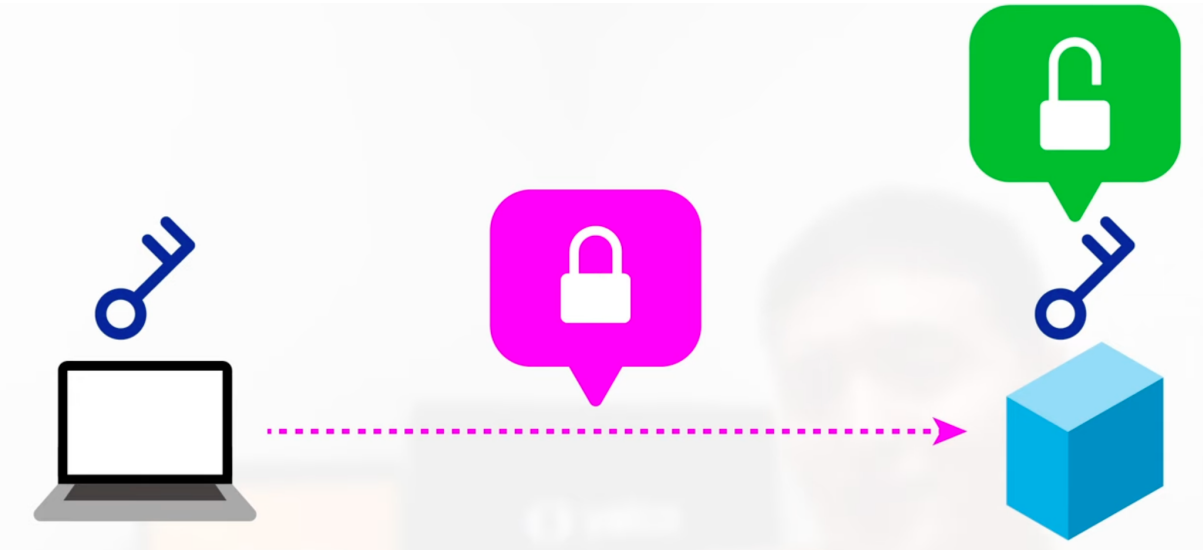
대칭키 & 비대칭키

대칭키(Symmetric Key)



- **어떤 정보를 암호화, 복호화할 때 사용하는 키가 동일한 알고리즘**을 의미한다.
    - 즉, **암호화 할 때 필요한 키 값**과, **해당 정보를 복호화할 때 필요한 키 값**이 **동일**한 경우이다.

- **전송자**는 상대방에게 보내고자 하는 메시지를 **키와 함께 특정 알고리즘을 통해 암호화**한다.
    - **수신자**는 **키와 함께 특정 알고리즘을 거꾸로 돌려 복호화**한다.

- **암호화된 정보를 확인하기 위해 전송자, 수신자 모두 동일한 키를 가지고 있어야 한다.**

  → **키 값을 알지 못하면 절대 암호화된 정보를 해독할 수 없다.**

- **다만, 동일한 키를 어떤 식으로 안전하게 교환할 수 있을지 생각해야 한다. (키 배송 문제)**
    - 물리적으로 직접 만나 키값을 전달하지 않는 한, **대칭키 전달 과정에서 해킹 위험에 노출될 수 있다.**

→ 전송자가 수신자에게 전달하는 과정에서 키값을 함께 전송하면 누군가 해당 키 값을 가로챌 수 있다.

- **인원이 많아질수록 키 교환의 횟수도 늘어나며 관리해야 할 키의 수가 많아지게 된다.**

공개키(Asymmetric Key)

- **어떤 정보를 암호화, 복호화할 때 사용하는 키가 서로 다른 알고리즘**을 의미한다.
  - **A키**로 암호화를 하면 **B키**로만 복호화가 가능하다.

    → **즉, 동일한 키로는 복호화가 불가능하다.**
  - 공개키의 **키 배송 문제를 해결**하기 위해 고안되었다.

- 대칭키와 다르게 **비대칭키를 활용한 암호화에는 개인키, 공개키 두 가지가 사용**된다.
  - **공개키** → **모든 사람**이 접근 가능한 키
  - **개인키** → **특정 사용자만**이 가지고 있는 키

- **비대칭키를 활용한 암호화**는 **두 가지**로 나뉜다.
  - **공개키로 정보를 암호화하는 방식**
    - **어떤 정보를 특정 사용자에게 보낼 때 해당 사용자의 공개키를 통해 정보를 암호화하여 전송**한다.
      1. 부산에 살고 있는 철수가 **영희의 공개키를 통해 정보를 암호화**한 후 영희에게 전송한다.
      2. 정보는 영희의 공개키로 암호화되었기 때문에 **열어보기 위해 영희의 개인키를 사용**한다.

         → **위에서 이야기했듯이 동일한 키로는 복호화가 불가능, 즉 공개키로는 해독이 불가하다.**
      3. 영희의 개인키는 영희 자신만 가지고 있으므로, 받은 정보를 안전하게 해독할 수 있다.

         → **키 배송 문제를 해결한 방법이라고 볼 수 있다.**

→ 키가 서로 다르기 때문에 암호화/복호화 과정이 매우 복잡하다.

- **개인키로 정보를 암호화하는 방식**
  - **어떤 정보를 특정 사용자에게 보낼 때 자기 자신의 개인키를 통해 정보를 암호화하여 전송**한다.
    1. 부산에 살고 있는 철수가 개인키를 통해 정보를 암호화한 후 영희에게 전송한다.
    2. 철수의 공개키는 모두에게 공개가 되어있다.
    3. 영희는 정보를 받은 후 공개된 철수의 공개키를 통해 정보를 해독한다.

       → **정보 안에 무엇이 들었는지보다, 정보를 누가 보냈는지에 초점을 둔 방법이다.**

       → **철수의 개인키로 암호화한 정보는 철수의 공개키로만 열 수 있기에,** 어떤 정보가 철수의 공개키로 인해 해독된다면 **해당 정보는 철수가 보낸게 확실하다는 뜻**이 된다.

       → 해당 기술은 **데이터 제공자의 신원이 보장**되는 전자서명 등의 공인인증 체계에서 사용된다.

References

- https://www.youtube.com/watch?v=H6lpFRpyl14
- https://universitytomorrow.com/22