4.1 대칭 암호를 이용한 대칭키 분배

4장. 키 분배와 사용자 인증

키 분배 (1)

1. A가 키를 선택한 뒤 B에게 직접 전달
2. 제3자가 키를 선택한 뒤에 A와 B에게 직접 전달
3. A와 B의 공유키로 한 사람이 새 키를 만들고 공유키로 암호화하여 상대방에게 전송한다.
4. A와 B가 제3자인 C와 암호화된 연결이 확립되어 있다면, C가 암호화된 링크를 통해서 A와 B에게 키를 전달한다.

키 분배 (2)

- 방법 1, 2
  - 링크 암호화에서 적합 (링크 다른 쪽만 교환)
  - 네트워크 상에서는 곤란
- 방법 3
  - 링크 암호나 종단 간 암호화에 모두 사용 가능
  - 공격자가 사용된 키 하나만 얻을 수 있다면, 그 이후 모든 키 노출
- 방법 4
  - 종단 간 암호화에 적합

4 번째 방법에서 키 사용

- 세션키(Session key):
  - 세션이라고 하는 논리적 연결이 유지되는 동안 모든 사용자 데이터는 일회용 세션키로 암호화
  - 한 세션에만 사용
- 영구 키(Permanent key):
  - 영구 키는 세션키 분배에 필요한 키
  - 복수 회 사용
  - 키 분배 센터(KDC: key distribution center)에서 활용
- KDC(Key Distribution Center) 필요
  - 양쪽에게 일회용 세션키 분배

KDC 키 분배 절차

1. A가 B와 통신을 원하면 연결 요청 패킷을 KDC에 전송
   - A와 KDC 사이의 통신은 A와 KDC가 공유하고 있는 마스터키로 암호화
2. KDC가 연결요청 후 KDC는 일회용 세션키 생성
   - 세션키를 A와 공유하고 있는 영구키로 암호화한 다음 A에게 전송
   - 동일한 방법으로 KDC는 이 세션키를 B와 공유하고 있는 영구키로 암호화한 뒤 B에게 전송
3. A와 B는 논리적 연결가능.
   - 세션키를 이용하여 데이터를 암호화하여 전송