Contents

Chapter 1

이동 통신 보안

1.1 이동통신보안

1주차

암호화 기본 기법 네 가지. 이걸로 보안 시스템 구현 가능.

- 대칭키: $A : c = E(k, m)$, $A \to B : \mathsf{ID}(A), c$, $B : m = D(k, c)$. ID는 그 사람을 식별하기 위함. 공개키보다 빠르다. 블록 or 스트림 암호. 블록의 경우 운영모드가 있음. 전사공격 유일하게 허용. $O(2^n)$. AES, SEED, ARIA, LEA. 키 분배 문제. 확장성 문제(x명의 경우, $\binom{x}{2}$). 키 분배 문제: 키분배센터(KDC)라는 제 삼자 이용. KDC가 A와 B에게 k 전달. 커버러스 통신이 이거 사용.

$$\begin{aligned} A \to C &: \mathsf{ID}(A), \mathsf{ID}(B) \\ C \to A &: c_1 \leftarrow E_{k_{ac}}(k_{ab}), c_2 \leftarrow E_{k_{bc}}(k_{ab}) \\ A &: k_{ab} \leftarrow D_{k_{ac}}(c_1), c \leftarrow E_{k_{ab}}(m) \\ A \to B &: c, c_2 \\ B &: k_{ab} \leftarrow D_{k_{bc}}(c_2), m = D_{k_{ab}}(c). \end{aligned} \tag{1.1}$$

  이 과정의 문제점은, 키가 추가로 필요하다는 점. 추가로 필요한 키도 보호가 필요하다는 점. 이 문제를 공개키 암호가 해결할 수 있음.

- 공개키: 키가 두 개. 비밀키, 공개키. 둘은 수학적 연계. $B \to A : c = E_{pk_A}(m), A : m = D_{sk_A}(c)$. 내가 보냈음을 인증 가능. (인증, 부인방지. 공개키를 조작할 수 있나?) $B \to A : c = E_{sk_A}(m), A : m = D_{pk_A}(c)$. 이 둘을 합치면?

- 전자서명

- 해시

[1]

[1] 우리나라는 it 소비 강국. 해커의 공격이 많음.

Chapter 2

해석학 및 응용

Chapter 3

해석학 및 응용

3.1 1주차

3.1.1 체의 공리

다음이 성립하는 집합 $\mathbb{F}$를 체라고 한다.

- 덧셈: 교환 법칙, 결합 법칙, 0이 존재, 역원이 존재.
- 곱셈: 교환 법칙, 결합 법칙, 1이 존재, 역원이 존재.
- 분배 법칙.

실수 집합 $\mathbb{R}$은 체이다.

$\mathbb{R}$에는 다음 두 조건을 만족하는 $P(\neq 0)$가 존재한다.

3.1.2 순서의 공리

- 덧셈과 곱셈은 닫힘.
- $a \in \mathbb{R}$에 대해 다음 셋 중 단 하나만 성립. $a \in P, a = 0, -a \in P$.

순서가 있으니 $<, >, =$ 등을 사용할 수 있음.

Theorem 3.1.1. $\forall a, b, c \in \mathbb{R}, a > b, c > 0 \implies ac > bc$.

Proof. $a - b > 0, c > 0$이므로, $ac - bc = (a - b)c > 0$. 따라서 $ac > bc$이다. □

3.1.3 시작

X를 $\mathbb{R}$의 공집합이 아닌 부분 집합이라 하자.

Definition 3.1.1. $\forall x \in X, a \geq x$인 a가 존재 할 때, X를 위로 유계(bounded above)라 하고, a를 X의 상계(upper bound)이라 한다. $\forall x \in X, b \leq x$인 b가 존재 할 때, X를 아래로 유계(bounded below)라 하고, b를 X의 하계(lower bound)이라 한다.

Definition 3.1.2. a가 X의 상계이고, b가 X의 상계일 때, $a \neq b$라면, a를 X의 상한(supremum) 또는 (least upper bound)라 한다. 기호로는 $\sup X = a$로 나타낸다.

$X = (-\infty, 10)$일 때, 최댓값은 없고, $\sup X = 10$이다.

Chapter 4

소프트웨어적 사고

Chapter 5

리더십챌린지

Chapter 6

삶과 윤리

Chapter 7

인문학 리더십

Chapter 8

사제 동행 세미나

무요.