Contents

Chapter 1

Mobile Telecommunication Security

1.1 Cryptography Primitive

암호화의 기본 기법으로 대칭 키 암호화, 비대칭 키 암호화, 전자 서명 그리고 해시가 있다. 이를 바탕으로 보안 시스템을 구현할 수 있다.

Symmetric Key Encryption

대칭 키 암호는 암호화 키와 복호화 키가 같은 암호 알고리즘을 뜻한다. 따라서 송신자와 수신자는 서로 같은 키를 공유해야 한다. 대칭 키 암호 통신 과정은 1.1과 같다.

$$\begin{aligned} \mathcal{A} &: c = E(k, m) \\ \mathcal{A} \to \mathcal{B} &: ID(\mathcal{A}), c \\ \mathcal{B} &: m = D(k, c) \end{aligned} \tag{1.1}$$

블록 암호와 스트림 암호가 대칭 키 암호에 속한다. 대표적인 대칭 키 암호에는 AES, SEED, ARIA, LEA가 있다. 대칭 키 암호는 공개 키 암호보다 빠르기에 대용량 데이터를 암호화하는데 이점이 있으나, 다음과 같은 키 분배 문제를 가지고 있다는 단점이 있다.

- 같은 키를 어떻게 공유할 것인가? 공유 도중에 도청자가 키를 탈취할 수 있다.
- 많은 사람들이 통신을 할 경우, 사람마다 보유해야 하는 키가 많아진다. (x명의 경우, $\binom{x}{2}$)

키 분배 문제를 해결하기 위한 시도로 키 분배 센터(KDC)라는 신뢰가능한 제 3자를 이용할 수 있다. 커버러스라고 불리는 통신이 이를 사용한다. KDC를 이용한 통신 과정은 1.2와 같다. 그러나 이 또한 근본적으로 키 분배 문제를 해결하지 못한다.

$$\begin{aligned} \mathcal{A} \to \mathcal{C} &: ID(\mathcal{A}), ID(\mathcal{B}) \\ \mathcal{C} \to \mathcal{A} &: c_1 \leftarrow E_{k_{ac}}(k_{ab}), c_2 \leftarrow E_{k_{bc}}(k_{ab}) \\ \mathcal{A} &: k_{ab} \leftarrow D_{k_{ac}}(c_1), c \leftarrow E_{k_{ab}}(m) \\ \mathcal{A} \to \mathcal{B} &: c, c_2 \\ \mathcal{B} &: k_{ab} \leftarrow D_{k_{bc}}(c_2), m = D_{k_{ab}}(c). \end{aligned} \tag{1.2}$$

Asymmetric Key Encryption

비대칭 키(혹은 공개 키로도 불림)는 대칭 키 암호와 다르게 암호화 키(공개 키)와 복호화 키(비밀 키)가 다른 암호 알고리즘을 뜻한다. 두 키는 서로 수학적으로 연계되어, 하나의 키로 암호화 되었다면, 다른 하나의 키로만 복호화 할 수 있다. 통신 과정은 1.3와 같다. 비대칭 키 암호의 단점은 대칭 키 암호보다 느리기 때문에 작은 양의 데이터를 처리할 때 사용한다.

$$\begin{aligned} \mathcal{B} \to \mathcal{A} &: c = E_{pk_{\mathcal{A}}}(m) \\ \mathcal{A} &: m = D_{sk_{\mathcal{A}}}(c) \end{aligned} \tag{1.3}$$

공개 키 암호의 장점은 송신 시 자신이 통신하기로 한 송신자인지를 1.4와 같이 인증할 수 있다.

$$\begin{aligned} \mathcal{B} \to \mathcal{A} &: c = E_{sk_{\mathcal{A}}}(m) \\ \mathcal{A} &: m = D_{pk_{\mathcal{A}}}(c) \end{aligned} \tag{1.4}$$

일반적으로, 대용량의 데이터를 암호화하여 송신하고 싶을 때, 비대칭 키 암호를 이용하여 대칭 키를 암호화하여

공유하고, 대칭 키를 이용하여 데이터를 암호화하는 하이브리드 기법을 이용한다. 통신 과정은 1.5와 같다.

$$
\begin{aligned}
a &: kab \\
a &: c_1 = e(kab, M) \\
a &: c_2 = e(pk_b, k_a b) \\
atob &: c_1, c_2 \\
b &: k_a b = d(sk_b, c_2) \\
b &: m = d(k_a b, c_1)
\end{aligned}
\tag{1.5}
$$

암복호화, 전자서명(DSS), 키교환(DH). RSA, ECC는 전부 가능 RSA는 데탑에서는 사용할만한데...스마트폰이나 iot에서 사용할 때 문제가 생김 오버헤드가 너무 커. ECC는 이걸 해결해. TLS는 예전에는 RSA를 쓰다가 ECC로 바꿈.

Hash Function and Digital Signature

해시함수는 임의 길이의 데이터를 고정 길이 데이터로 변환하는 함수이다. 일방향 함수이며, 해시값은 통계적으로 유일. 해시함수는 데이터의 무결성(혹은 메시지 인증)을 검증하는데 활용됨.

$$
\begin{aligned}
&\mathcal{A} : \mathsf{sign} = E(sk_{\mathcal{A}}, H(m)), c = E(pk_{\mathcal{B}}, m) \\
\mathcal{A} \to \mathcal{B} :& \\
&\mathcal{B} : m = d(sk_b, c), checkh(m) = d(pk_a, ehash)
\end{aligned}
\tag{1.6}
$$

수동적인 공격자는 통신자 간에 전달되는 데이터를 도청만 하는 공격자를 말한다. 도청을 막기위해 기밀성이 필요하며, 통신자들은 공격자가 도청을 하는지 안하는지 알 수 없다. 반면에 능동적인 공격자는 도청뿐만 아니라 데이터를 직접 건드리는 공격자를 말한다.

mac은 공개키 기반이 아니라는 장점이 있다. 두 대상이 비밀키를 공유하고 있을 때, 메시지를 보낼 때 태그도 함께 보냄. 해시값을 대칭 키로 암호화.

$$
\begin{aligned}
\mathcal{A} &: \mathsf{mac} = E(k_{\mathcal{AB}}, H(m)) \\
\mathcal{A} \to \mathcal{B} &: m, \mathsf{mac} \\
\mathcal{B} &: \text{check } D(k_{\mathcal{AB}}, \mathsf{mac}) \stackrel{?}{=} H(m)
\end{aligned}
\tag{1.7}
$$

암호 기술 없이 사용하는 mac도 있음. 아래 참고. $s_{\mathcal{AB}}$은 사전에 공유한 비밀 값. 최근에는 hmac을 사용함.

$$
\begin{aligned}
\mathcal{A} &: \mathsf{mac} = H(m \parallel s_{\mathcal{AB}}) \\
\mathcal{A} \to \mathcal{B} &: m, \mathsf{mac} \\
\mathcal{B} &: \text{check } H(m \parallel s_{\mathcal{AB}}) \stackrel{?}{=} \mathsf{mac}
\end{aligned}
\tag{1.8}
$$

mac는 부인방지(자신이 보낸게 아니라고 시치미 때는 것을 막는 것)가 안됨. 왜냐하면 MAC값은 $\mathcal{A}$뿐만 아니라 $\mathcal{B}$도 만들 수 있기 때문. 이를 해결할 수 있는 방법으로 전사서명이 있음. 전자 서명은 인증에 추가로 부인방지까지

가능함. 전자서명 과정은 다음과 같음.

$$
\begin{aligned}
\mathcal{A} &: \text{generate } k_{\mathcal{AB}} \\
\mathcal{A} &: \mathsf{sign} = E(sk_{\mathcal{A}}, H(m)), c_m = E(k_{\mathcal{AB}}, m), c_k = E(pk_{\mathcal{B}}, k_{\mathcal{AB}}) \\
\mathcal{A} \to \mathcal{B} &: c_m, c_k, \mathsf{sign} \\
\mathcal{B} &: k_{\mathcal{AB}} = D(sk_{\mathcal{B}}, c_k) \\
\mathcal{B} &: m = D(k_{\mathcal{AB}}, c_m) \\
\mathcal{B} &: \text{check } H(m) \stackrel{?}{=} D(pk_{\mathcal{A}}, \mathsf{sign})
\end{aligned}
\tag{1.9}
$$

중간자 공격, 전달하는 메시지를 위조. 공개키를 자신의 공개키로 위조. 서명도 자신의 개인키로 서명. 그러면 받는 사람은 서명 검증 단계에서 valid를 얻음. 문제: 이 공개키가 진짜로 내가 통신하고자 하는 사람의 것인가? 해결시도: CA라고 하는 신뢰하는 제 3자에게 공개 키를 요구하는 방법. -¿ 근본적인 해결 X 이것도 통신중에 바뀔 수 있음.

해결방법: 이 공개키는 내거라는 인증서를 만든다. 신뢰할 수 있는 제 3자가 인증서 발행. 인증서에는 크게 소유자의 ID, 공개 키, 그리고 발급자의 서명(위조 방지)가 있다.

안전한 공개키 암호 기술을 사용하기 위해 공개키 기반 구조(PKI, 인증서를 사용하는 인프라)가 필요.

CA(certification authority): 인증기관. -¿ 인증서 관리. RA(registration authority): 등록기관. -¿ 사용자 신분 확인.

Y가 발행한 X의 인증서 Y¡¡X¿¿.

root 인증서 : 발급자와 요청자가 같은 사람.

root 인증서를 가지고 CA의 기능을 수행한다? 크롬에 설치?

CA가 하나만 있는건 현실적으로 어려움. 한국 사람이 중국의 CA를 신뢰해서 알리 익스프레스에서 거래가 가능한가? 여러 CA가 신뢰관계를 쌓아야함. -¿ X1이 X2의 인증서를 발급하여 A에게 전달. (신뢰관계 형성) -¿ A는 X2의 공개키를 신뢰할 수 있음.

인증서를 취소해야 할 때. 유효기간의 만료. 인증서가 사라져서 재발급 해야 할 때. 등

인증서 취소 목록(CRL) -¿ 취소 목록 생성 일시, 다음 생성 일시 (스케줄), 취소된 인증서 목록(일련번호, 취소 일시 등), CA의 서명.

시간이 지날수록 CRL 크기 증가. 시간차공격 가능. 단일 CRL일 경우 관리가 어려움.

인증서 검증 방법: 1. 유효한가? 2. 경로 검증 3. 인증서 용도 등...

자기가 자기한테 인증서를 발급한다. -¿ 루트인증서. 내 공개키를 신뢰하게 만드는 상위 CA가 없을 때.

미션?

Diffie-Hellman(이하 DH) 키 교환은 암호 키를 교환하는 하나의 방법으로, 두 사람이 암호화되지 않은 통신망을 통해 공통의 비밀 키 k를 공유할 수 있도록 한다. 휫필드 디피와 마틴 헬만이 1976년에 발표하였다. 앨리스 $\mathcal{A}$와 밥 $\mathcal{B}$이 공개된 통신망에서 DH 키 교환을 하기 위해서는 그림 1.1와 같은 절차를 거친다.

마지막 단계에서 $\mathcal{A}$와 $\mathcal{B}$은 $g^{ab} \mod p$라는 공통의 k를 공유하게 된다. $\mathcal{A}$와 $\mathcal{B}$ 외에는 a, b를 알 수 없으며, p, g, A, B만 알 수 있다. DH 키 교환은 통신을 하는 대상과 비밀 정보를 공유할 수 있지만, 상대방에 대한 인증은 보장되지 않으며 중간자 공격이 가능하다. $\mathcal{A}$와 $\mathcal{B}$이 상대방에 대한 인증을 하지 못할 경우, 공격자 $\mathcal{E}$는 그림 1.2과 같이 중간에서 통신을 가로채 $\mathcal{A}$와 $\mathcal{E}$, 그리고 $\mathcal{E}$와 $\mathcal{B}$ 사이에 각각 두 개의 DH 키 교환을 생성하고, $\mathcal{A}$와 $\mathcal{B}$이 각각 서로와 통신을 하는 것처럼 위장할 수 있다.

따라서, 공개 키 A 또는 B를 건네 받을 경우, 이 공개 키가 $\mathcal{A}$ 또는 $\mathcal{B}$의 공개 키가 맞는지 인증서를 이용하여 확인해야 한다.

공동인증기관(루트 CA) – 상호인증 – 정부 인증 체계

$$
\begin{array}{ccc}
\mathcal{A} & & \mathcal{B} \\
\text{choose } p, g & \xrightarrow{\qquad\qquad} & p, g \\
\text{choose } a & & \\
A \ := \ g^a \mod p & \xrightarrow{\qquad\qquad} & A \\
 & & \text{choose } b \\
B & \xleftarrow{\qquad\qquad} & B \ := \ g^b \mod p \\
k \ := \ B^a \mod p & & k \ := \ A^b \mod p
\end{array}
$$

Figure 1.1: Diffie-Hellman Key Exchange

1.2 Kerberos Protocol

인증을 하는 서버가 3개 나옴. 그래서 커버러스라고 함.

대칭키 암호를 사용한 사용자 인증.

상호인증: 통신 참여자가 각자 상대방 신분을 확인함. 키 교환 가능.

기밀성을 보장하는가? 메시지 재전송 공격을 막을 수 있는가? (적시성.)

옛날에 보낸 메시지를 도청해서 보관하다가 나중에 보내서 송신자인 척 함.

해결 방법: 1. 서로가 메시지를 보내고 받는 횟수를 카운팅함. 2. 시간정보를 넣음. 3. 랜덤값을 송신자한테 보내고 이걸 암호화하라고 함.

1.2.1 Needham Schroeder Protocol

니덤-슈로더 프로토콜. KDC 기반 세션키 분배 프로토콜. 앨리스와 밥은 KDC를 신뢰함. 앨리스와 밥은 각자 Ka Kb를 가지고 있음. KDC는 둘 다 가지고 있음.

$$
\begin{aligned}
\mathcal{A} \to \mathsf{KDC} &: ID(\mathcal{A}) \parallel ID(\mathcal{B}) \parallel N_1 \\
\mathsf{KDC} \to \mathcal{A} &: E(k_{\mathcal{A}}, k \parallel ID(\mathcal{B}) \parallel N_1 \parallel E(k_{\mathcal{B}}, k \parallel ID(\mathcal{A}))) \\
\mathcal{A} \to \mathcal{B} &: E(k_{\mathcal{B}}, k \parallel ID(\mathcal{A}))
\end{aligned}
\tag{1.10}
$$

$\mathcal{A}$		$\mathcal{E}$		$\mathcal{B}$
choose p, g	$\longrightarrow$	p, g	$\longrightarrow$	p, g
choose a				
$A := g^a \mod p$	$\longrightarrow$	A		
		choose e_1		
		$A := g^{e_1} \mod p$	$\longrightarrow$	A
				choose b
		B	$\longleftarrow$	$B := g^b \mod p$
		choose e_2		
B	$\longleftarrow$	$B := g^{e_2} \mod p$		
$k_2 := B^a \mod p$				$k_1 := A^b \mod p$

Figure 1.2: Man in the Middle Attack in Diffie-Hellman Key Exchange

1.2.2 Kerberos Protocol

커버러스는 제 3의 신뢰된 인증서버를 통해 개방된 분산 환경에 존재하는 사용자간의 인증과 세션키 교환을 지원하는 인증 서비스이다.

임의의 클라이언트 $\mathcal{C}$가 서버 $\mathcal{S}$에 접속하기 위해서는, 자격이 없는 클라이언트 $\mathcal{C}'$가 신분 위장 후 $\mathcal{S}$에 접속하는 시도를 막기위해 인증을 시도해야한다.

기호를 다음과 같이 정리한다.

- $\mathcal{C}$: 클라이언트(사용자)
- $\mathcal{S}$: 어플리케이션 서버
- $\mathcal{S}_{auth}$: 인증 서버
- ID_x: x에 대한 식별자
- P_x: x가 사용하는 패스워드
- AD_x: x의 네트워크 주소
- $k_{x,y}$: x와 y가 공유하는 비밀키

초기 커버러스 1. 패스워드가 평문 2. 재전송공격 3. 다른 서버에 인증하기 위해서는 티켓을 다시 받아야함. 4. 일방향 인증

TGS를 이용한 커버러스 1. 티켓의 유효기간에 따른 트레이드오프 2. 일방향 인증

1.2.3 Kerberos Protocol V4

롱텀 키: 계속 쓰는 키. 세션 키: 잠깐 쓰고 버리는 키.

C는 AS를 신뢰할 수 있음. Kc는 C하고 AS만 공유하는 데, 평문에 IDtgs 로 인증하면서, TS2로 재전송 공격도 막으므로 신뢰 가능함.

Chapter 2

해석학 및 응용

2.1 Axiom of Real Number

실수 $\mathbb{R}$는 체의 공리 2.1.1, 순서의 공리, 완비성의 공리 세 가지를 따른다.

Axiom of Field

실수의 체 공리를 설명 하기 전에, 체(field)에 대해 먼저 정의한다.

Definition 2.1.1. 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.

다음은 실수의 체 공리이다.

Axiom 2.1.1. $\mathbb{R}$은 체이다.

Axiom of Order

Axiom 2.1.2. Let P be a nonempty subset of $\mathbb{R}$ which we define as the set of positive real numbers. Then P have following axioms:

- Axiom 1. If $a, b \in P$, then $a + b \in P$.
- Axiom 2. If $a, b \in P$, then $a \cdot b \in P$.
- Axiom 3. If $a \in \mathbb{R}$ then only one of the following holds: $a \in P$ or $-a \in P$ or $a = 0$.

Property 2.1.1. Let P be a nonempty subset of $\mathbb{R}$ which we define as the set of positive real numbers. Then P have following properties:

- $\forall a, b, c \in \mathbb{R}$, exactly one of $a < b$, $a = b$ and $a > b$ is true. 순서가 있으니 $<, >, =, \geq, \leq$ 등을 사용할 수 있음.
- $\forall a, b, c \in \mathbb{R}$, if $a < b$ and $b < c$ then $a < c$.
- $\forall a, b \in \mathbb{R}$, if $a \leq b$ and $a \geq b$ then $a = b$.
- $\forall a, b, c \in \mathbb{R}$, if $a < b$ then $a + c < b + c$.
- $\forall a, b, c \in \mathbb{R}$, if $a < b$ and $c > 0$ then $ac < bc$.

Axiom of Completeness

이 장에서 항상 X는 $\mathbb{R}$의 공집합이 아닌 부분 집합이라 하자. 완비성의 공리를 설명하기 전에, 유계, 상계 그리고 상한에 대해 정의한다.

Definition 2.1.2. 모든 $x \in X$에 대하여, $a \geq x$를 만족하는 $a \in \mathbb{R}$가 존재 할 때, X를 위로 유계(bounded above)라 하고, a를 X의 상계(upper bound)이라 한다.

Definition 2.1.3. a가 X의 상계이고 모든 X의 상계 a'에 대해 $a \leq a'$라면, a를 X의 상한(supremum or least upper bound)이라 한다. 기호로는 $\sup X$로 나타낸다.

완비성의 공리는 다음과 같다.

Axiom 2.1.3 (Completeness)**.** X가 위로 유계일 때, $\sup X$는 존재하며, 유일하다. (유일하다는 공리가 아닐수도.)

?

Proposition 2.1.1. X가 위로 유계이고, a가 X의 상계일 때, $a = \sup X$라면, 모든 $\varepsilon < 0$에 대해 $a - \varepsilon < x \leq a$를 만족하는 $x \in X$가 존재하며, 그 역도 성립한다.

Proof. ($\Rightarrow$) 여기서는 대우 명제를 증명한다. 모든 $\varepsilon < 0$에 대해 $a - \varepsilon < x \leq a$를 만족하는 x가 존재하지 않는다고 가정하자. 이는 즉 모든 x에 대해 $a - \varepsilon < x$를 만족하므로, $a - \varepsilon$은 X의 상계가 된다. $a - \varepsilon < a$이기 때문에 a는 $\sup X$가 아니다.
($\Leftarrow$) 모든 $\varepsilon < 0$에 대해 $a - \varepsilon < x \leq a$인 x가 존재하므로 $a - \varepsilon$은 상계가 아니다. 이는 a보다 작은 모든 실수가 상계가 아니라는 뜻이므로, a는 상한이다. $\square$

$\sup X = \infty$라면, X는 위로 유계가 아니다.
$X = \emptyset$이면, $\sup = -\infty$. $\forall r \in \mathbb{R}$, $x \in X \implies x \leq r$이다.(p이면 q이다 에서 p가 거짓이면, 이 조건문은 무조건 참).

Definition 2.1.4. X가 위로 유계가 아니면, $\sup X = \infty$이라 한다. X가 아래로 유계가 아니면 $\inf X = -\infty$이라 한다.

실수 $\mathbb{R}$은 위로 유계도, 아래로 유계도 아니다.
아르키메데스의 성질

Theorem 2.1.1. 모든 $a, b \in \mathbb{R}, a > 0$에 대하여, $na > b$이 성립 되는 적당한 $n \in \mathbb{N}$가 존재한다.

Proof. (역이 모순이라는 것을 증명) 모든 자연수 n가 $na \leq b$를 만족하는 $a > 0$이 존재한다고 가정하자. b는 $A = \{na : n \in \mathbb{N}\}$의 상계이고, A는 위로 유계이다. 완비성의 공리에 의해, $\sup A$는 존재한다. 즉 $(n+1) \cdot a \leq \sup A$를 만족한다. 이는 $na < \sup A - a$이므로, $\sup A - a$는 A의 상계이다. 상한의 정의에 의해, $a \leq 0$이므로,
정리 2.1.1에 의해, 모든 $\varepsilon > 0$에 대해 $\sup A - \varepsilon < n \leq \sup A$를 만족하는 n이 존재한다. $\square$

이를 통해 알 수 있는 것. $0 < a < b$에 대해 $na > b$이 성립하는 n이 존재한다. a가 아무리 작고 b가 아무리 커도, a를 계속 더하면 b를 넘을 수 있음.
자연수 집합 $\mathbb{N}$은 실수 $\mathbb{R}$에서 위로 유계가 아니다.

Exercises

Exercise 1:
모든 $n \geq 4$에 대해, $n! > 2^n$임을 보여라.

Solution 1:

수학적 귀납법으로 보인다. $4! = 24 > 2^4$이므로 $n = 4$일 때 성립. $k > 4$에 대하여, $k! > 2^k$가 성립한다고 가정하자. 그러면 $(k+1)! > 2^k \cdot (k+1) > 2^k \cdot 2 > 2^(k+1)$이므로 증명은 완성된다.

Exercise 2:

Solution 2:
$A_2 = A_2^o and A_2^e$이다. $\sup A_2^o = \frac{1}{2}$ $\inf A_2^e = -\frac{1}{2}$ 뭐 대충 이느낌.

Exercise 3:
$A = (-\infty, 3) and (4, 5]$에서의 상한과 하한을 구해라.

Solution 3:
$\sup A = 5, \inf A = -\infty$

Exercise 4:
$a, b \in \mathbb{R}$이라 하자. 임의의 ε에 대하여, $|a - b| < \varepsilon$이면, $a = b$임을 보여라.

Solution 4:
$A = \{\varepsilon \in \mathbb{R} : \varepsilon > 0\}$이라 하자. $A = (0, \infty)$이다. $|a - b|$는 A의 하계이다. A는 아래로 유계이다. 완비성의 공리에 의해, $\inf A$가 유일하게 존재한다. $\inf A \geq |a - b|$이다. $\inf A = 0$이다. $|a - b| \geq 0$이므로, $|a - b| = 0$이다.

Exercise 5:
(베르누이 부등식)$x > -1$이면 모든 자연수 n에 대하여 $(1 + x)^n \geq 1 + nx$임을 보여라.

Solution 5:
PMI(?) $(1 + x)^1 = 1 + x \geq 1 + 1x$이므로 성립. $(1 + x)^k \geq 1 + kx$가 성립한다고 가정하자. $(1 + x)^(k + 1) = (1 + x)^k \cdot (1 + x) \geq (1 + kx) \cdot (1 + x) = 1 + kx + x + kx^2 \geq 1 + kx + x = 1 + (k + 1)x$가 성립하므로 증명은 완성된다.

2.2 Sequence

Definition 2.2.1. We call l the **limit** of the sequence $\{x_n\}$, which is written $x_n \to l$, if the following condition holds: For each real number $\varepsilon > 0$, there exists a natural number N such that, for every natural number $n \geq N$, we have $|x_n - l| < \varepsilon$. The sequence $\{x_n\}$ is said to **converge** to the limit l.

Theorem 2.2.1. If the limit of a sequence exists then it is unique.

Proof. Let l_1, l_2 are limit of the sequence $\{x_n\}$. Then we have

$$\begin{aligned} \forall \varepsilon > 0, \exists N_1 : \forall n \geq N_1, |x_n - l_1| < \frac{\varepsilon}{2} \\ \forall \varepsilon > 0, \exists N_2 : \forall n \geq N_2, |x_n - l_1| < \frac{\varepsilon}{2}. \end{aligned} \tag{2.1}$$

Let $N = \max(N_1, N_2)$. Then we have

$$\begin{aligned} \forall n \geq N, |x_n - l_1| < \frac{\varepsilon}{2} \\ \forall n \geq N, |x_n - l_2| < \frac{\varepsilon}{2}. \end{aligned} \tag{2.2}$$

Now we completes the proof by following.

$$|l_1 - l_2| = |l_1 - x_n + x_n - l_2| \leq |x_n - l_1| + |x_n - l_2| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \tag{2.3}$$

□

Theorem 2.2.2. If the limit of a sequence exists then the sequence is bounded.

Proof. Let l_1 is limit of the sequence $\{x_n\}$. Then we have

$$\forall \varepsilon > 0, \exists N : \forall n \geq N, |x_n - l| < \varepsilon. \tag{2.4}$$

It follows that

$$|x_n| = |x_n - l + l| \leq |x_n - l| + |l| < \varepsilon + |l|\,. \tag{2.5}$$

Let $M = \max(x_1, \cdots, x_{N-1})$. Then we completes the proof by following.

$$\forall n, x_n \leq \max(M, \varepsilon + |l|). \tag{2.6}$$

□

Theorem 2.2.3 (Squeeze theorem)**.** Let $x_n \to l, y_n \to l$. Then

$$\forall n, x_n \leq z_n \leq y_n \implies z_n \to l. \tag{2.7}$$

Proof. Since $x_n \to l, y_n \to l$, we have

$$\begin{aligned} \forall \varepsilon > 0, \exists N_x : \forall n \geq N_x, -\varepsilon < x_n - l < \varepsilon \\ \forall \varepsilon > 0, \exists N_y : \forall n \geq N_y, -\varepsilon < y_n - l < \varepsilon. \end{aligned} \tag{2.8}$$

Let $N = \max(N_x, N_y)$. since $x_n \leq z_n \leq y_n$, we completes the proof by following

$$\forall \varepsilon > 0, n \geq N, -\varepsilon < x_n - l \leq z_n - l \leq y_n - l < \varepsilon. \tag{2.9}$$

□

2.2.1 Monotone Sequences

Definition 2.2.2. the sequence $\{x_n\}$ is **monotone increasing sequence** if $\forall n, x_n \leq x_{n+1}$.

Lemma 2.2.1. If a sequence is increasing and bounded above, then its supremum is the limit.

Proof. Let $x := \sup\{x_n\}$. □

Lemma 2.2.2. If a sequence is decreasing and bounded below, then its infimum is the limit.

Proof. □

Theorem 2.2.4 (Monotone convergence theorem, MCT)**.** If a sequence is bounded and monotone, then it converges.

Proof. □

2.2.2 Subsequences

Definition 2.2.3. $\{x_{n_k}\}$ is a **subsequence** of $\{x_n\}$ if $\{n_k\}$ is increasing sequence.

Theorem 2.2.5. If a sequence $\{x_n\}$ has a limit l then all subsequence $\{x_{n_k}\}$ of $\{x_n\}$ also have a limit l.

Proof. It is clear that $n_1 \geq 1$. Suppose that $n_k \geq k$. Since n_k is increasing sequence, we have $n_{k+1} > n_k \geq k$. It follows that $n_{k+1} \geq k+1$ and we have

$$n_k \geq k. \tag{2.10}$$

Let $x_n \to l$. We completes the proof by following.

$$\forall \varepsilon > 0, \exists k : \forall n_k \geq k, |x_{n_k} - l| < \varepsilon. \tag{2.11}$$

□

2.2.3 Nested Sequences

Definition 2.2.4. Let $I_n = [a_n, b_n]$, where $|I_n| = b_n - a_n$ denotes the **length** of such an interval. One can call I_n a sequence of nested intervals, if

$$\forall n, I_{n+1} < I_n, \tag{2.12}$$

Theorem 2.2.6 (Nested intervals theorem)**.** Let $I_n = [a_n, b_n]$ is nested. If $(b_n - a_n) \to 0$, then $\exists! x \in \mathbb{R}$ such that $x \in I_n$.

Proof. First we prove existence. Note that a_n is bounded. By MCT, $a_n \to \sup A$. Let $x = \sup A$. Since b_n is upper bound, $a_n \leq x \leq b_n$. then $x \in I_n$. Now we prove uniqueness. Assume that $y \in I_n$. then $a_n \leq y \leq b_n$. It follows that $0 \leq y - a_n \leq b_n - a_n$. By squeeze theorem, $y - a_n \to 0$. It follows that $a_n \to y = x$. □

Theorem 2.2.7 (Bolzano-Weierstrass theorem)**.** bounded sequence has a convergent subsequence.

Proof. Let $\{x_n\}$ is a bounded sequence. Then we have

$$\forall n, \exists M > 0 : -M \leq x_n \leq M. \tag{2.13}$$

Let $I_1 = [0, M], I_n = [\frac{(2^n-1)M}{2^n}, M]$. Since $\forall k, I_k \supset I_{k+1}$, I_n is nested. By nested intervals theorem, $|x_{n_k} - x| < \frac{M}{2^{n-1}}$. □

2.2.4 Cauchy Sequences

Definition 2.2.5. a sequence $\{x_n\}$ is **Cauchy sequence** if

$$\forall \varepsilon > 0, \exists N : \forall m > n \geq N, |x_m - x_n| < \varepsilon. \tag{2.14}$$

Theorem 2.2.8. if a sequence converges, then it is cauchy sequence.

Proof. Let $x_n \to l$. Then

$$\begin{aligned} \forall \varepsilon > 0, \exists N : \forall n \geq N, |x_n - l| < \frac{\varepsilon}{2}, \\ \forall \varepsilon > 0, \exists N : \forall m \geq N, |x_n - l| < \frac{\varepsilon}{2}. \end{aligned} \tag{2.15}$$

Let $m > n$. Then

$$|x_m - x_n| = |x_m - l + l - x_n| \geq |x_m - l| + |x_n - l| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2}. \tag{2.16}$$

□

Theorem 2.2.9. A cauthy sequence is bounded.

Proof. Let x_n is a cauchy sequence. Then

$$\exists N : \forall m > n \geq N, |x_m - x_n| < 1. \tag{2.17}$$

Let $n < N$. Then

$$|x_n| < \max(|x_1|, \cdots, |x_{N-1}|). \tag{2.18}$$

Let $n \geq N$. Then

$$|x_n| = |x_n - x_N + x_N| \leq |x_n - x_N| + |x_N| < 1 + |x_N|. \tag{2.19}$$

Let $M = \max(|x_1|, \cdots, |x_{N-1}, 1 - |x_N||)$. Then $\exists M : |x_n| \geq M$. This completes the proof. □

Theorem 2.2.10 (Cauchy's convergence test)**.** A sequence converges if and only if it is cauchy sequence.

Proof. We claim that $x_{n_k} \to l \implies x_n \to l$.
Let $\{x_n\}$ is a cauchy sequence and $\{x_{n_k}\}$ is a subsequence of $\{x_n\}$. Then

$$\begin{aligned} \forall \varepsilon > 0, \exists N_1 : \forall m > n \geq N_1, |x_m - x_n| < \frac{\varepsilon}{2} \\ \forall \varepsilon > 0, \exists N_2 : \forall n_k > k \geq N_2, |x_{n_k} - l| < \frac{\varepsilon}{2}. \end{aligned} \tag{2.20}$$

Let $N = \max(N_1, N_2)$. Then we completes the proof by following:

$$|x_n - l| = |x_n - x_{n_k} + x_{n_k} - l| \leq |x_n - x_{n_k}| + |x_{n_k} - l| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \tag{2.21}$$

□

2.2.5 Abstract

Figure 2.1: Relations of theorem about sequence

2.2.6 Exercise

$x_1 = 2$, $x_{n+1} = (2x_n + 3)/(x_n + 2)$.

Proof. Claim: $x_{n+1} - (2x_n + 3)/(x_n + 2) > 0$.

$x_1 = 2$, $x_{n+1} = (2x_n + 3)/(x_n + 2) = x_n^2 - 3/x_n + 2$.

Claim: $x_n^2 > 3$.

using induction.

$x_1^2 = 4 > 3$.

Assume that $x_k^2 > 3$.

$x_{k+1}^2 - 3 = (2x_k + 3/x_k + 2)^2 - 3 = x_k^2 - 3/(x_k + 2)^2 > 0$.

$x_n > x_{n+1}$ and $x_n > \sqrt{3}$.

By MCT, x_n has a limit. Let $x_n \to x$.

$x_{n+1} \to 2x + 3/x + 2 \implies x = \sqrt{3}$. □

Chapter 3

리더십챌린지

리더와 팔로워.

중간 30 기말 30 과제 10 출석 20 수업참여 10(기본 7 + 플러스 요인 3(일대일 코칭 참가 등))

리더 vs 관리자. 리더. 가장 중요하게 해야 할 일이 무엇인지에 대한 합의를 이끌어 내는데 초점. 관리자. 구성원들의 성과를 향상시키는데 초점.

리더십과 성과의 관계.

성과를 높이는 것: 생산성, 결근/이직, 일탈적 직장행동(¡-¿)조직시민행동, 조직몰입(여기서 일하고 싶어) 등등 -¿ 이것들을 높이는(혹은 낮추는) 원인? = 사원의 태도/행동 (¡-¿) 리더의 태도/행동 -¿ 리터의 특성/기술이 좋아야함.

리더십을 어떤 관점으로 분석할까? 특성(내면, 타고난 재능), 행동(나타나는 행동), 권력-영향력(행동이 미치는 영향력, 사원 간의 관계), 상황(주변 환경이 리더를 만든다.), 통합(전부 다 ㅋ)

3.1 리더십의 정의

리더십의 정의는 합의된 것이 없다. 그래도 말하자면, 리더십이란 다음 중 하나로 정의할 수 있다. 보통 리더십에서 목표달성과 영향력은 리더십의 정의에 인정한다.

- 목표달성을 위한 활동에 영향을 미치는 과정.
- 다른 사람들에 의해서 리더라고 인정받는 과정.
- 영향력 행사 과정
- 변화를 촉발하는 능력.

연도별 리더십: 리더와 팔로워 사잉에서 일어나는 현상에서, 관계나 행동의 패턴의 흐름. 수평적이고 민주적으로 바뀌어감.

공식적 리더, 비공식적 리더. -¿공적으로 리더의 역할을 받았는가? 비공식적 리더는 뭔데?

직접적 리더, 간접적 리더 -¿ 직접적: 회사 상사, 교수, 동아리 회장 등. 간접적: 존경하는 사람?, 저명한 학자, 시민 운동가

3.2 권력-영향력 관점에서의 리더십

대상: 집단/개인

def. 권력이란? 대상A이 다른 대상B의 행동에 영향을 미치기 위해 가지고 있어야 하는 능력.

def. 의존성이란? B가 필요로 하는 것이 A가 소유하고 있을 경우. A에 대한 B의 관계. B의 의존성이 커질 수록, A는 더 큰 권력을 얻음.

공식적 권력. -¿ 지위에 의해 형성. 1. 보성을 줄 수 있기에 생기는 권력. 2. 벌을 줄 수 있기에 생기는 권력. 3. 규정, 근거에 의해 생기는 권력. (?)

개인적 권력. -¿ 개인의 매력, 특성에 생김 1. 전문성이 뛰어나서 생김. 막 뭔가 배우고 싶을 때. 2. 인간적 매력에서 생겨남. (준거적 권력)

권력을 행사하기 위한 행동 패턴은 여러가지가 있다. 이중 가장 효과 높은 세 가지는 다음과 같다. 참고로 압력에 의한 권력행사는 효과가 낮다. 1. 이성적 설득. 2. 대상의 감정적 몰입을 이끌어 냄. 대상의 가치에 호소. 3. 대상이 의사결정에 참여시키도록 함.

부드러운 전술을 먼저 사용하는 것이 효과적임. 정치적 기술(사람 간의 커뮤니티 형성 비슷한 거)이 권력 전술의 성패를 결정함. 조직의 문화에 따라 선택하는 권력 전술이 달라짐.

대표적인 영향력 발생과정 1. 수단에 의한 복종 : 보상 혹은 처벌 때문에 행동을 따름. 2. 내면화 : 주어진 제안이 자신의 가치와 신념에 빗대어 볼 때 옳다고 생각하고 행동을 따름. 3. 개인적 동일시 : 존경에 의한 행동 모방.

영향력 행사의 결과 1. 몰입 : 제안을 효과적으로 실행하기 위해 노력함. 2. 복종 : 제안을 응하지만 열성적이진 않음. 최소한의 노력만 함. 3. 저항 : 제안을 응하지 않음. 뭐, 딱봐도 1 ¿ 2 ¿ 3번이죠 성과의 크기가.

리더의 권력 -a- 리더의 영향력 행사 -b- 행사의 결과 -c- 리더의 권력 a: 권력에 따른 행동의 차이 b: 권력과 행동이 미치는 결과 c: 권력에 따른 태도

적절한 권력 전술을 선택하고 행사. 지위에 의존하지말고 전문가, 준거적 권력을 개발.

Chapter 4

삶과 윤리

수업참여 10점: 자기소개 및 수업신청 이유 등 한글 워드 1장, 사진 전화번호 등도 첨부.

중간 30점 - 3페이지 글자크기 10 줄간격 160 자유로운 에세이 표절 gpt 금지. 기말 40점 - 4페이지

이름 학과 수업신청 이유 칼라 추출. 토론결과 발표. 한 팀.

조장 30초. 스트레칭?.

4.1 윤리학의 핵심 주제들

- 공리주의: 전체의 효율성을 강조. 정의를 사회 전체의 행복을 극대화하는 데에서 찾는다.
- 자유주의: (자유지상주의(강경한 자유주의)) 개인의 선택의 자율 보장하는 것을 최우선으로 여김. 권리 ¿ 선.
- 칸트주의: 엄격한 자유주의. 도덕 = 정언 명령에 따른 자유로운 행동. 자유 아래 의무를 인식하고 행동해야 함.
- 평등자유주의: 기본적 자유는 침해하지 않는 선에서 평등원칙과 차등원칙을 강조. 자유주의에서 사회주의를 약간 가져옴.
- 미덕주의: 공동체의 미덕을 구현한 사람에게 권력을 주는 것이 정의. 공동선의 본질을 파악한 사람에게 최곡 공직과 영예가 돌아가야 함.

트롤리 문제: 윤리적 딜레마 플라톤의 동굴: 우리가 알고 있는게 정말 맞는 것인가?

확정 편향하는 이유는 체력적으로 편하게 하기 위함.

토론 주제: 동굴 밖에 나온 사람은 동굴 안의 사람을 계몽시켜야 한다. 그것이 철학자가 할 일이다. 이것에 대해 어떻게 생각하는가?

4.2 윤리적 딜레마

Exercise 6:

임수 수행을 위해 목표 지점에 미사일을 발사하려고 하는데, 목표 지점 근처에 어린 아이가 있다. 만약 당신이라면 어떻게 할 것인가? 그리고 그렇게 생각한 이유는 무엇인가?

Solution 6:

이윤기: (바로 쏘는)쏜다. 이유: 대를 위한 소의 희생. -¿ 반박: 대가 어느 쪽인지 알 수 없다. 민간인을 죽인게 여론 상 불리할 수 있다. 최이안: 기회를 주고, 실패 직전에 쏜다. 이유: 조금 기다린다고 하더라도 바로 실패하지 않는다. -¿ 반박: 기회를 준다는 게 실패로 이어질 수 있다. 쉽지 않음. 김재학: 쏜다. 이유: 테러리스트들이 어떤 사람들을 죽일지 모른다. 빨리 죽이는 게 맞다. -¿ 반박: 대가 어느 쪽인지 알 수 없다. 민간인을 죽인게 여론 상 불리할 수 있다. 김용우: 기회 주고 쏜다. 주요 목적이 테러리스트 죽이는 것. 윤리적 문제 고려할 때 기다리고 쏜다.

김동현: 안쏜다. 이유: 지금 안쏘더라도 기회는 온다. 굳이 민간인이 피해를 입는 상황에서 쏠 필요가 없다. -¿ 반박: 기회가 언제 올 지 모른다. 기회가 오기 전에 죽을 수 있음.

Exercise 7:

민간인을 어떻게 할까? 1. 놔두고 올라가는 것(실제로 선택함). 2. 묶고 운에 맡기는 것. 3. 죽이는 것.

Solution 7:

김동현: 3. 죽인다. 민간인이 아닐 수 있음. 놔뒀을 때 임무가 실패할 확률이 높다. 김용우: 3. 죽인다. 신원확인이 안됨. 놔뒀을 때 임무가 실패할 확률이 높다. -¿ 반박: 민간인일 수 있다. 라는 점이 문제가 된다. 죽인다고 해서 임무가 성공할 수 있나? 죽인다고 임무 성공 보장이 없다. 최이안: 2, 3: 첫 번째랑 다른점: 지금 상황은 잘못되면 우리가 죽는다. 안죽는 상황을 만든다. -¿ 반박: 민간인일 수 있다. 라는 점이 문제가 된다. 죽인다고 해서 임무가 성공할 수 있나? 죽인다고 임무 성공 보장이 없다. 김재학: 2: 묶어둔다. 이유: 직접 죽이는 건 죄책감이 든다. 임무는 성공해야 함. 임무가 성공을 한다면 굳이 죽일 이유가 없다. -¿ 반박: 결과가 달라지지 않는다. 리스크는 있음. 어중간한 느낌이다. 이윤기: 3: 죽인다. 이유: 불안하다. 살아있으면, 신경쓰여서 임무에 집중이 안될 수 있다. -¿ 반박: 죽여도 죄책감에 집중이 안될 수 있다.

4.3 공리주의, Utilitarianism

공리주의적으로 생각할 때 총 합이 최대의 효율을 내야 함.

피자 5조각과 아이 5명. 피자에 대한 쾌락의 양이 다르다.

[이름] [1조각에 대한 쾌락] [2조각에 대한 쾌락] 이승우 11 2 이미영 9 6 한송희 4 1 김덕룡 7 3 박서현 10 5

공리주의적으로 볼 때, 송희는 안주고 미영이에게 2조각을 준다. 나머지는 1조각씩 준다.

공리적이려면, 일단 합리적, 이타적이어야 한다. 그래야 작동한다.

[유죄인가? 무죄인가? 유죄라면 얼만큼?] 시신을 버리지 않으면 우리는 살 수 있다. 제비뽑고 죽을 사람을 선택.

김동현: 무죄: 정당방위, 어쩔 수 없음. 이윤기: 무죄: 죄를 따질 문제가 아니다? 김재학: 무죄: 동의 하에 죽었으니 이건 자연사다. 최이안: 유죄: 서로가 어쩔 수 없는 동등한 상황이었어. 그래서 당위성을 부여할 수 없다.

공리주의의 이익/쾌락 원리 감정에는 쾌락과 고통 2가지가 있다. (모든 욕구를 쾌락과 고통으로 치환 가능하다.)

공리주의는 생명을 돈으로 환산가능ㅎ마. 거부감은 극복해야 할 충동적 감정임.

4.3.1 존 스튜어트 밀

존 스튜어트 밀은 공리주의 원칙에 인간적인 접근을 시도했다. 밀은 경험주의 인식론, 공리주의 윤리학을 가진 자유주의자. 자유주의적 정치경제 사상을 가족 있었으나, 사회주의적 요소도 일부 가지고 있다. 공리주의에 공상적 사회주의와 낭만주의를 가미했다. 밀은 자유를 포기하지도, 타인의 자유를 침해하지도 않았던 자유주의자.

밀은 양뿐만 아니라 질적 쾌락도 고려해야 한다고 한다. 쾌락과 고통이 전부이나, 더 가치있는 쾌락이 존재한다고 주장 배부른 돼지와 배고픈 소크라테스. ?

무엇이 더 나은 쾌락인가? 1. 세계격투기, 2. 셰익스피어 햄릿, 3. 사망토론 햄릿이 가장 고급스러운 쾌락이다. 이유는 영혼의 고급능력을 이끌어내기 때문이다.

질적으로 다른 쾌락이 존재한다. 아니다.

김용우: 아니다. 이유: 질적 쾌락의 기준이 애매하다. 최이안: 존재한다. 이유: 운동의 쾌락, 누워서 보는 쾌락은 질이 더 낮다. 김재학: 존재하고. 이유: 지속가능한 쾌락이 질적으로 나은 쾌락이다. 김동현: 아니다. 이유: 질적 쾌락과 양적 쾌락을 나눌 수 없다.

테러리스트를 고문해서 핵을 멈춰야 하는가?

최이안: 테러리스트까지는 고문 가능. 행동에 대한 대가를 치루고 있는거니까. 근데 주변인들까지? 이건 또 다른 문제다. 책임의 무게에 따라 선택할 수 있다. 김재학: 전부 고문함. 많은 사람들을 살리는 것이 가장 중요하다. 김용우: 테러리스트까지는 고문 가능. 행동에 대한 대가를 치루고 있는거니까. 근데 주변인들까지? 이건 또 다른 문제다. 김동현: 전부 고문함. 많은 사람들을 살리는 것이 가장 중요하다.

4.4 자유주의

자유주의는 온정주의, 도덕법제화, 소득과 부의 재분배를 거부한다. 개인의 신체나 목숨에 간섭하는 법에 반대하고, 제도나 법을 통한 미덕을 강조하는 것을 반대하고, 과도한 세금 징수를 거부한다.

최해갑 가족의 행위는 자유를 향한 투쟁의 과정인가? 아니면 공동체로부터 이탈하고자 하는 윤리적 행위인가?

- 이윤기: 반 윤리적 행위: 국가가 그 사람에게 주는 혜택이 있는데, 그만큼 의무를 다해야 한다. 의무를 다하지 않고 있는 것이다.
- 김용우: 반 윤리적 행위: 이유가 있어서 철거는 하는건데, 공동체적으로 볼 때, 평화와 질서를 위한 일인데 자기만을 위해서 하는 건 반 윤리적 행위이다.
- 김재학: 자유를 행한 투쟁: 남한테 피해를 주지 않았다. 그냥 내가 여기에 살고 있는 것 뿐이다.
- 최이안: 반 윤리적 행위: 국가가 그 사람에게 주는 혜택이 있는데, 그만큼 의무를 다해야 한다. 의무를 다하지 않고 있는 것이다.
- 김동현: 반 윤리적 행위: 비도덕적인 것 같다. 남들 다하는데 나만 안하면 이건 남한테 피해를 주는 것 같다.

하이에크에 따르면, 인간의 이성은 불완전하며, 이러한 무지야말로 인간에게 자유가 필요한 근거이다. 구성주의적 합리주의는 이성의 힘을 과신하여, 자유를 파괴하는 오류를 범했다.

Chapter 5

인문학 리더십

ttakala@hanmail.net

과제 3개

출석 20점 자기소개 10점 중간고사 30점 - 한글 워드 기준 3장 줄간격 글자크기 160과 10 ”자유로운” 에세이. 챗gpt금지. 기말고사 40점 - 한글 워드 기준 4장 제출은 pdf로

10점짜리 자기소개 - 한글 워드 기준 1장 채우기. 글자 10pt 줄간격 160

사진, 전화번호, 수업 신청 배경 (사진 포함 1장임.)

조장이 하는 일. 조원소개서, 토론 10분 - 조장 중심 발표.

조원소개서: 이름, 학과, 수업 신청 배경

5.1 2주차

메데이아 리더십, 스파르타쿠스 리더십

5.1.1 메데이아

그리스인 이아손(이올코스의 왕 아이손의 아들). 콜키스에 금이 많아 식민지를 건설하려 함. -¿ 원정대 여정

펠리아스가 이아손 죽이려고 콜키스 황금모피를 가져오라함. (왕위를 물려주기 싫었음.)

콜키스 왕 아이에테스에 보물(황금모피)을 달라고 함. -¿ 미친놈인가? -¿ 불을 뿜는 황소를 사용해서 밭을 갈라고 함. + 용의 이빨을 뿌리라고 함.(백골의 용사가 나옴 ㄷ)

이 때 메데이아는 이아손에게 연고를 줌(불 방지) + 백골용사를 막는 부적 줌. 용을 제거(혹은 재우고)하고 황금모피 이아손한테 줌. + 결혼 약속.

모피 가져왔지만 왕위 안줌. -¿ 메데이아 빡침 -¿ 펠리아스 죽이고 코린토스로 쫓겨남.

코린토스 왕 크레온. -¿ 메데이아와 이혼하면 왕위를 주겠다 함. -¿ 메데이아를 칼같이 배신.

결국 이아손과 크레우사가 결혼, 메데이아는 개빡침

복수 시작. 왕(크레온)과 아내(크레우사, 크레온 딸)를 불 붙는 드레스로 죽임. 자신의 아들 2명(이아손의 아들이므로)를 칼로 죽임.

메데이아는 이아손을 조롱하며 떠남.

5.1.2 스파르타쿠스

스파르타쿠스: 트라키아 출신.

5.2 3주차

수업목표: 목표지향적 리더십.

코카서스 3국 역사.

해시오도스 해석, 아이스킬로스 해석 2개.

5.2.1 코카서스

조지아. 흑해 옆. 최초 포도주 생산 지역으로 알려져 있음. 카즈베기산 아르마니아인(노아의 후손), 아제르바이잔인(불의 땅 - 땅에서 가스때문에 불이 자연스럽게 나옴.)

프로메테우스는 코카서스의 바위산에서 형벌을 받음.

프로메테우스 : 티탄족과 바다요정의 후손, 티탄 신들의 심부름꾼. 능력 : 미래예지, 제작(장인), 저항(제우스에 저항)

헤시오도스의 해석(일반적인 해석): 제우스는 선, 프로메테우스는 악.

제우스를 기만(제물에 장난을 침), 인간에게 불을 줌.-이게 왜?

프로메테우스는 인간남자를 만듬. 여성은 제우스가 여자(판도라)를 만듬. - 제우스가 인간에게 내리는 벌. 둘이 결혼해서 자식을 낳음. 그것이 인류가 만들어진 이유. 판도라 속 희망도 사실 악한 것이다. -¿ 과도한 희망 = 불행

독재에 저항하고, 존엄성을 지키는 프로메테우스와 코버첸코(영화 비스트)의 공통점. 김동현: 자기 목숨보다 소중한 무언가가 있어야 하지 않을까? 자기희생정신이 있어야 한다. 이창연: 본인의 신념. -¿ 자기 희생. 존엄성이 신념이 깔려있었고, 자기의 신념에 반하는 일. 박채우: 프로메테우스 인간을 행복하게 해주기 위함. 자기행복보다는 남의 존엄성을 지켜줌. 장지연: 사회적 관습이 자신이 생각 사이에서 타협하지않고 저항하는 모습. 이진현: 저항하기 힘든 상황에서 자신만의 뚜렷한 관점과 신념이 있기에 저항할 수 있었다.

아이스킬로스 해석

제우스와 프로메테우스의 갈등 구조만 보자. 이전에는 제우스-선, 프로메테우스-악이었지만, 여기서는 프로메테우스를 선으로 본다. 제우스는 자신의 미래를 알고 싶어 프로메테우스에게 요청. 그러나 거절. 화딱지 나버림.

프로메테우스는 인간을 도왔음. 그리고 제우스의 비밀(테티스 여신을 인간과 결혼시킴. (신과 결혼하면 자신을 능가하기 때문))을 함구.

25. 고통받는 인간 여성 (고통받는 남성 신과 비슷.) 프로메테우스가 이오를 보니깐, 나중에 제우스의 부인이 되는 걸 봄. 지금은 고통받고 있지만, 미래엔 잘 될꺼야. 라며 위로해줌.

역사적 인물들의 비전 중 가장 인상 깊었던 인물. 이순신: 높은 관료들이 고문을 줌. 배도 불태워지고, 그 상황속에서 중꺽마. 이순신은 억까를 당하는 상황속에서도 나라를 지키겠다는 비전을 가짐. 세종대왕: 글자를 알면 똑똑해져서 안된다. 그러나 글자를 만들었죠. 김유신: 삼국통일. 원래 귀족 출신이 아닌데, 삼국통일을 하겠다는 의지하나로 전쟁에 참여해서 삼국을 통일했다. 스티브 잡스: 애플 CEO, 회사가 잘돌아가려면 시스템이 잘 갖추어져야 하는데, 시스템을 구성할 때, 기준이 자기가 예외가 아닌 등의 시스템을 구성함.

5.3 컨버전스 리더십

5.3.1 헤라클레스

올림푸스 신과 기간테스의 대전쟁에서, 운명의 여신은 인간의 도움을 받으면 기간테스를 이길 것이라 예언한다. 제우스는 인간 영웅을 만들기 위해 알크메네라는 인간 여성과 관계를 맺었고, 그렇게 태어난 아이가 헤라클레스이다. 기간테스와의 전쟁 후, 헤라클레스는 헤베와 결혼한다. 헤라클레스는 알크메네와 함께 테베로 정착한다. 오르코메노스와 테베와의 전쟁 중, 헤라클레스의 큰 활약으로 테베가 승리하게 되고, 테베의 공주 메가라와 결혼한다. 헤라클레스를 싫어하던 헤라는 헤라클레스에게 광기를 일으켜 아내와 아들을 죽이게 만든다. 정신을 되찾은 헤라클레스는 자살하려 했으나, 12가지의 과업을 완수하여 속죄하라는 신탁을 받는다.

이 과업은 인간이 자연을 정복하고 통합해가는 일련의 과정으로 이해 가능하면서, 동시에 인간 내면에 감추어진 야수적 권력욕과 동물적 성욕을 제거하고, 폭력성과 예측불가능성을 잠재우고자 하는 인격 수양의 과정으로도 이해가능하다.

5.3.2 로물루스

로마 건국. 뭐 어쩌라고.

5.3.3 헤라클레스의 12과제

헤라클레스의 첫 번째 과업은 사자를 죽이는 것이다. 사자는 야수적 권력 욕망을 뜻한다. 두 번째 과업은 뱀(히드라)을 죽이는 것이다. 죽여도 계속 재생하자, 불을 붙여 재생하지 못하게 하고, 불사의 머리는 바위로 눌러 움직히지

못하게 했다. 뱀은 성적 욕망을 뜻하며, 없애더라도 다시 생기기에 욕망을 없애는 것이 아닌 억제하는 것으로 해석할 수 있다. 세 번째 과제는 암사슴을 생포하는 것이다. 암사슴은 자연변화, 농사를 뜻한다. 이는 인간이 이용해야 하는 것이기에 죽이는 것이 아닌 생포하는 것으로 과업이 되었다. 네 번째 과업인 돼지(야수성)도 생포하는 것이다.

다섯 번째 과업부터는 조금 달라지는데, 아우게이아스의 외양간을 청소하는 것이다. 아우게이아스는 약 3000 마리의 동물이 있으며, 약 30년간 청소하지 않은 외양간이다. 이는 문명의 오염을 청소하는 뜻을 담고 있다. 헤라클레스는 인근 강의 물을 끌어와 마굿간을 청소하고, 감사의 표시로 소 300마리를 선물받았다.

여섯 번째 과업은 식인 괴조, 스팀팔로스 새를 퇴치하는 것이다. 이 새는 인간이 가진 부정적 이상을 뜻한다. 헤라클레스는 징과 노래를 이용하여 식인괴조를 놀래켜 하늘로 올려보내고 활로 쏴 죽인다.

일곱, 여덟, 아홉, 열 번째 과제는 각각 크레타 황소, 디오메데스 야생마, 히폴리테 허리띠, 게리온 황소때를 생포 혹은 훔치는 것이다. 이는 각각 남쪽, 북쪽, 동쪽, 서쪽에 원정을 나가는 것을 의미하며, 그리스의 세력 확장 이야기가 반영된 것이다.

열한 번째 과제와 열두 번째 과제는 원래 열 개의 과제에서 추가된 것이다. 열한 번째 과제는 헤스페리데스의 사과를 가져오는 것이다. 이 사과는 힘과 기지를 뜻한다. 헤스페리데스의 사과는 제우스와 헤라의 결혼 증표로, 이는 용이 지키고 있다. 아틀라스는 사과를 주는 대신, 자기 대신 하늘을 떠받쳐달라는 거래를 제시했다. 헤라클래스는 이에 응하는 척하며, 사과만 가져간다.

열두 번째 과제는 하데스의 케르베로스를 생포하는 것으로, 이는 저승세계를 상징한다. 이는 그리스 영웅이 삶과 죽음의 구조에 직접 개입할 수 있다는 것을 보여준다. 헤라클레스는 완력을 사용하여 케르베로스를 지상으로 끌고온다.

토론: 스티브잡스: PPT -¿ mp3 전화 인터넷 하나로 융합해서 스마트폰 손흥민: 최근에 이강인과의 불화. 손흥민이 이를 감싸주면서 팀적으로 더 돈독해지는 사건이 있었다. 빌게이츠: 컴퓨터 기술 발전, 교육 개선, 빈곤층 해결 등 전체적으로 모든 것을 해결한 사람. 명량해전: 이순신, 위기상황에서 우리나라 병사들을 잘 이끌어나가 상황을 해결하는 것으로. 12가지의 의미에 대한 의견 –¿ 과업이라고 하지만, 이는 성장해나가는 과정. 과업을 통해 도전과 참회 속죄를 통해 깨달음을 얻는 헤라클레스의 인생은 우리의 인생과 비슷하다.

Chapter 6

Zero Trust Security

제이슨 가비스 그리고 제리 채프먼이 쓴, 제로 트러스트 보아, 기업 환경에서의 보안 운영을 참고하여 작성했다.

6.1 introduction

기술이 발전하면서, 원격 사용자가 기업 내부의 리소스에 연결이 가능하게 보안의 경계가 확장되었다. 이로 인해, 기업은 새로운 보안 모델을 적용해야 했다.