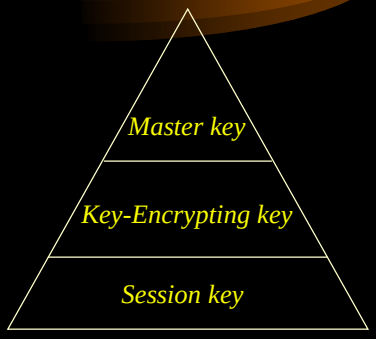
암호이론과 보안 — KEY 관리

❑ Key Management

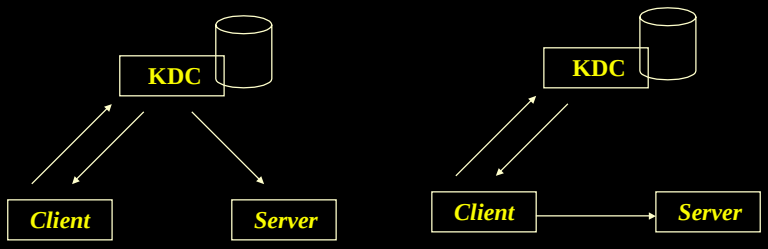
- Key Generation (생성)
- Key Distribution (분배)
- Key Update (갱신)
- Key Revocation (취소)
- Key Destruction (폐기)
- Key Installation (설치)
- Key Storage (저장)
- Key Recovery (복구)



암호이론과 보안 — KEY 분배

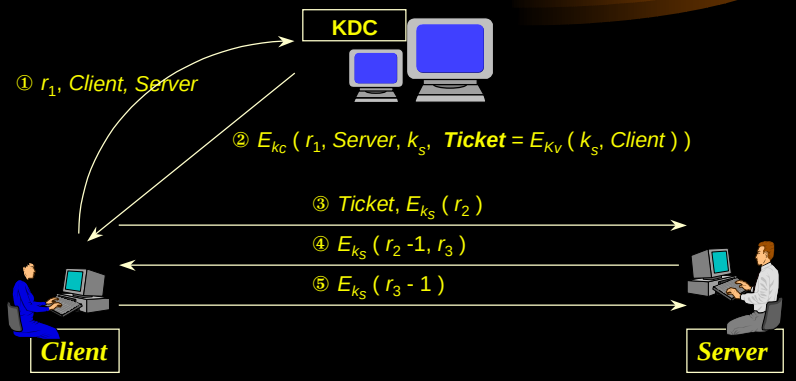
❑ 중앙 집중식 키 분배

- 키 분배 센터 (Key Distribution Center : KDC)



❑ 중앙 집중식 키 분배

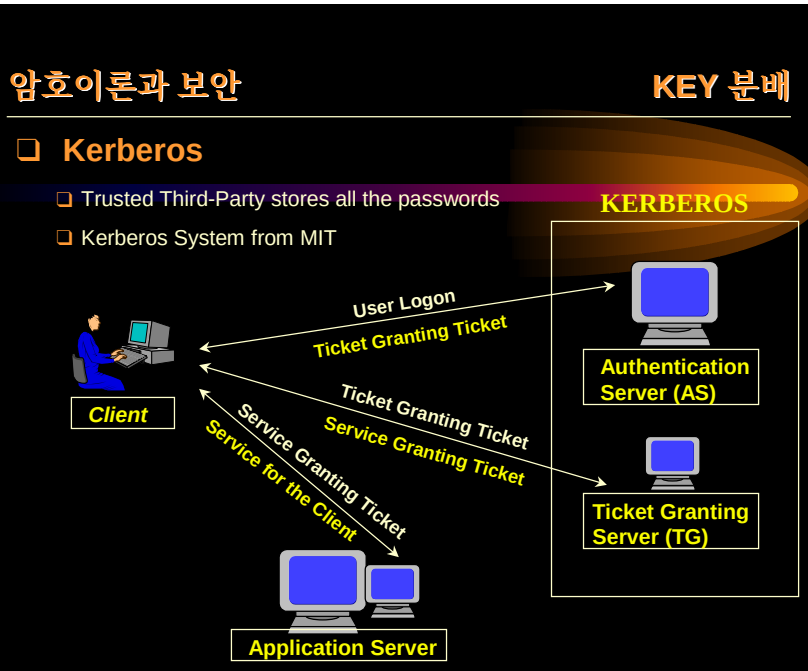
- ❑ *Needham-Schroeder* Protocol



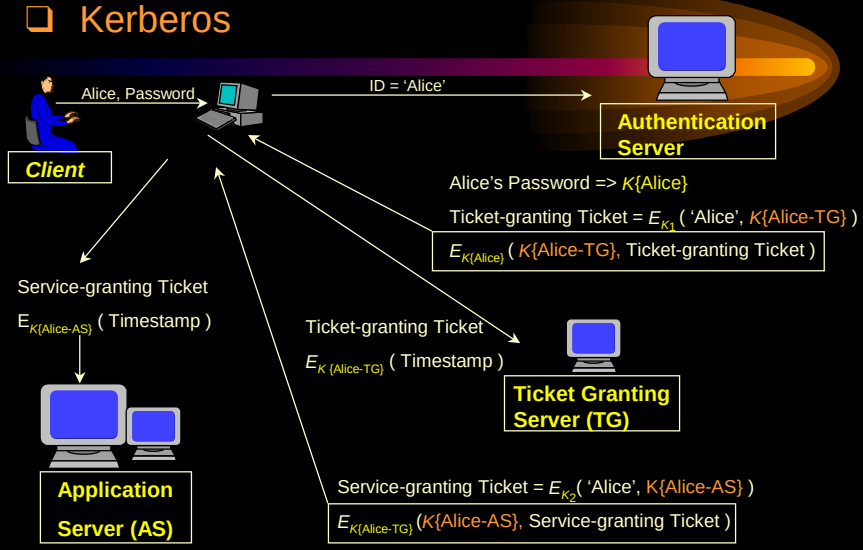
암호이론과 보안 KEY 분배

❑ Kerberos

- ❑ Trusted Third-Party stores all the passwords
- ❑ Kerberos System from MIT

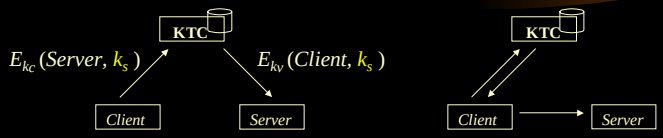


❑ Kerberos

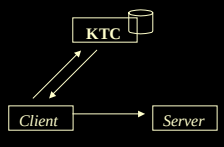


❑ 중앙 집중식 키 분배

❑ 키 번역 센터 (Key Translation Center : KTC)



❑ 대칭키 인증서 (Symmetric Key Certificate)



① E_{kT} (k_c, Client), E_{kc} (Server, k_s), E_{kT} (k_v, Server)

② E_{kv} (Client, k_s)

③ E_{kv} (Client, k_s)

❑ 중앙 집중식 키 분배

❑ 공개키 분배 센터

인증기관 (Certificate Authority)

X.509 Certificate

Version
Serial Number
Algorithm Identifier
Issuer
Period of Validity
Subject
Public key Information
Signature

Version : 인증서 구성의 버전을 나타낸다. 기본 값은 1988
Serial Number : CA에 의해서 인증서에 부여한 유일한 정수 값
Algorithm Identifier : 인증서를 서명하는 데에 사용된 알고리즘과 parameter
Issuer : 인증서를 생성하고 서명한 CA
Period of Validity : 인증서가 유효한 첫째 날과 마지막 날
Subject : 인증서가 발급되는 사용자
Public key Information : 사용자 공개키와 공개키가 사용되는 알고리즘 식별자
Signature : 위의 모든 항목에 일 방향 해쉬함수를 적용한 결과를 CA의 개인키로 서명한 값

❑ 분산식 키 설정

❑ 대칭형 암호에 기반을 둔 키 설정

① $Client \rightarrow Server : E_k(k_s, t, Server)$

[프로토콜 : 시각표를 이용한 세션 키 전송 프로토콜]

① $Client \leftarrow Server : r$
② $Client \rightarrow Server : E_k(k_s, r, Server)$

[프로토콜 : 난수를 이용한 세션 키 전송 프로토콜]

① $Client \rightarrow Server : r$

[프로토콜 : 합의된 방식에 의한 세션 키 도출 프로토콜]

❑ 분산식 키 설정

❑ 대칭형 암호에 기반을 둔 키 설정

① $Client \rightarrow Attacker : Client$
② $Client \leftarrow Attacker : f(r)$
③ $Client \rightarrow Attacker : E_k(f(r))$

[프로토콜 : 공격자의 서버 가장공격]

① $Client \rightarrow Server : Client$
② $Client \leftarrow Server : r_1$
③ $Client \rightarrow Server : E_k(f(r_1)) \oplus k_s, E_{k_s}(r_1)$

[프로토콜 : 일 방향 개인식별과 세션 키 분배 프로토콜]

암호이론과 보안 KEY 분배

❑ 분산식 키 설정

❑ 공개키 암호에 기반을 둔 키 설정

① $Client \rightarrow Server : [k_s, t, Client]P_v$

[프로토콜 : 세션 키 전송 프로토콜]

① $Client \rightarrow Server : [r_1, Client]P_v$
② $Client \leftarrow Server : [r_1, r_2]P_c$
③ $Client \rightarrow Server : [r_2]P_v$

[프로토콜 : 상호 개인식별과 세션 키 설정 프로토콜]