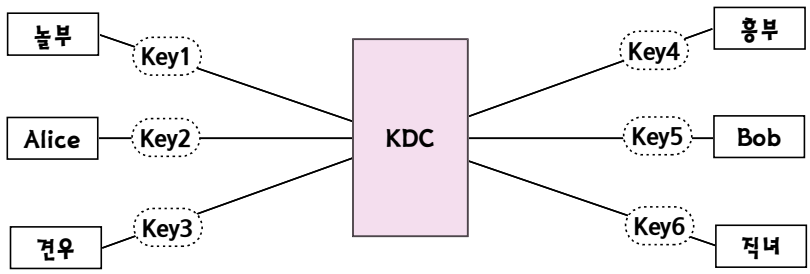
2. 키-분배센터(KDC)

• 먼저, 키-분배센터는 **대칭키 암호에서 비밀키 수를 최소화하기 위한 것**이다.
• 키-분배센터는 KDC(Key Distribution Center)라 한다.
• KDC는 대칭키 기반 암호에서 필요하다.

◉ KDC 기본 구조



• 그림처럼, KDC와 각 개인은 하나의 **대칭키(비밀키)를 공유**한다.(key1~key6)
• KDC는 자신과 새로 구성원이 되는 상대 사이에 공유하는 비밀키를 생성한다.
• 비밀키는 KDC와 각 구성원 사이에만 사용된다.(구성원끼리 통신에는 사용 불가)
• 구성원끼리 통신을 위해서, KDC는 **비밀키**를 이용하여 **세션 비밀키를 생성**해 준다.

▣ 놀부가 흥부와 비밀통신을 하려는 경우(대칭키 이용)

① 놀부는 흥부와 비밀통신을 위해 KDC에게 **세션 비밀키 요청 메시지**를 보낸다.
→ 비밀통신을 위해서는 반드시 **일회용 세션 비밀키**가 필요하다.
→ 세션 비밀키 요청 메시지는 **평문**으로 보낸다.(놀부 ID와 흥부 ID가 포함)

② KDC는 놀부의 통신 요청을 흥부에게 알린다.

③ 흥부가 동의하면, **KDC는 두 사람 사이의 세션 비밀키를 생성**한다.
• 놀부와 흥부 사이의 세션 비밀키는 놀부와 흥부의 비밀키를 이용하여 생성한다.
• 두 사람은 세션 비밀키를 이용하여 비밀통신을 할 수 있다.
• 세션 비밀키는 두 통신자 사이에 오직 한번만 사용한다.**(한번 사용 후 폐기)**
• 세션 비밀키는 공격자가 두 사람 중 어느 한 사람으로 위장하는 것을 방지한다.

KDC 프로토콜

KDC 관련 프로토콜은 몇 가지를 소개한다. 세부적인 내용은 생략한다.

(1) 하나의 KDC를 이용하는 단순 프로토콜

- 이 단순 프로토콜은 재생공격을 방지할 수 없는 **단점**이 있다.
  → 공격자가 중간에서 메시지를 저장해 두었다가 나중에 재전송(replay)할 수 있다.
- KDC 이용자가 증가하면 병목현상이 발생되므로 여러 개의 KDC를 설치하여 운영한다.
- 이 단순 프로토콜은 결함이 있어서 실제로 사용되지는 않는다.

(2) Needham-Schroeder(니덤-슈뢰더) 프로토콜

- 이 프로토콜은 문제점이 없다.(매우 좋은 프로토콜)
  → 송수신자 사이에 다중 시도-응답을 주고받는 방법을 사용한다.
- 이 프로토콜은 재전송 공격(reply attack)을 막는다.
  → 내부적으로 2개의 비표를 사용한다.(송수신자의 각 비표)
- 이 프로토콜은 다른 많은 프로토콜의 기초가 되고 있다.
  → **커버로스**는 Needham-Schroeder 프로토콜에 기반하고 있다.

(3) Otway-Rees 프로토콜

- 이 프로토콜도 특별한 결함은 없는 프로토콜이다.
- 이 프로토콜이 안전하기 위해서는 KDC 서버가 몇가지 작업을 수행해야 한다.
  → 아무튼, 세부적인 내용은 필요가 없으므로 생략한다.

기출문제 분석

1. 키 분배 문제를 해결하기 위한 방법으로 옳지 않은 것은? [2015년 국회 9급]

① 키를 사전에 공유
② 공개키 암호를 사용
③ Diffie-Hellman 알고리즘을 이용
④ 키 배포 센터(KDC)를 이용
⑤ SEED 암호 알고리즘을 이용

♤ **키 분배 문제 해결**

- SEED 암호는 대칭키 암호이다. **대칭키** 암호는 키 분배 문제를 **발생**시킨다.
- 키 분배 문제 해결은 공개키 암호와 연관을 가진다.
- 대칭키 암호는 키 분배 문제를 해결할 수 없다.

정답 : ⑤

2. 다음 중 kerberos 인증 프로토콜에 대한 설명으로 옳지 않은 것은? [2014년 서울 9급]

① Needham-Schroeder 프로토콜을 기반으로 만들어졌다.
② 대칭키 암호 알고리듬(algorithm)을 이용한다.
③ 중앙 서버의 개입 없이 분산 형태로 인증을 수행한다.
④ 티켓 안에는 자원 활용을 위한 키와 정보가 포함되어 있다.
⑤ TGT를 이용해 자원 사용을 위한 티켓을 획득한다.

♤ **kerberos 인증 프로토콜**

- 커버로스는 분산 환경에서 대칭키를 이용하는 중앙집중식 인증 방식이다.
  → 커버로스는 중앙 서버를 이용하여 분산 형태로 인증을 수행한다.
- 클라이언트는 KDC(키 배포 센터)에서 TGT를 요청하여 Kerberos 세션을 시작한다.
  → 이 요청은 통상적으로 로그인할 때 자동으로 수행된다.
  → TGT는 Ticket Granting Ticket(티켓 부여 티켓) 약어이다.
- TGT는 특정 서비스를 위한 다른 티켓을 얻는 데 필요하다.
- TGT는 여권과 비슷한 개념이다.
  → TGT는 여권처럼 사용자의 신원을 확인하며, 다수의 "비자"를 얻을 수 있도록 한다.
  → 여기서, "비자"(티켓)는 원격 시스템 또는 네트워크 서비스에 사용하기 위한 것이다.

정답 : ③