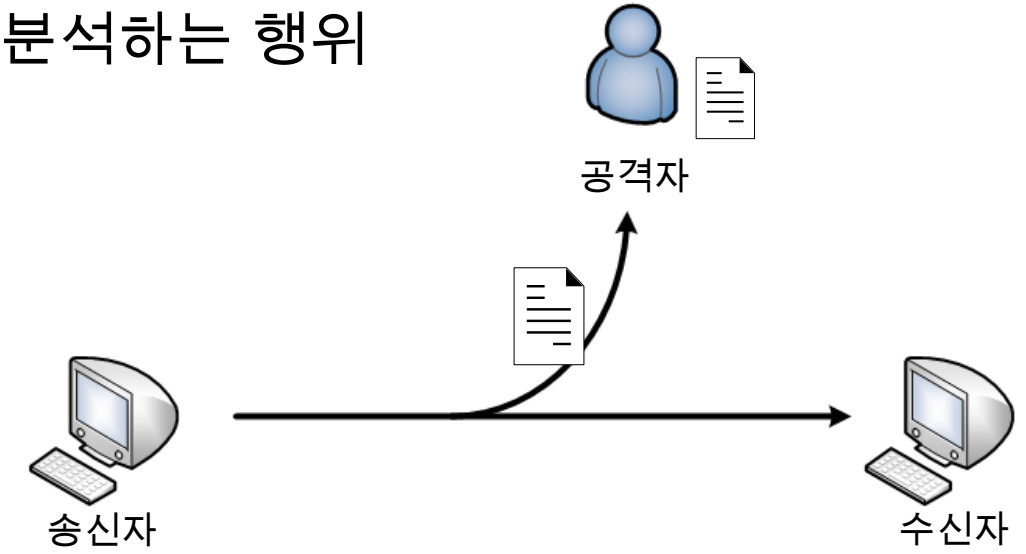
- 보안 목표
  - 기밀성(Confidentiality)
    - 비인가된 접근자로부터 정보를 노출시키지 않는 원칙
      - 정보의 보관뿐만 아니라 전송에도 적용
        - e.g., 암호화가 되지 않은 데이터가 유출됐을 경우
  - 무결성(Integrity)
    - 정보의 정확성과 완전성을 보장하는 원칙
      - 데이터가 불법적으로 생성, 변경, 삭제되지 않도록 함
        - e.g., 제조업체의 제품 품질 관리 데이터를 변경하여 제품의 품질 기준을 통과하지 못하게 된 경우
  - 가용성(Availability)
    - 사용자가 필요 시 언제든 정보에 접근할 수 있도록 하는 원칙
      - 시스템이 정상적으로 동작하여 요청을 지체없이 처리할 수 있어야 함
        - e.g., 전자 상거래 웹 사이트가 DDoS 공격을 받아 서버가 다운되어 고객들이 사이트에 접속하지 못한 경우

보안 개요

- 공격(Attack)
  - 악의적이거나 권한이 없이 정보의 안전성을 침해하려는 행위
  - 소극적 공격(Passive Attack)
    - 공격자의 목표가 단순히 정보를 획득하는 것
      - 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)
    - 데이터를 변경하거나 해를 끼치는 것
      - 소극적 공격에 비해 공격 탐지가 쉬움
      - 데이터를 변경, 비정상적인 패턴의 공격은 로그 및 경고가 발생하거나 네트워크 트래픽에서 이상을 감지할 수 있음
      - 무결성, 가용성을 위협

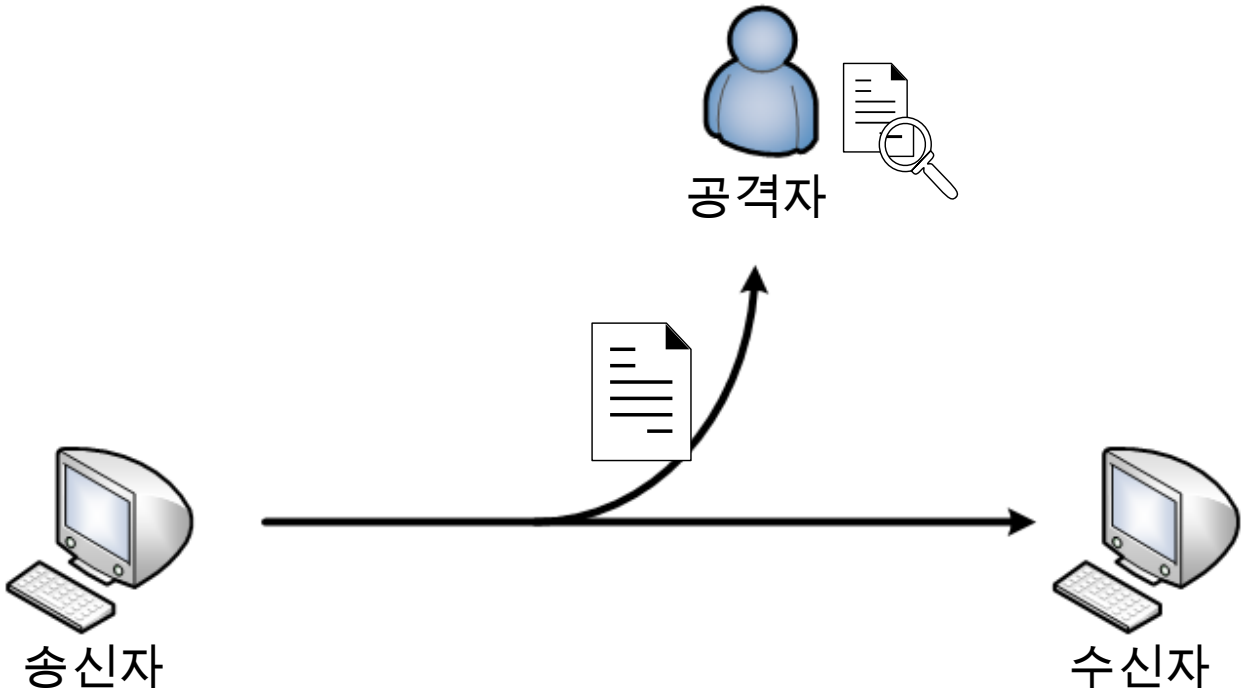
보안 개요

- 공격(Attack)
  - 소극적 공격(Passive Attack) (1/2)
    - 스니핑(Sniffing)
      - 네트워크 상 정보를 몰래 훔쳐보는 행위
    - 일반적으로 작동하는 IP필터링과 MAC 주소 필터링을 수행하지 않고, 랜 카드로 들어오는 전기적 신호를 모두 읽어내림
    - 스누핑(Snooping)
      - 네트워크 상 정보를 감시, 분석하는 행위



보안 개요

- 공격(Attack)
  - 소극적 공격(Passive Attack) (2/2)
    - 트래픽 분석(Traffic Analysis)
      - 암호화된 트래픽을 분석하여 기타 정보를 획득하는 행위
        - e.g., Wireshark, tcpdump

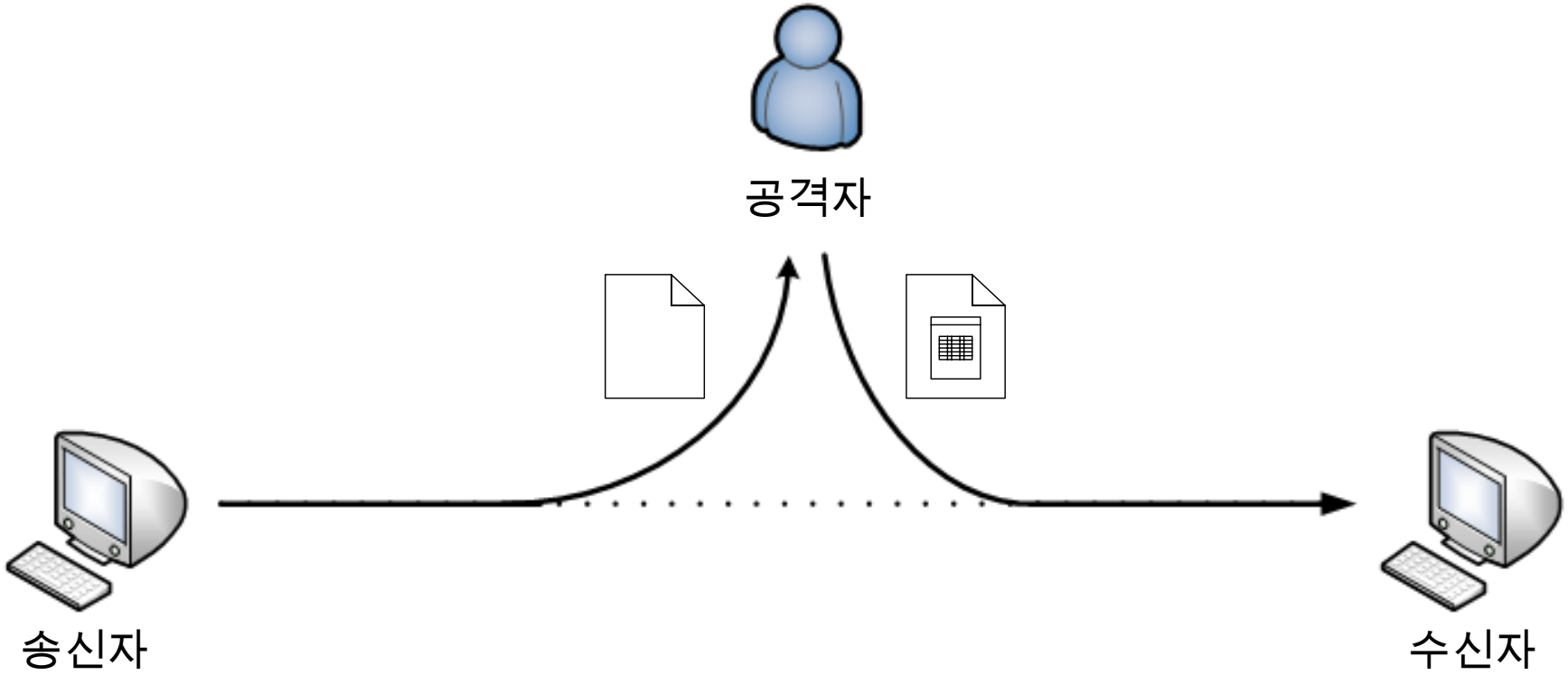


보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack)
    - 스푸핑(Spoofing)
      - 네트워크 상 정보를 시스템을 속여서 가져가는 행위
      - 종류
        - ARP(Address Resolution Protocol) 스푸핑
          - 근거리 통신망 하에서 주소 결정 프로토콜 메시지를 이용하여 상대방의 데이터 패킷을 중간에 가로채는 중간자 공격 기법
        - IP(Internet Protocol) 스푸핑
          - 타인의 IP를 강탈해 권한을 회득하려는 공격 기법
        - DNS(Domain Name System) 스푸핑
          - DNS에서 전달하는 IP주소를 변조하거나 DNS 서버를 장악하여 사용자가 의도치 않은 주소로 접속하게 만드는 공격 기법

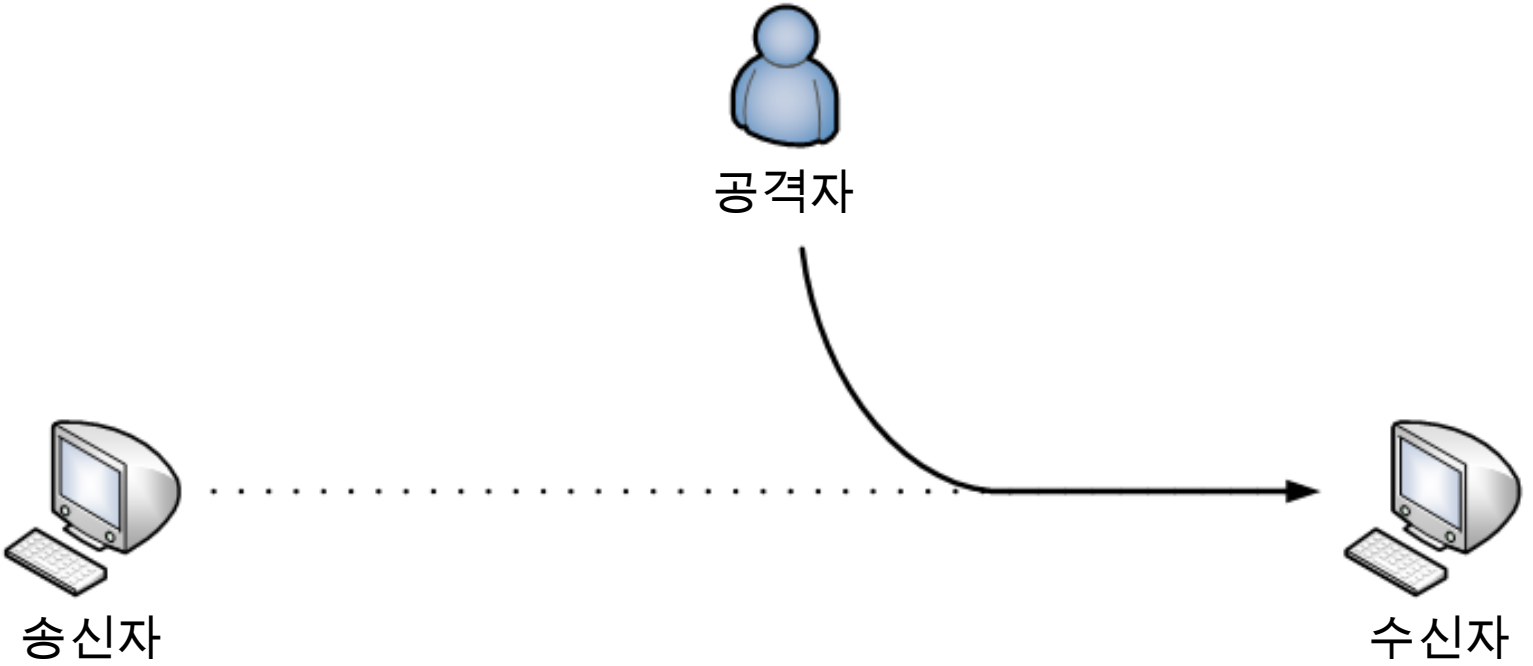
보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 무결성(1/4)
    - 메시지 변조(Modification)
      - 사용자의 허가없이 데이터의 내용을 수정하는 공격
        - e.g., SQL injection



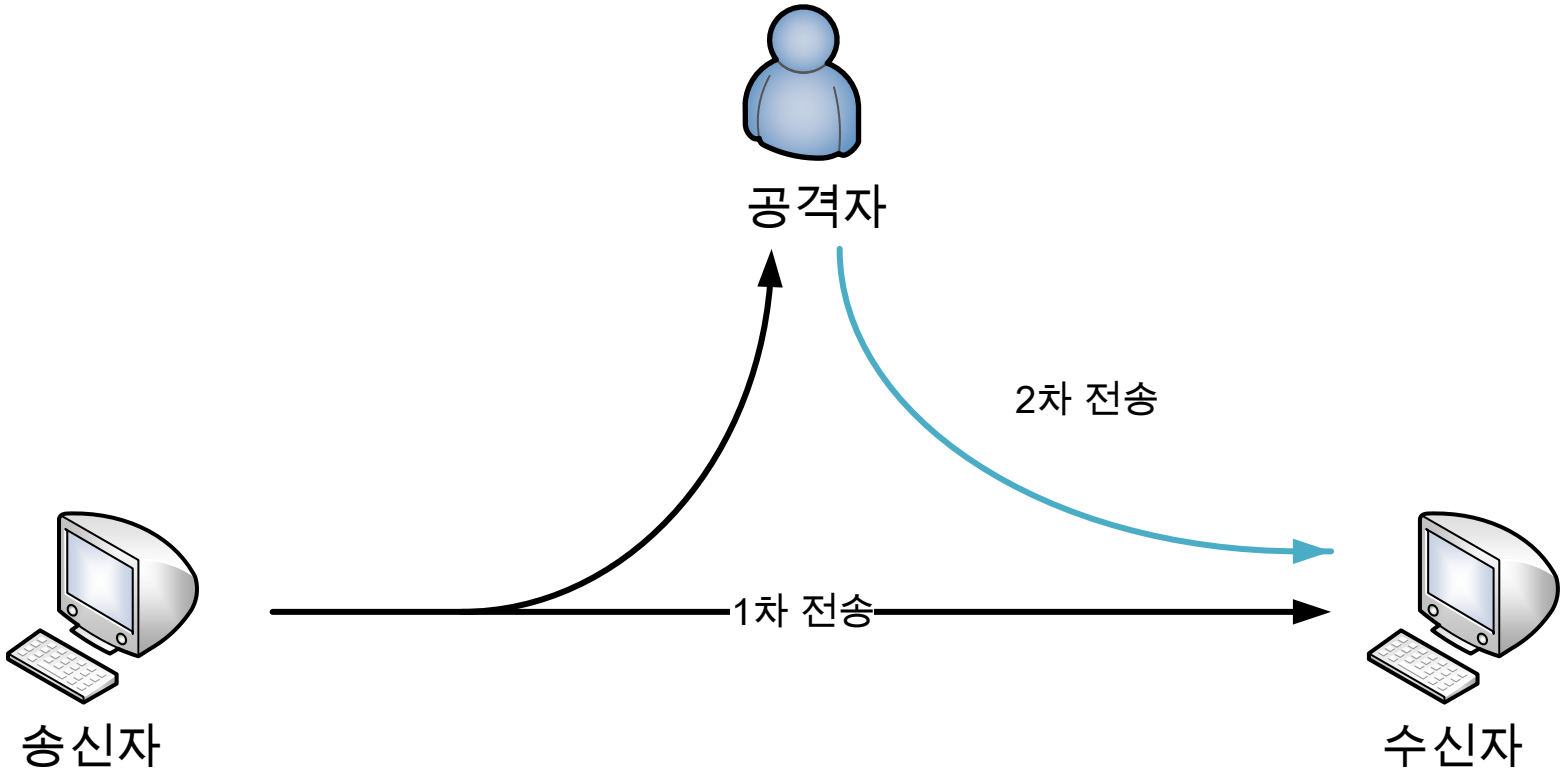
보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 무결성(2/4)
    - 가장(Masquerading)
      - 타인 또는 시스템으로 가장하여 불법적으로 접근하는 공격
        - e.g., A가 B인 척 가장하여 이메일을 보내는 것



보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 무결성(3/4)
    - 재전송(Replay)
      - 이전에 전송된 데이터를 가로채서 다시 전송하는 공격
        - e.g., RFID 카드를 이용하여 출입을 할 때 이 무선 신호를 가로채는 경우



보안 개요

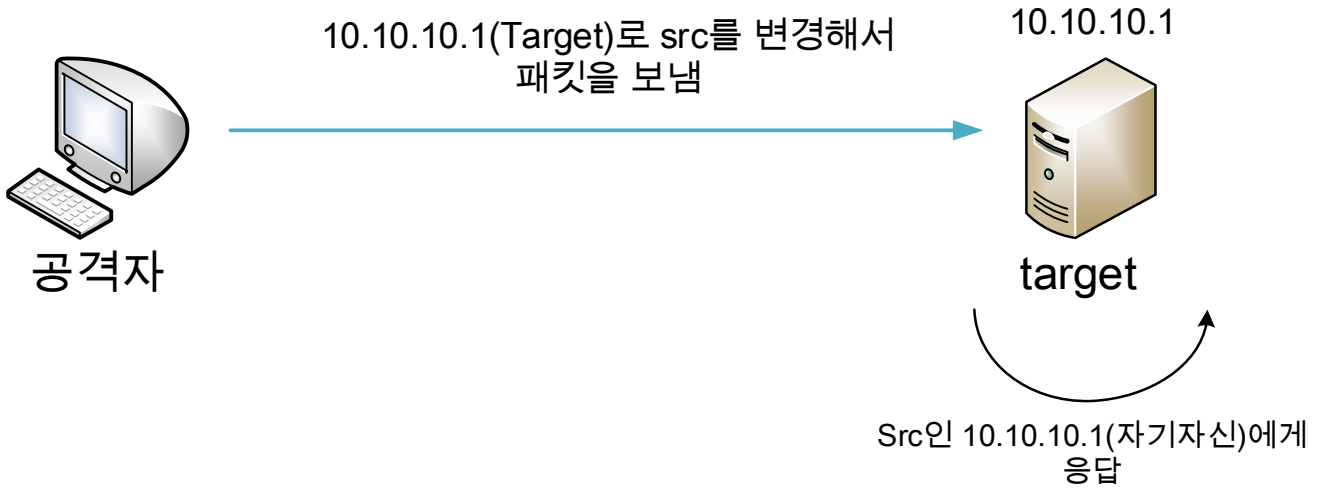
- 공격(Attack)
  - 적극적 공격(Active Attack) – 무결성(4/4)
    - 부인(Repudiation)
      - 공격자가 자신이 공격했다는 사실을 숨기거나 책임을 회피하려는 시도
        - e.g., 사용자가 온라인 쇼핑에서 결제를 한 후, 쇼핑몰에서 결제를 하지 않았다고 주장
      - 발신자 부인(Sender Repudiation)
        - 수신자는 메시지의 진위 여부를 확인할 수 있는 방법 필요
          - e.g., 디지털 서명, 로그 유지
      - 수신자 부인(Receiver Repudiation)
        - 발신자는 메시지가 성공적으로 전달되었음을 증명
          - e.g., 디지털 서명, 로그 유지

보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 가용성(1/4)
    - 서비스 거부(DoS, Denial of Service)
      - 시스템에 과도한 부하를 발생시켜 정당한 사용자가 해당 서비스를 이용할 수 없도록 만드는 공격
        - DoS : 한 대의 컴퓨터가 대량의 요청을 보내 서버를 마비시키는 경우
        - DDoS(Distrubuted DoS) : 수천 대의 감염된 컴퓨터가 동시에 특정 사이트에 접속을 시도하여 사이트를 다운시키는 경우

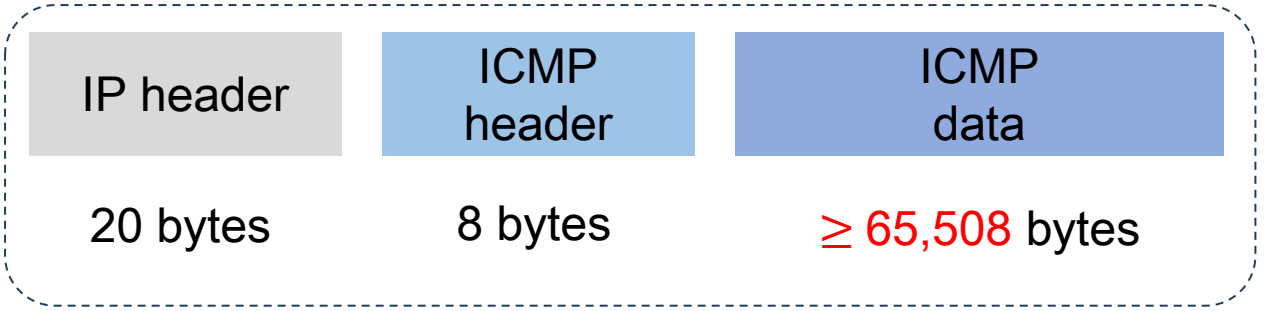
보안 개요

- 공격(Attack)
  - 적극적 공격(Active Attack) – 가용성(2/4)
    - 서비스 거부 공격(DoS)의 종류
      - Land 공격
        - 출발지 IP 주소와 목적지 IP주소값을 똑같이 만들어서 공격 대상에게 전달
          - e.g., 최신 보안 패치 적용, 방화벽 설정



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, MTU보다는 큰 Ping을 차단하거나 일정 수 이상의 ICMP 패킷을 무시하도록 설정

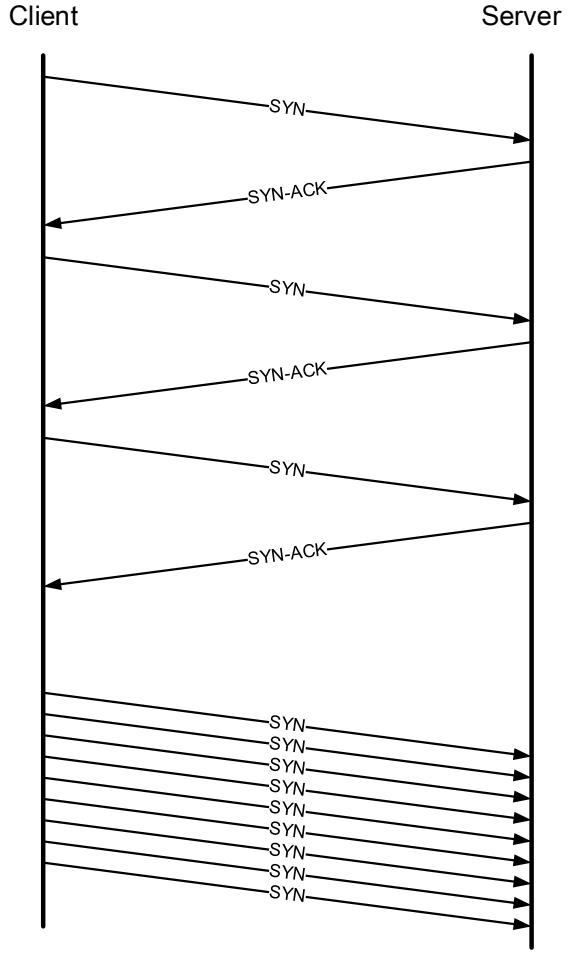


*MTU(Maximum Transmission Unit)
네트워크를 통해 전송될 수 있는 최대 패킷 크기. 일반적으로 이더넷의 MTU는 1500 바이트

* 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
      - TCP SYN Flooding 공격
        - TCP 패킷의 SYN 비트를 이용한 공격 방법으로 대량의 요청을 전송해 대상의 시스템을 Flooding 하게 만드는 공격
        - SYN 패킷에 대해 SYN-ACK 보내고 클라이언트가 ACK를 기다리는데 ACK가 오지 않아 연결 대기열이 가득 차게 됨 즉, 악의적인 SYN만 보냄으로써 서버의 SYN Backlog을 가득 채워 신규 커넥션을 받지 못함
          - e.g., SYN cookies 사용



보안 개요

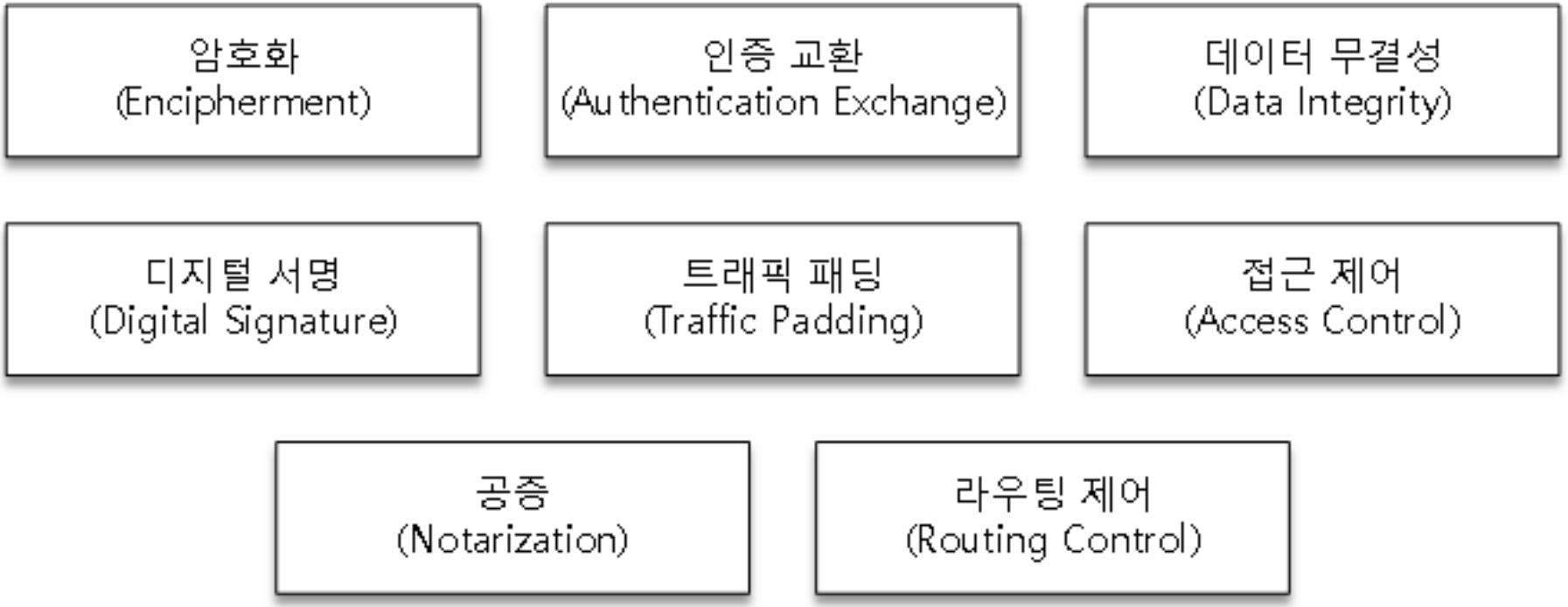
- 보안 서비스
  - 시스템이나 데이터의 보안을 유지하기 위해 제공되는 기능이나 작업

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.>

보 안 개 요

- 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 이해할 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
  - 디지털 서명(Digital Signature)
    - 데이터를 전자적으로 서명하고, 그 서명을 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 (3/3)
  - 접근 제어(Access Control)
    - 사용자가 데이터나 데이터의 출처에 대한 접근권한을 가지는지 여부를 입증하기 위한 방법
      - e.g. ACL(Access Control List), RBAC(Role Base Access Control)
  - 인증 교환(Authentication Exchange)
    - 두 당사자가 서로의 신원을 확인하기 위해 교환하는 방법
      - e.g., MAC(Message Authentication Code)

보안 개요

- 암호
  - 대칭-키 암호화 (Symmetric-key Encipherment)
    - 동일한 키를 사용하여 데이터를 암호화하고 복호화
    - 대량의 데이터를 암호화하기 편리
      - 암/복호화하는 것이 비대칭키에 비해 연산의 복잡성이나 속도가 빠름
      - 고정된 크기의 블록으로 처리하기 때문에 메모리 사용이 예측가능해 CPU와 메모리 자원을 덜 소모함.
      - 사람이 증가할 수록 키 관리가 어려워지며 탈취의 우려가 있음
  - 비대칭-키 암호화 (Asymmetric-key Encipherment)
    - 공개키(Public key)로 암호화하고 개인키(Private-key)로 복호화
      - 키 분배가 불필요하며 대칭키에 비해 안전성이 높음
      - SSL/TLS 프로토콜에서 클라이언트와 서버 간의 세션 키를 안전하게 교환하는 데에 사용하거나 디지털 서명에 사용
      - 대칭키에 비해 복잡한 연산으로 속도가 느리며 동일한 보안 수준을 유지하기 위해 긴 키를 필요로 함
        - 128비트 대칭키 암호화는 약 3073비트의 RSA 키와 유사한 보안 수준을 제공

보안 개요

- 암호

대분류	중분류	알고리즘	설명
대칭키 방식	블록 암호 알고리즘	3DES	DES의 보안성을 강화하기 위해 개발된 알고리즘으로, 세 번의 DES 암호화 연산 사용
		AES	128, 192, 256 bit키를 사용하며 128 bit 블록 처리 키 크기에 따라 10, 12, 14회 라운드 수행 e.g., HTTPS 통신에서 데이터를 암호화
		SEED	128 bit 키와 블록 사용 국제표준 부합, 민간 사용 목적 e.g., 국내 금융 기관이나 정부 기관에서 정보 보호 목적으로 사용
	스트림 암호	RC4	키 길이에 따라 다양한 비트 수의 출력 스트림 생성
비대칭키 방식	인수분해	RSA	큰 숫자를 소인수분해하는 게 어렵다는 것에 기반하여 개발 e.g., HTTPS의 인증서에 사용되어 웹 브라우저와 웹 서버간의 통신을 보호
	이산대수	DSA	유한체 상의 임의의 수를 기반으로 하는 이산 로그 문제와 관련된 수학적 연산 사용

보안 개요

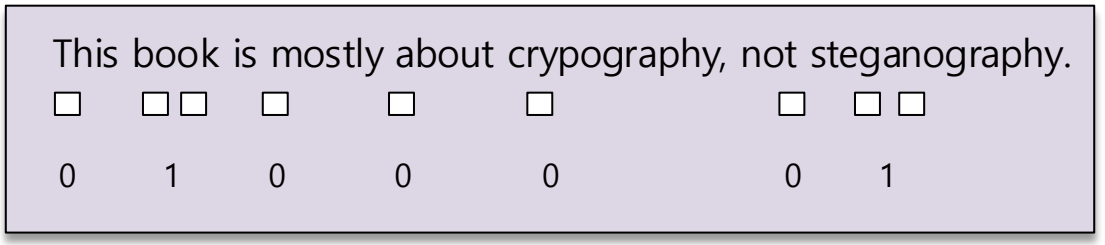
- 암호
  - 해싱(Hashing)
    - 다양한 길이의 메시지를 해시함수(Hash Function)로 고정된 길이의 메시지로 압축
    - 해싱 완료시, 해시값을 통해 원해 문자열을 알 수 없으며 변조 여부만 확인 가능(단, 비밀키 사용시에만 본래 문자열 알 수 있음)
    - 동일 문자열은 동일 해시 알고리즘을 사용 시 반드시 동일한 해시값을 출력
  - 암호화와 해싱의 차이
    - 암호화: 수신자와 송신자 사이의 암호화와 복호화 두 단계가 존재하며 '데이터 노출 최소화'가 목표
    - 해싱: 암호화된 텍스트의 해시값을 검사해 '데이터 변조가 없었는지 자체의 무결함의 증명하는 것'이 목표

보안 개요

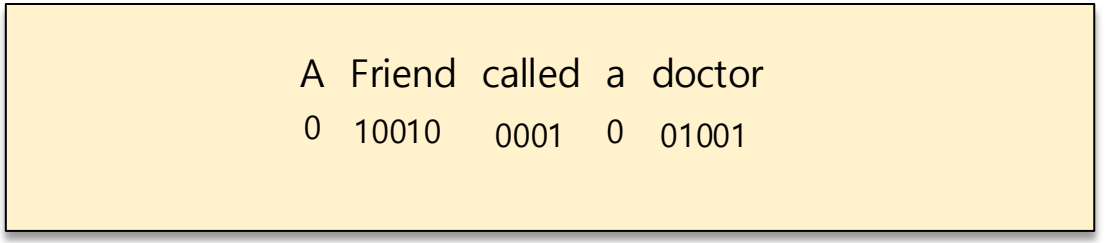
- 스테가노그래피(Steganography)(1/3)
  - 메시지를 다른 것으로 덮어서 감추는 것
  - 역사적 사용
    - 메시지를 나무 조각에 새긴 뒤 밀랍에 담금
    - 메시지 행간, 종이의 뒷면에 비밀 메시지를 적음
      - 일정 각도의 빛에 노출될 때 메시지가 드러나도록 함
      - e.g., 양파주스, 암모니아 소금
    - 무의미한 메시지 안에 비밀 메시지를 숨기는 널 암호 (Null Cipher)

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 11001101 11110000
픽셀 2	10010010 10101011 11001101
픽셀 3	11100010 10010011 10111010

목 차

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

암호 수학

- 대수 구조(Algebraic Structure)
  - 집합과 그 집합에 포함된 원소들에 적용되는 연산
  - 일반적인 대수 구조
    - 군(G, group)
    - 환(Ring)
    - 체(Field)

대수 구조

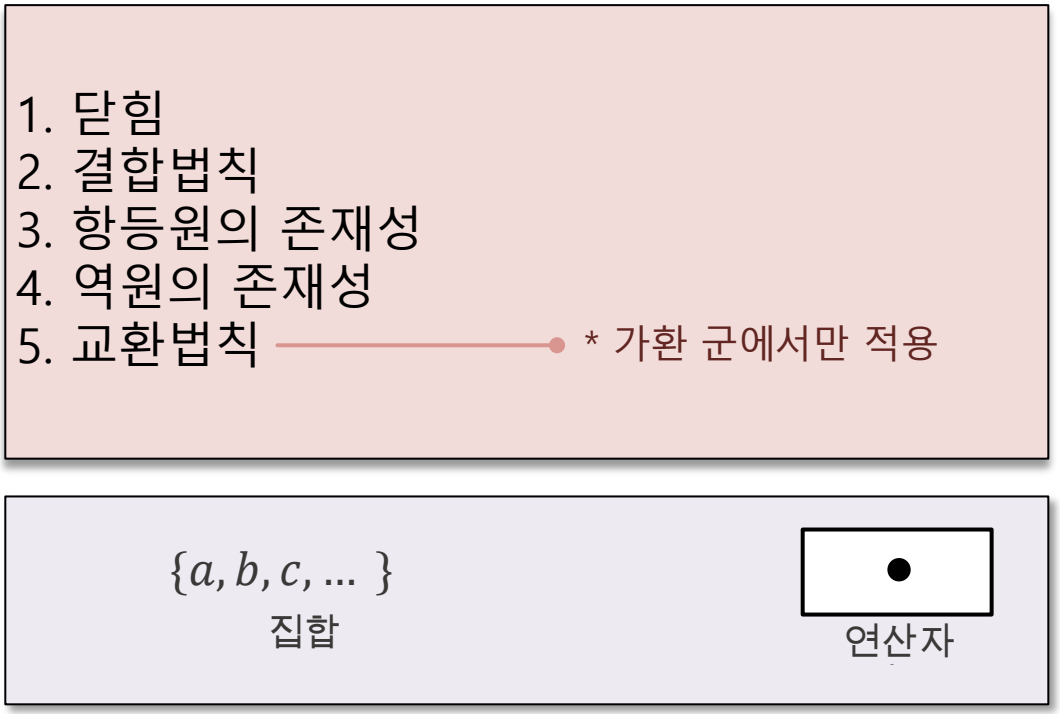
- 군(G, group)
  - 정의
    - 네 개의 성질을 만족하는 이항 연산 "•"이 정의된 원소들의 집합

$$G = < G', \bullet >$$

      - 이항연산 : 수학적으로, 두 개의 원소를 가지고 하나의 결과를 생성하는 연산
  - 성질
    - 닫힘
      - a와 b가 G의 원소인 경우, $c = a \cdot b$ 또한 G의 원소
    - 결합법칙
      - a, b, c가 G의 원소인 경우 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$를 만족
    - 항등원의 존재성
      - G의 임의의 원소 a에 대해, $e \cdot a = a \cdot e = a$를 만족하는 항등원 $(Identity\ Element)$ e가 존재
    - 역원의 존재성
      - G의 원소 a에 대해, $a \cdot a' = a' \cdot a = e$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)
    덧셈 연산이 정의된 $G = < Zn, + >$ (Zn = {0, 1, ⋯ , (n − 1)})은 가환군

    - 집합은 연산에 대해 닫혀있음

      $0 \leq a, b < n$
      $0 \leq a + b < 2n$
      $\rightarrow mod\ n$
      $0 \leq a + b < n$
    - 결합법칙 만족
      - e.g., $(4 + 3) + 2 = 4 + (3 + 2)$
    - 교환법칙 만족
      - e.g., 5+2 = 2+5
    - 항등원 0
      - 모든 정수, 실수 집합의 덧셈 항등원은 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)
  - 부분군(H, Subgroup)
    - G = <S, •>가 군이고, T가 S의 공집합이 아닌 부분 집합이라고 할 때, 군 $H = < T, \cdot >$ 는 G의 부분군이다.

    - H는 G의 항등원을 포함
    - H는 자기 자신에 대해 폐쇄적
      - e.g., 짝수 집합의 원소들 끼리 더하면 짝수
    - H는 각 원소의 역원을 포함
      - 예제) 군$H = < Z_{10}, + >$ 는 군$G = < Z_{12}, + >$ 의 부분군인가?
        - 폐쇄성의 성질을 만족하지 않음

대수 구조

- 군(G, group)
  - 순환 부분군(Cyclic Subgroup)
    - 만약 군의 부분군이 어떤 원소의 멱승(power)을 사용하여 생성된다면 부분군을 순환 부분군이라고 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
  - 순환군
    - 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 $G = < Zn^*, \times >$ 로부터 세 개의 순환 부분군이 생성
      - $H_1 = < \{1\}, \times >$, $H_2 = < \{1,9\}, \times >$, $H_3 = G$

✓ H_1은 항등원만을 원소로 갖는 집합
$1^0 \ mod \ 10 = 1$ (중지 : 이런 과정 반복)

✓ H_3은 3으로부터 생성된 순환 부분군

$$3^0 \ mod \ 10 = 1$$
$$3^1 \ mod \ 10 = 3$$
$$3^2 \ mod \ 10 = 9$$
$$3^3 \ mod \ 10 = 7$$

✓ H_3은 7로부터 생성된 순환 부분군

$$7^0 \ mod \ 10 = 1$$
$$7^1 \ mod \ 10 = 7$$
$$7^2 \ mod \ 10 = 9$$
$$7^3 \ mod \ 10 = 3$$

대수 구조

- 군(G, group)
  - 예제)
    - 군 $G = < Zn^*, \times >$ 로부터 세 개의 순환 부분군이 생성
      - $H_1 = < \{1\}, \times >$, $H_2 = < \{1,9\}, \times >$, $H_3 = G$

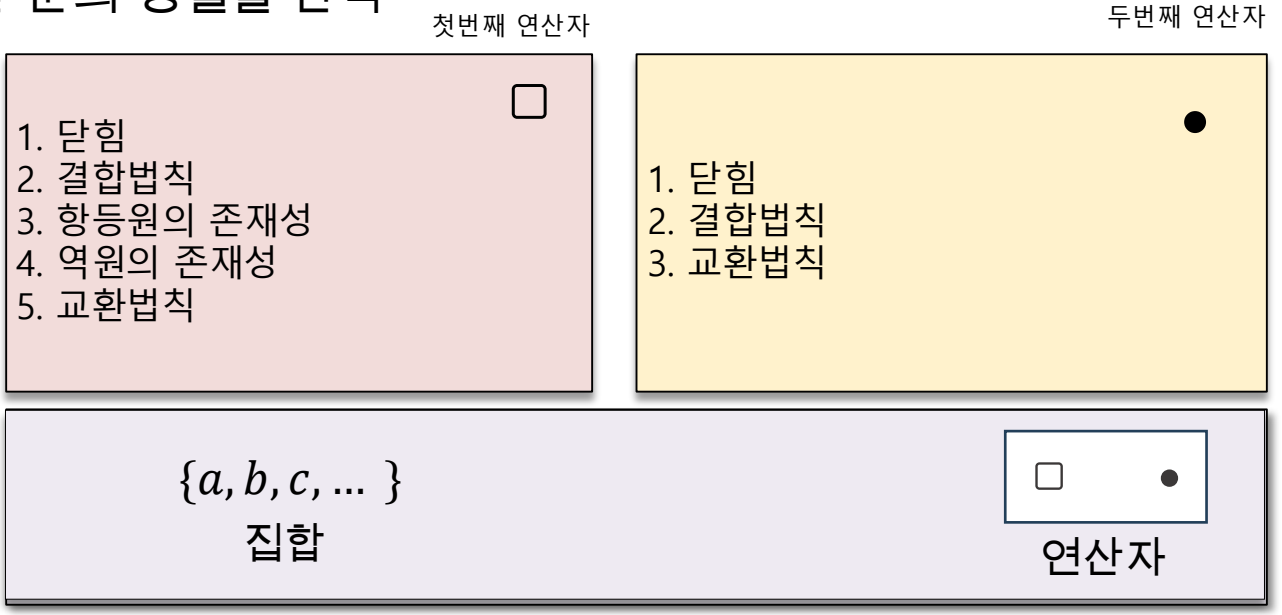
      ✓ H_2는 9로부터 생성된 순환 부분군
      $9^0 \ mod \ 10 = 1$
      $9^1 \ mod \ 10 = 9$

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
      - 군의위수 : 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

- 환(Ring)
  - 정의
    - 집합 R'에 두 연산 ▢, • 이 정의된 대수구조 $R = < R', ▢, \cdot >$
      - 특정 암호시스템에서 주로 사용(e.g., 격자 기반 암호)
  - 성질
    - 첫 번째 연산 < R′, ▢>은 가환 군의 성질을 만족
    - 두 번째 연산 < R′, •>은 반 군의 성질을 만족

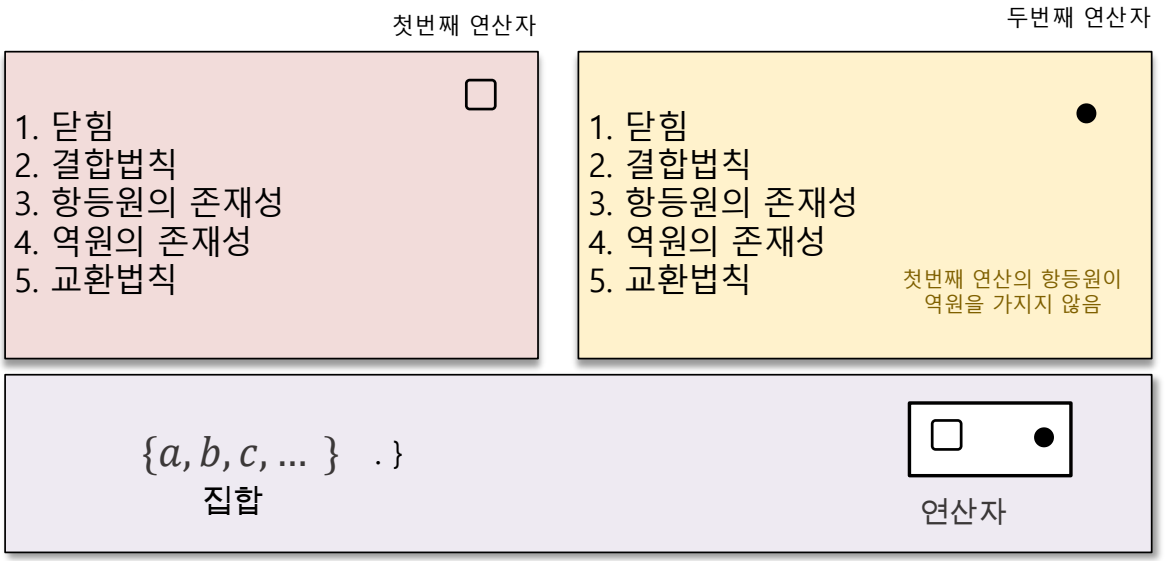


대수 구조

- 환(Ring)
  - 특징
    - 두 번째 항등원은 역원이 없을 수도 있음
      - 첫 번째 연산은 +,-만이 들어갈 수 있으며 두 번째 연산은 x만 들어갈 수 있음
      - 예제)
        - 덧셈과 곱셈의 두 연산이 정의된 집합 Z_n은 가환환일 때, 첫 번째 연산은 덧셈과 뺄셈을 모두 사용할 수 있으나 두 번째 연산은 나눗셈이 아닌 곱셈만이 들어갈 수 있다
          → 나눗셈은 집합 밖의 원소를 만들어냄
          $5 \div 2 = 2.5$

대수 구조

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



대수 구조

- 체(Field)
  - 유한 체(Finite Field)

"갈로아 체 $GF(p^n)$는 p^n개의 원소를 갖는 유한 체이다"

- 원소의 개수 p^n (p는 소수, n은 양의 정수)
- 갈로아 체(Galois field)라고 부름
- $GF(p^n)$

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

$+$	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 연산(일반적으로 덧셈, 곱셈)으로 구성된 대수적 구조
    - 폐쇄성, 결합법칙, 항등원, 역원을 만족 (가환 군은 교환법칙까지)
  - 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

- 개요
  - 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 경우, 집합의 원소들이 비트 형태로 표현되기 때문에 네 개의 연산들이 적용될 수 없음
    - 예제)
      2비트 워드들로 구성된 집합 $\{00, 01, 10, 11\}$인 $GF(2^2)$체를 정의할 수 있음

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

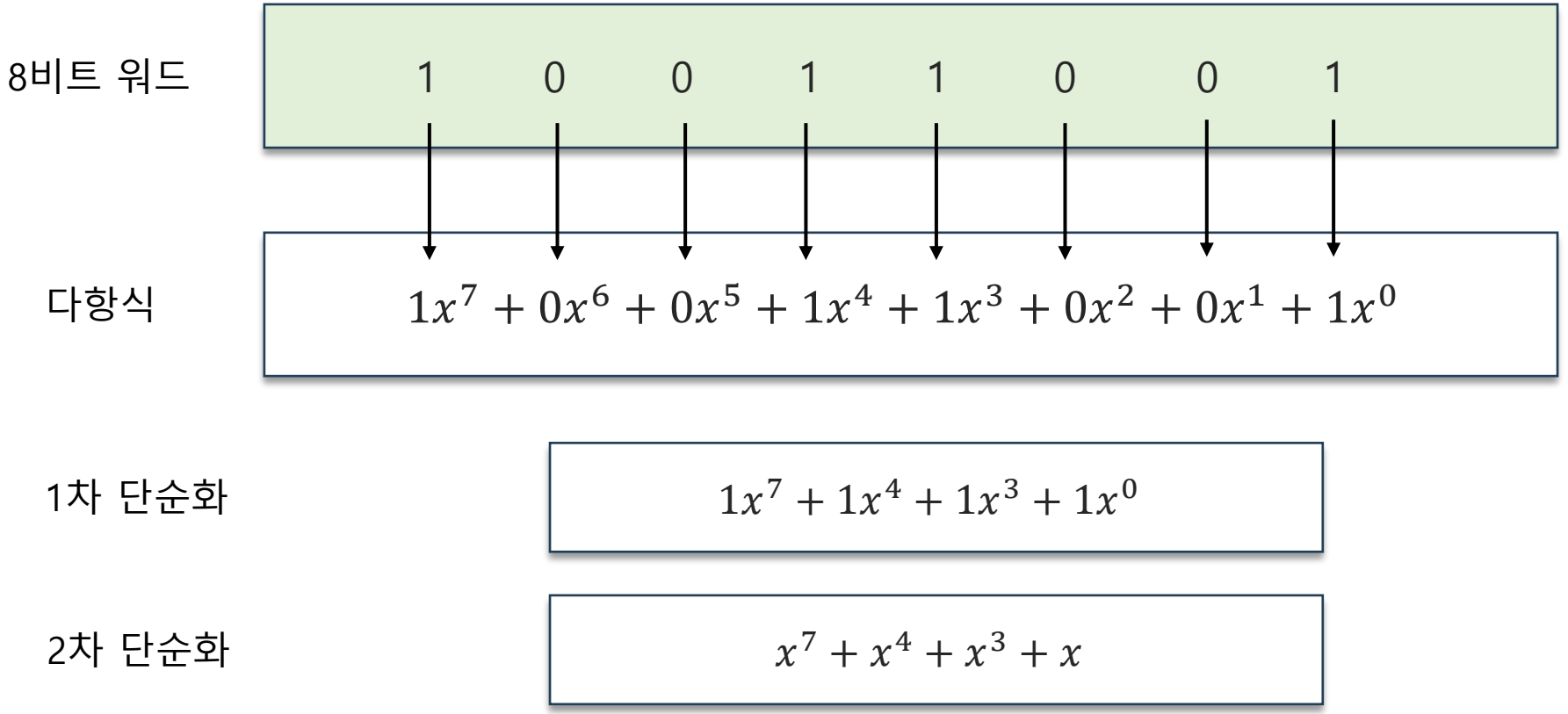
- 다항식(Polymjomial)
  - n비트 워드들을 차수 $n-1$의 다항식 형태로 표현

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

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

$GF(2^n)$체

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



$GF(2^n)$체

- 다항식(Polymjomial)
  - 연산
    - n비트 워드들을 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(Polymjomial)
  - 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(Polymjomial)
  - 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(Polymjomial)
  - 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 유한체
    - 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)