

# 암호학과 네트워크 보안

- 보안 개요, 암호 수학 -

우 승 찬([seungchan@pel.sejong.ac.kr](mailto:seungchan@pel.sejong.ac.kr))

세종대학교 프로토콜공학연구실

# 목 차

---

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

# 목 차

---

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

# 보안 개요

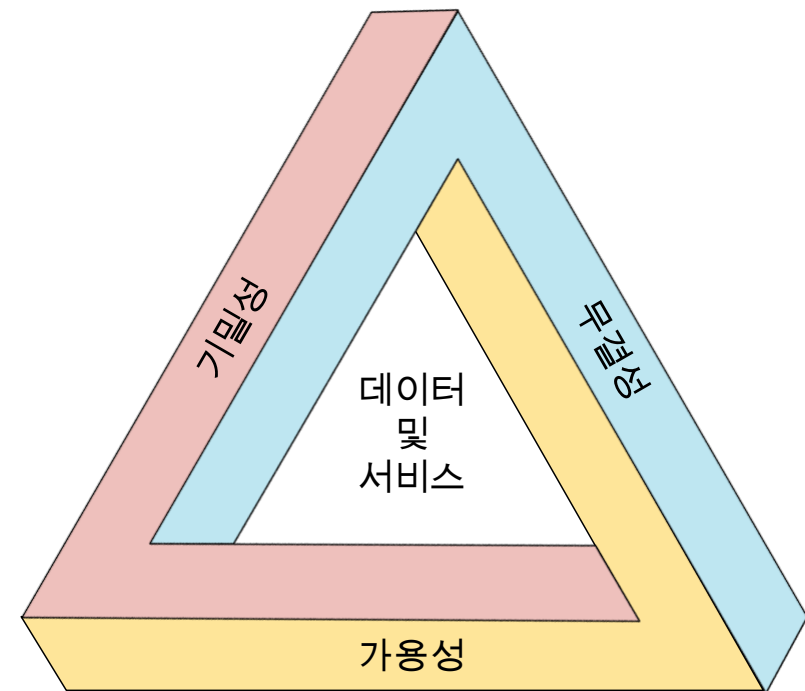
- 개요

- 정보를 안전하게 보호하기 위해서는 보안 목표를 만족해야 함

- 보안 목표

- CIA 트라이어드

- 기밀성(Confidentiality)
      - 정보 내용의 노출 방지
    - 무결성(Integrity)
      - 정보 내용의 변조 방지
    - 가용성(Availability)
      - 정보 사용의 지연 방지



# 보안 개요

---

- 보안 목표

- 기밀성(Confidentiality)

- 비인가자로부터 정보의 내용이 노출되지 않도록 하는 것
  - 전송되는 데이터의 내용을 보호하여, 비인가자가 정보의 실제 내용에 접근하는 것을 방지함

- 무결성(Integrity)

- 비인가자로부터 정보가 변경되거나 삭제되지 않도록 하는 것
  - 데이터가 제3자에 의해 중간에 변조하는 것을 방지함

- 가용성(Availability)

- 정보를 인가된 자가 필요로 하는 시점에 접근 가능해야 하고 접근에 방해받지 않도록 하는 것

# 보안 개요

---

- 공격(Attack)

- 정보의 안전성을 침해하는 것과 관련된 모든 행위
  - 보안의 세 가지 목표는 보안 공격에 의해서 위협받음

- 적극성에 따른 분류

- 소극적 공격

- 공격자의 목표는 단지 정보를 획득하는 것
    - 공격자가 데이터를 변경하거나 시스템에 해를 끼치지 않음
    - 공격을 탐지하기가 어려움

- 적극적 공격

- 데이터를 바꾸거나 시스템에 해를 입힘
    - 공격자가 다양한 방법들을 사용하기 때문에 방어하기보다는 탐지하기가 쉬움

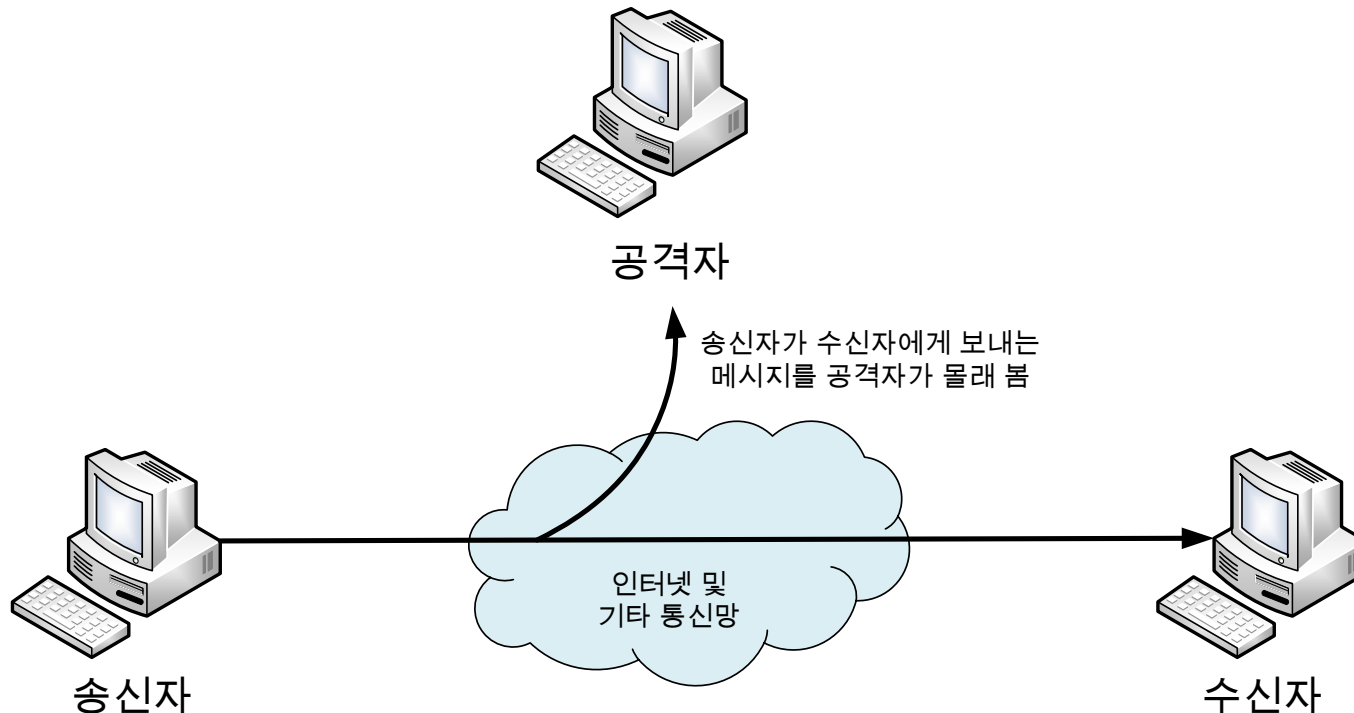
# 보안 개요

- 공격(Attack)

- 소극적 공격(Passive Attack) (1/2)

- 스누핑(Snooping)

- 공격자가 전달되는 정보와 내용을 몰래 취득하거나 보는 것
      - e.g., 기밀 정보를 가지고 있는 메시지 탈취



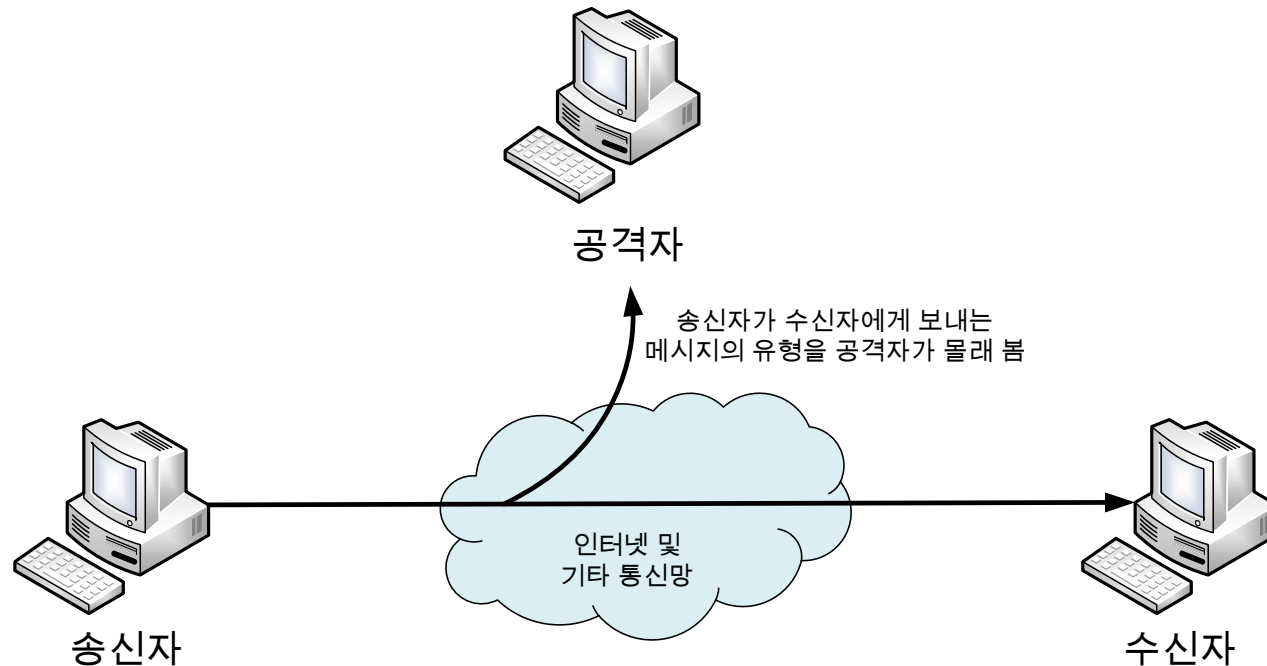
# 보안 개요

- 공격(Attack)

- 소극적 공격(Passive Attack) (2/2)

- 트래픽 분석(Traffic Analysis)

- 암호화된 데이터의 트래픽을 분석함으로써 다른 형태의 정보를 얻는 것
      - e.g., 와이어샤크





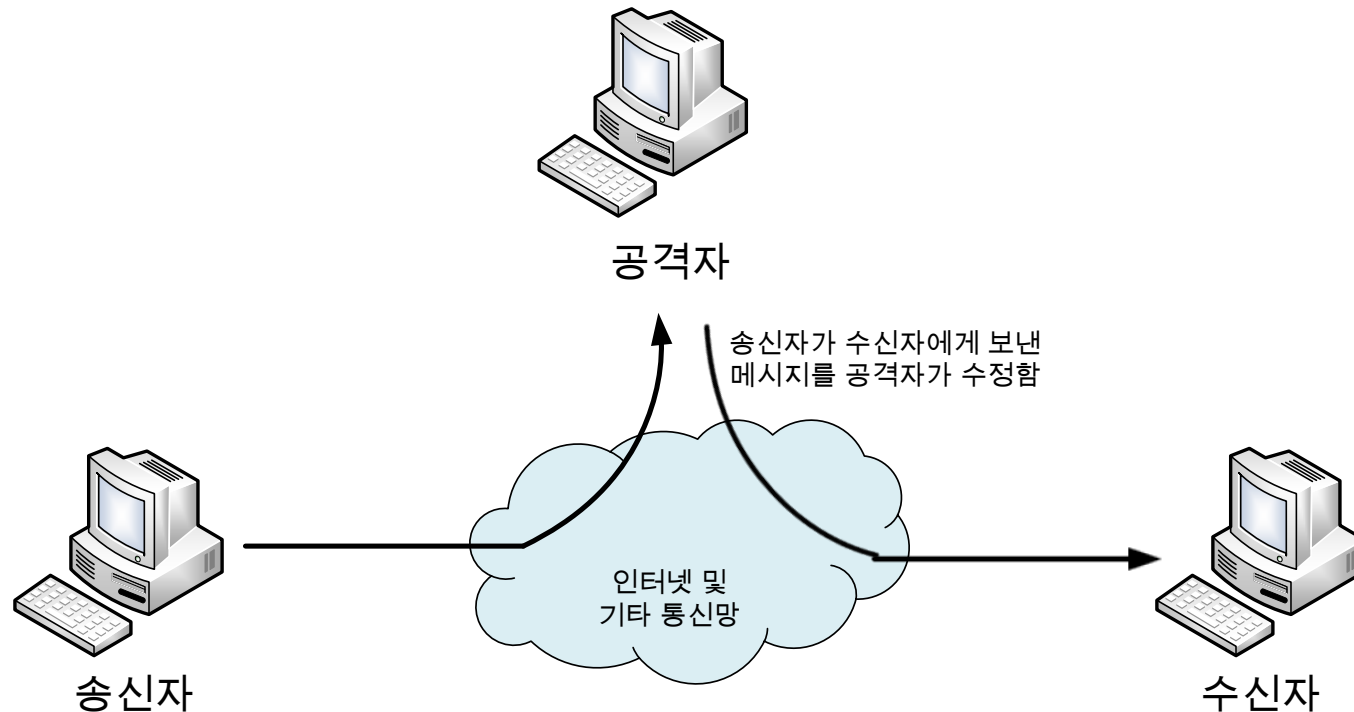
# 보안 개요

- 공격(Attack)

- 적극적 공격(Active Attack) (1/4)

- 변경(Modification)

- 공격자가 정보를 획득한 후 자신에게 유리하도록 정보를 조작하는 것
      - e.g., 메시지 본문에 악의적인 내용을 삽입



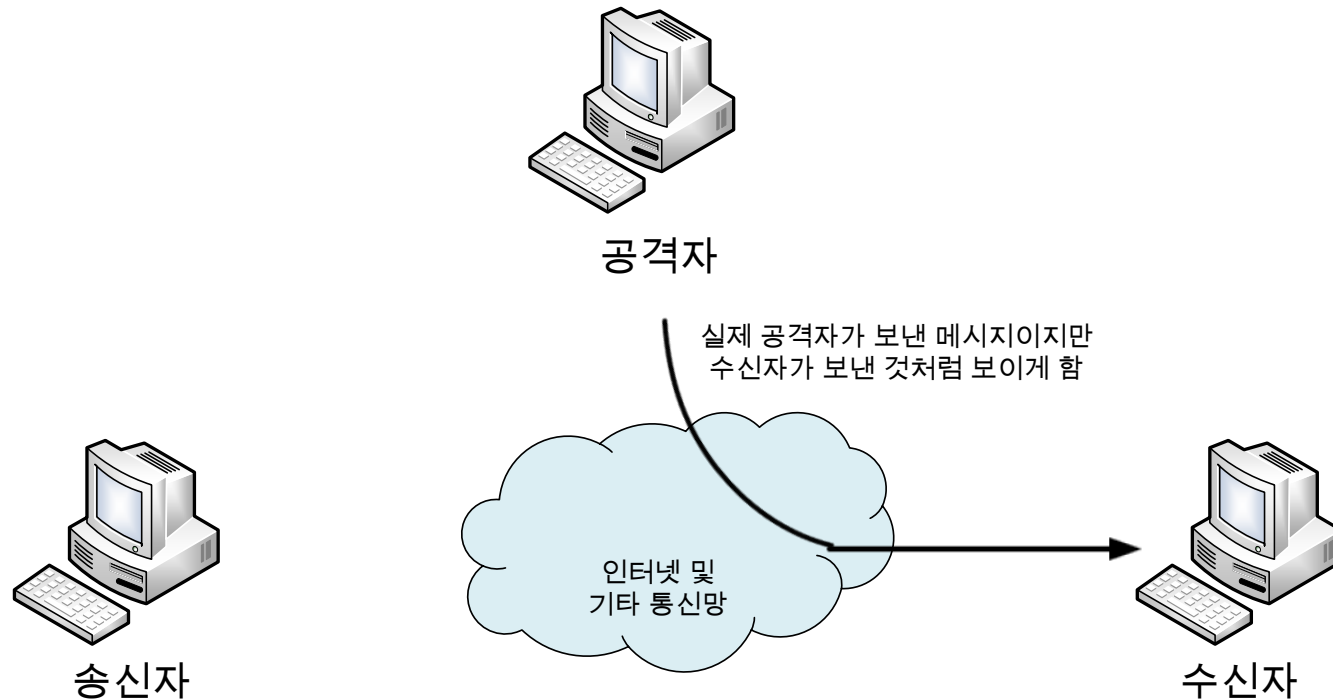
# 보안 개요

- 공격(Attack)

- 적극적 공격(Active Attack) (2/4)

- 신분 위장(Masquerading)

- 권한을 가진 개체처럼 가장하여 공격을 행사하는 것
    - 다른 형태의 적극적 공격과 병행해서 수행됨
      - e.g., 성적입력 시스템 접근에 권한을 가진 개체로 위장하여 데이터 변경



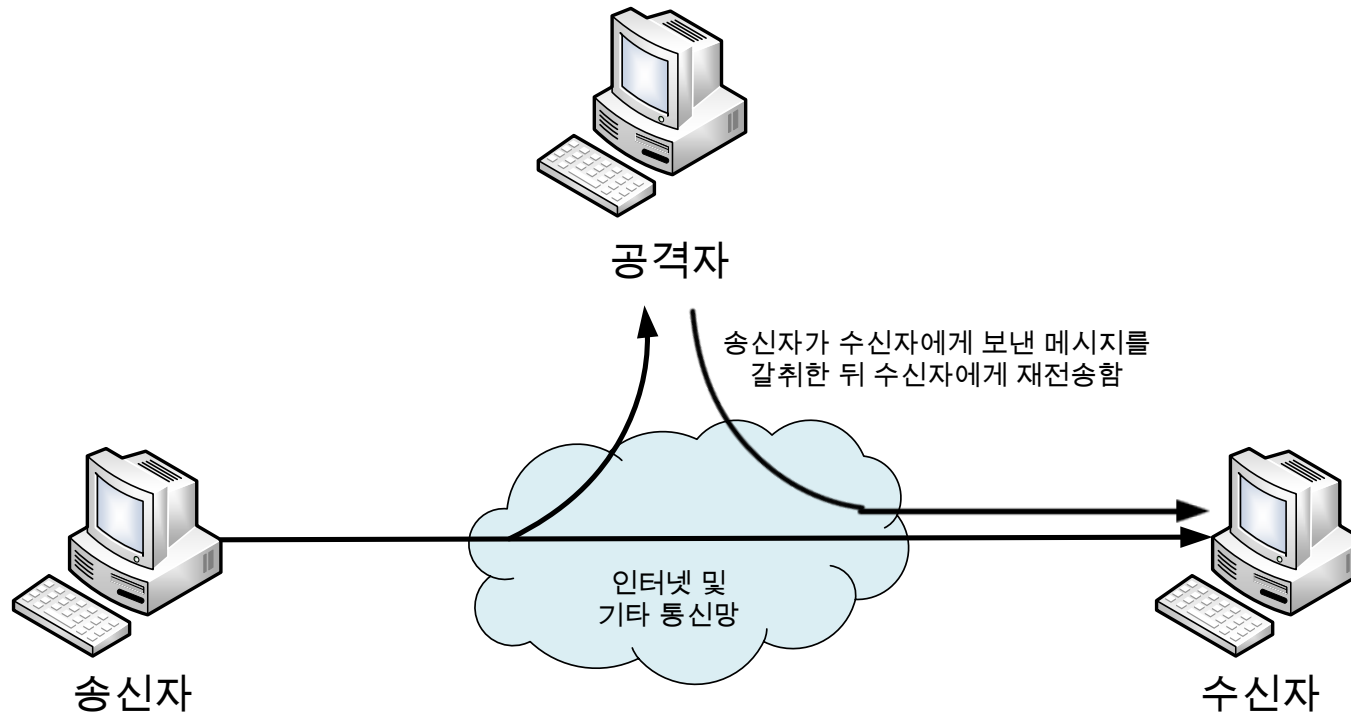
# 보안 개요

- 공격(Attack)

- 적극적 공격(Active Attack) (3/4)

- 재전송(Replaying)

- 획득한 데이터를 보관하고 있다가 시간이 경과한 후 재전송하여 인가되지 않은 사항에 접근하는 공격 형태
      - e.g., 공격자가 해시를 탈취하고 수신자에게 재전송



# 보안 개요

---

- 공격(Attack)
  - 적극적 공격(Active Attack) (4/4)
    - 서비스 거부(DoS, Denial of Service)
      - 시스템의 서비스를 느리게 하거나 완전히 차단시키는 공격
      - 대량의 데이터 패킷을 통신망으로 보내 과부하를 일으킴
    - 분산 서비스 거부(DDoS, Distributed DoS)
      - 공격자를 분산적으로 배치해 동시에 서비스 거부 공격을 하는 방법

# 보안 개요

- 서비스와 메커니즘

- 보안 서비스

- 시스템의 보안이나 데이터 전송의 보안을 보장하기 위해 제공되는 서비스
- 보안 메커니즘에 의해 보안 서비스가 구현됨



# 보안 개요

---

- 서비스와 메커니즘

- 보안 서비스(1/2)

- 데이터 기밀성(Data Confidentiality)

- 인가된 개체만 데이터를 읽을 수 있도록 보호하는 서비스
    - 메시지의 일부분이나 전체에 대한 기밀성을 포함

- 데이터 무결성(Data Integrity)

- 수신된 데이터가 인증된 개체로 보낸 것과 정확히 일치하는 지에 대한 확신을 제공하는 서비스

- 연결형 무결성 서비스

- 보낸 메시지가 변경 없이 송신되는 것을 보장함

- 비연결형 무결성 서비스

- 개별 IP 데이터그램의 수정에 대해서만 보호 서비스를 제공함

# 보안 개요

---

- 서비스와 메커니즘

- 보안 서비스(2/2)

- 인증(Authentication)

- 통신이 검증되었다는 것을 확인해주는 서비스
    - 대등 개체 인증
      - 연결하고 있는 개체의 신분을 확인시켜 줌
    - 데이터-출처 인증
      - 비연결 전송에서 수신된 데이터의 출처를 확인시켜 줌

- 부인봉쇄(Nonrepudiation)

- 통신의 주체가 통신에 참여했던 사실을 부인하는 것을 방지
      - 메시지가 잘 전송되었다는 증명을 제공함

- 접근 제어(Access Control)

- 비인가된 접근으로부터 데이터를 보호함
      - 누가 어떤 조건에 어떤 자원을 사용하도록 하는지와 같은 자원에 대한 접근을 제한

# 보안 개요

---

- 서비스와 메커니즘

- 보안 메커니즘(1/3)

- 보안 서비스를 구현하는데 사용되는 기술적 도구들

- 암호화(Encipherment)

- 수학적 알고리즘을 사용하여 데이터를 읽을 수 없는 형태로 변환하는 것
  - 데이터의 변환과 복구는 알고리즘에 사용되는 키에 따라 달라짐

- 데이터 무결성(Data Integrity)

- 데이터에 데이터를 검사하는 값을 추가하고 그 검사 값이 같을, 때 데이터 무결성이 보장됨
    - e.g., 체크섬



# 보안 개요

---

- 서비스와 메커니즘

- 보안 메커니즘(2/3)

- 트래픽 패딩(Traffic Padding)

- 공격자가 트래픽 분석을 하지 못하도록 트래픽에 가짜 데이터를 삽입

- 디지털 서명(Digital Signature)

- 송신자가 데이터에 서명을 하고 수신자가 그 서명을 검증하는 방법
      - e.g., 공인인증서(인증 기관에서 발급된 것을 증명)

- 인증 교환(Authentication Exchange)

- 자신의 신원을 다른 사람에게 증명하기 위하여 메시지를 교환함

# 보안 개요

---

- 서비스와 메커니즘

- 보안 메커니즘(3/3)

- 라우팅 제어(Routing Control)

- 공격자가 특정 경로에서 도착하지 못하도록 다른 경로를 선택하고 지속적으로 변화시켜줌

- 공증(Notarization)

- 신뢰할 수 있는 제3자를 통해 데이터 교환의 무결성, 출처, 목적지 등의 특성들을 보증하는 것

- 접근 제어

- 사용자가 시스템의 데이터나 데이터 출처에 대한 접근권을 가지는 지 여부를 입증하기 위한 방법을 사용함
- 비밀번호, PIN

# 보안 개요

- 서비스와 메커니즘
- 서비스와 메커니즘의 관계

보안 서비스	보안 메커니즘
데이터 기밀성	암호화, 라우팅 제어
데이터 무결성	암호화, 디지털 서명, 데이터 무결성 메커니즘
인증	암호화, 디지털 서명, 인증 교환
부인봉쇄	디지털 서명, 데이터 무결성 메커니즘, 공증
접근 제어	접근 제어 메커니즘

# 보안 개요

---

- 암호(Cryptography)
  - 대칭 키 암호화(Symmetric key Encipherment)
    - 암호화 하는 측과 복호화 하는 측이 하나의 비밀 키를 사용함
  - 공개 키 암호화(Public key Encipherment)
    - 하나의 키 대신 두개의 키 쌍, 즉 공개 키(Public-key)와 개인 키(Private-key)를 사용함
    - 공개 키를 통하여 암호화를 하고 복호화는 개인 키를 사용함
- 해싱(Hashing)
  - 키 값을 해시 함수(Hash Function)라는 수식에 대입시켜 계산하여 압축함
  - 데이터베이스 내의 항목들을 색인하고 검색하는데 사용

# 보안 개요

---

- 스테가노그래피(Steganography)
  - 메시지를 다른 것으로 덮어서 감추는 것
  - 역사적 사용
    - 보이지 않는 잉크를 이용하여 메시지 행간이나 종이의 뒷면에 비밀 메시지를 적음
      - e.g., 양파 주스, 암모니아 소금
    - 일정 각도의 빛에 노출될 때 메시지가 나오도록 함
  - 무의미한 메시지에서 각 단어의 첫 번째 또는 두 번째 문자가 비밀 메시지를 구성함

# 보안 개요

- 스테가노그래피(Steganography)
- 현대의 사용(1/2)
  - 텍스트 커버(Text Cover)
    - 텍스트를 이용하여 데이터를 숨김
    - e.g., A(0100001), HI(01001000 01001001)

This book is mostly about cryptography, not steganography

□	□□	□	□	□	□	□□
0	1	0	0	0	0	1

A	friend	called	a	doctor
0	10010	0001	0	01001

# 보안 개요

- 스테가노그래피(Steganography)
- 현대의 사용(2/2)
  - 이미지 커버(Image Cover)
    - 컬러 이미지 안에 데이터를 숨기는 것
    - 디지털 이미지는 3바이트의 픽셀로 구성됨
      - 빛의 삼원색(빨강, 녹색, 파랑)이 1바이트씩 표현
    - e.g., M

0101001 <u>1</u>	1011110 <u>0</u>	0101010 <u>1</u>
0101111 <u>0</u>	1011110 <u>0</u>	0110010 <u>1</u>
0111111 <u>0</u>	0100101 <u>0</u>	0001010 <u>1</u>

- 다른 커버
  - 오디오나 비디오 안에도 데이터를 숨길 수 있음

# 목 차

---

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



# 암호 수학

---

- 대수 구조(Algebraic Structure)
  - 집합과 집합에 포함된 원소들에 적용되는 연산
  - 일반적인 대수 구조



# 대수 구조

- 군( $G$ , group)

- 정의

- 네 개의 성질을 만족하고 이항 연산 “ $\cdot$ ”이 정의된 원소들의 집합

- 성질

- 닫힘

- 만약  $a$ 와  $b$ 가  $G$ 의 원소라면  $c = a \cdot b$  또한  $G$ 의 원소

- 결합 법칙

- 만약  $a, b, c$ 가  $G$ 의 원소라면,  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  를 만족

- 항등원의 존재성

- $G$ 의 임의의 원소  $a$ 에 대하여,  $e \cdot a = a \cdot e = a$  를 만족하는 항등원(Identity element)  $e$ 가 존재

- 역원의 존재성

- $G$ 의 원소  $a$ 에 대하여,  $a \cdot a' = a' \cdot a = e$  를 만족하는  $a$ 의 역원(Inverse) $a'$  존재

# 대수 구조

- 군(G, group)
- 가환 군(Commutative group)
  - 군의 네 개의 성질에 교환 법칙을 추가로 만족하는 군
    - 교환 법칙
      - G의 임의의 두 원소  $a, b$ 에 대하여,  $a \cdot b = b \cdot a$  를 만족

성질

1. 닫힘
2. 결합 법칙
3. 항등원의 존재성
4. 역원의 존재성

\* 교환 법칙 (가환 군에서만 만족)

$\{a, b, c, \cdot\}$



기호

군

# 대수 구조

- 군(G, group)

- e.g.,  $Z_n = \{0, 1, \dots, (n - 1)\}$  과 연산 기호  $+$ 가 정의된 군
  - 덧셈 연산이 정의된 집합  $G = \langle Z_n, + \rangle$  는 가환 군임
    - 이 군은 새로운 원소를 추가하지 않고 덧셈과 뺄셈 모두 사용
  - 성질 확인
    1. 집합은 연산에 대해 닫혀 있음  
 $Z_n$ 의 두 원소에 대한 합은  $Z_n$ 의 다른 값임
    2. 결합 법칙을 만족함 e.g.,  $4 + (3 + 2) = (4 + 3) + 2$
    3. 교환 법칙을 만족함 e.g.,  $3 + 5 = 5 + 3$
    4. 항등원이 0으로 존재함 e.g.,  $3 + 0 = 0 + 3 = 3$
    5. 모든 원소는 덧셈에 대한 역원을 가짐  
이 역원으로 뺄셈 사용 가능  
e.g., 3의 역원은 -3이고 -3의 역원은 3임

# 대수 구조

---

- 군( $G$ , group)
- 군의 종류
  - 유한 군(Finite group)
    - 유한 개의 원소를 갖고 있음
  - 무한 군(Infinite group)
    - 무한 개의 원소를 갖고 있음
- 군의 위수(Order)
  - 군에 있는 원소의 개수
    - 유한 군의 위수는  $n$ 개
    - 무한 군의 위수는  $\infty$ 개

# 대수 구조

- 환(R, ring)

- 두 개의 연산이 정의된 대수 구조  $R = \langle \{...\}, \bullet, \square \rangle$  로 표기
  - 첫 번째 연산은 가환 군에 요구되는 다섯 개 성질 만족
  - 두 번째 연산은 닫힘과 결합법칙을 만족하고 추가로 분배법칙을 만족함
- 가환 환(Commutative ring)
  - 두 번째 연산에 교환 법칙까지 만족하는 환

성질

<div>1. 닫힘</div> <div>2. 결합 법칙</div> <div>3. 교환 법칙</div> <div>4. 항등원의 존재성</div> <div>5. 역원의 존재성</div> <div><input checked="" type="checkbox"/></div>	<div>1. 닫힘</div> <div>2. 결합 법칙</div> <div>3. 분배 법칙</div> <div>* 교환 법칙 (가환 환에서만 만족)</div> <div><input type="checkbox"/></div>
<div>{a, b, c, · }</div> <div><div><input checked="" type="checkbox"/> <input type="checkbox"/></div><div>기호</div></div>	

환

# 대수 구조

- 환(R, ring)

- e.g., 정수 집합  $Z$ 와 연산 기호  $+, \times$ 를 정의한 환

- 덧셈과 곱셈의 두 연산이 정의된 집합  $R = \langle Z, +, \times \rangle$  은 가환 환임

- 덧셈은 다섯 개의 성질을 모두 만족함
    - 곱셈은 세 개의 성질을 만족함

- 성질 확인

1. 덧셈은 군의 5가지 성질 모두 만족
2. 집합은 연산에 대해 닫혀 있음  
 $Z$ 의 두 원소에 대한 곱은  $Z$ 의 다른 값임
3. 결합 법칙을 만족함 e.g.,  $4 \times (3 \times 2) = (4 \times 3) \times 2$
4. 교환 법칙을 만족함 e.g.,  $3 \times 5 = 5 \times 3$
5. 나눗셈은 집합 밖에 있는 원소를 만드므로 사용 불가  
e.g.,  $12 \div 5 = 2.4$

# 대수 구조

- 체(F, field)

- 첫번째 연산은 가환 군의 5가지 성질을 만족
- 두번째 연산은 첫 번째 연산의 항등원이 역원을 가지지 않는다는 것을 제외하고 가환 군의 5가지 성질을 만족
- $F = \langle \{ \dots \}, \bullet, \square \rangle$  로 표기됨

성질

- 1. 닫힘
- 2. 결합 법칙
- 3. 교환 법칙
- 4. 항등원의 존재성
- 5. 역원의 존재성



- 1. 닫힘
- 2. 결합 법칙
- 3. 교환 법칙
- 4. 항등원의 존재성
- 5. 역원의 존재성



(첫번째 연산의 항등원이 역원을 가지지 않음)

$\{a, b, c, \cdot\}$



기호

체



# 대수 구조

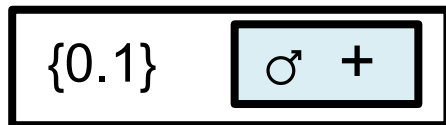
---

- 체(F, field)
- 유한 체(Finite field)
  - 유한개의 원소를 갖는 체
  - 유한 체가 암호에서 매우 중요한 구조
  - 유한개의 원소를 갖는 체의 원소의 개수는  $p^n$  임
    - $p$ 는 소수,  $n$ 은 양의 정수
- 유한체는 보통 갈로아 체(Galois field)라고 불리고  $GF(p^n)$ 으로 표현됨

# 대수 구조

- 체(F, field)
- $GF(P)$ 체
  - $n \neq 1$ 일 때의 갈로아 체
- $GF(2)$ 체
  - 현재 암호에서 가장 널리 쓰이는 체이다.

$GF(2)$



+	0	1
0	0	1
1	1	0

Addition

XOR 연산

$\otimes$	0	1
0	0	0
1	0	1

Multiplication

AND 연산

a	0	1
-a	1	0

a	0	1
$a^{-1}$	—	0

Inverses

# 대수 구조

- 정리

- 군, 환, 체 세 대수 구조는 덧셈/뺄셈, 곱셈/나눗셈과 같은 비슷한 연산이 정의된 집합들을 사용할 수 있게 해준다.

대수 구조	사용하는 일반적인 기호	사용하는 일반적인 정수 집합
군(group)	( + - ) or ( × ÷ )	$Z_n$ or $Z_n^*$
환(ring)	( + - ) and ( × )	$Z$
체(field)	( + - ) and ( × ÷ )	$Z_p$

# 목 차

---

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

# GF( $2^n$ )체

---

- GF( $2^n$ )체

- 암호학에서는 사칙연산(+ -  $\times$   $\div$ ) 이 모두 필요함  
즉, 암호학에서는 체를 사용
- 컴퓨터로 연산을 할 때, 양의 정수들은 컴퓨터에 n-비트 워드로 저장됨
  - n은 보통 8, 16, 32, 64
- 정수들의 범위는 0에서  $2^n - 1$ 이므로 모듈러는  $2^n$ 임

# GF(2<sup>n</sup>)체

- 다항식

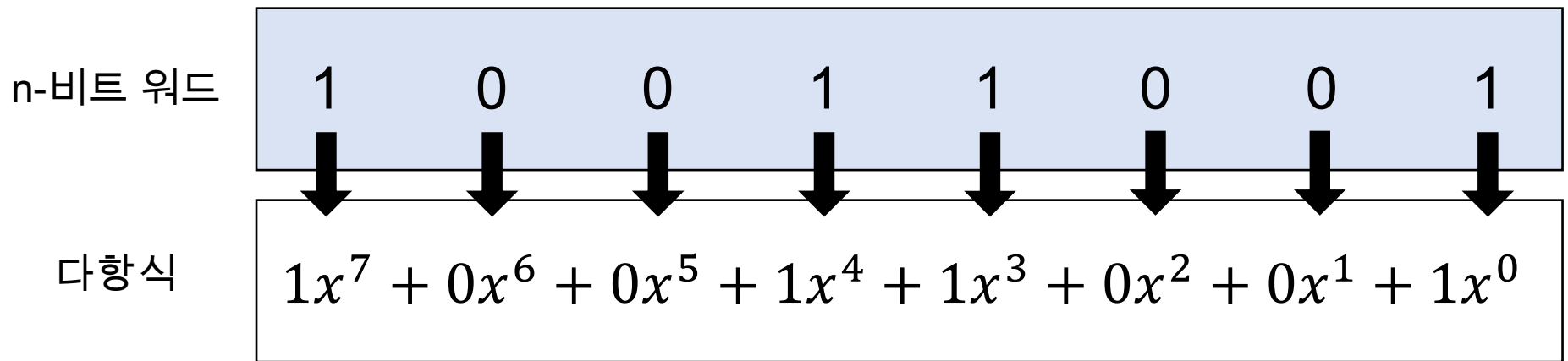
- n-비트 워드들 위에서 GF(2<sup>n</sup>)의 모든 성질들을 만족하는 연산 규칙을 정의할 수 있음
- 차수  $n - 1$ 의 다항식 형태로 표현하면 더욱 간단함.

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

- n-비트 워드들을 다항식으로 표현하기 위한 규칙
  - $x$ 의 지수승은 n-비트 워드에서 비트들의 위치를 정의함
  - 항들의 계수는 비트들의 값으로써 정의됨
    - 비트는 0과 1의 값을 갖기 때문에 다항식의 계수는 0 또는 1임

# GF( $2^n$ )체

- 다항식
- 예제



첫 번째 단순화

$$1x^7 + 1x^4 + 1x^3 + 1x^0$$

두 번째 단순화

$$x^7 + x^4 + x^3 + 1$$

# GF( $2^n$ )체

---

- 다항식

- 연산

- $n$ -비트 워드들을 표현하는 다항식들은 두 개의 체 GF(2)와 GF( $2^n$ )을 사용함

- 모듈로

- 두 다항식의 덧셈은 결코 그 집합에 속하지 않는 다항식을 생성하지 않음
- 두 다항식의 곱셈은  $n-1$ 보다 큰 차수를 가지는 다항식을 생성할 수도 있음
  - 모듈로 논리에 따라 모듈로 다항식으로 나누고 나머지만 생각함



# GF( $2^n$ )체

- 다항식
- 모듈로
  - 기약 다항식(Irreducible Polynomial)
    - 모듈로로써 정의되는 어떤 다항식으로도 나눌 수 없는 소수 다항식

차수	기약 다항식
1	$(x + 1), (x)$
2	$(x^2 + x + 1)$
3	$(x^3 + x^2 + 1), (x^3 + x + 1)$
4	$(x^4 + x^3 + x^2 + x + 1), (x^4 + x^3 + 1), (x^4 + x + 1)$
5	$(x^5 + x^2 + 1), (x^5 + x^3 + x^2 + x + 1), (x^5 + x^4 + x^3 + x + 1),$ $(x^5 + x^4 + x^3 + x^2 + 1), (x^5 + x^4 + x^2 + x + 1)$

# GF( $2^n$ )체

- 다항식

- 덧셈

$$1x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 \quad \text{+} \quad (+\text{는 XOR연산임})$$

$$0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0$$

$$-----$$
$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 \rightarrow x^5 + x^3 + x^1 + 1$$

- 덧셈에 대한 항등원

- 다항식 자신을 더하는 것은 0의 다항식을 만듦
  - 덧셈에 대한 항등원은 0의 다항식임

- 덧셈에 대한 역원

- GF(2)에서 계수를 가지는 다항식의 덧셈의 역원은 자기 자신임
  - 따라서 다항식의 덧셈과 뺄셈 연산은 같은 연산임

# GF( $2^n$ )체

- 다항식

- 곱셈

- 기약다항식을 이용하여 차수를 줄어줌

- 다항식 GF( $2^5$ ), 기약 다항식  $x^5 + x^2 + 1$

- $(x^4 + x^3 + 1) \times (x^3 + x^2 + 1) =$
- $x^4(x^3 + x^2 + 1) + x^3(x^3 + x^2 + 1) + (x^3 + x^2 + 1) =$
- $x^7 + x^6 + x^4 + x^6 + x^5 + x^3 + x^3 + x^2 + 1 =$
- $x^7 + x^5 + x^4 + x^2 + 1 =$
- $(x^7 + x^5 + x^4 + x^2 + 1) \bmod (x^5 + x^2 + 1) =$
- $x^2$

- 곱셈에 대한 항등원

- 항상 1임

- 곱셈에 대한 역원

- 두 다항식을 곱한 결과에 모듈로를 취했을 때의 나머지를 구함

# $GF(2^n)$ 체

---

- 뺄셈

- 덧셈과 뺄셈은 같은 연산임

- 나눗셈

- 나눗셈은 곱셈 역원을 사용한 곱셈

- 정리

- 유한체  $GF(2^n)$ 은  $n$ -비트 워드들에 대한 덧셈, 뺄셈, 곱셈, 나눗셈의 네 개의 연산들을 정의하기 위해 사용될 수 있음

---

# Thanks!

우 승 찬 ([seungchan@pel.sejong.ac.kr](mailto:seungchan@pel.sejong.ac.kr))