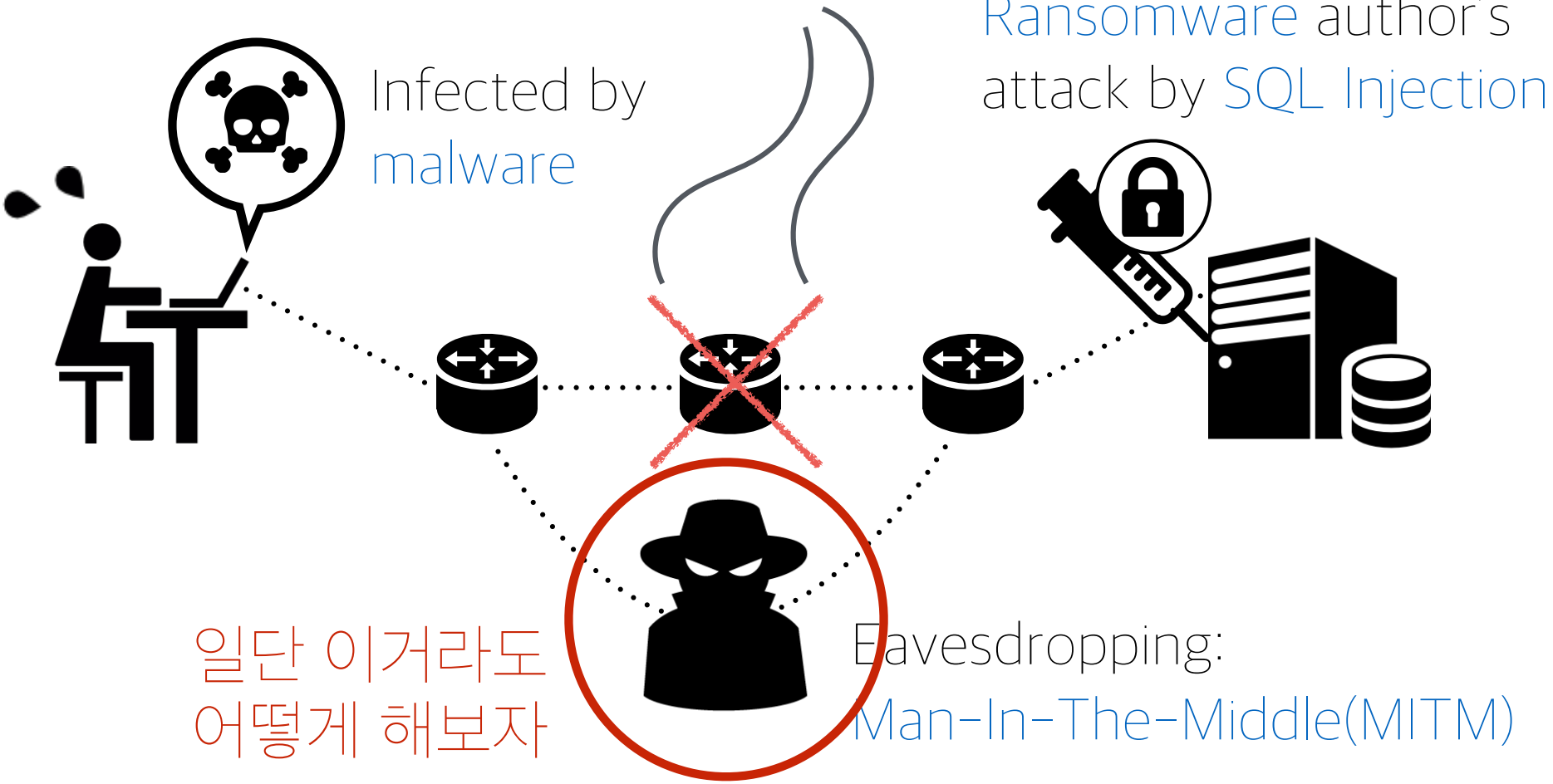
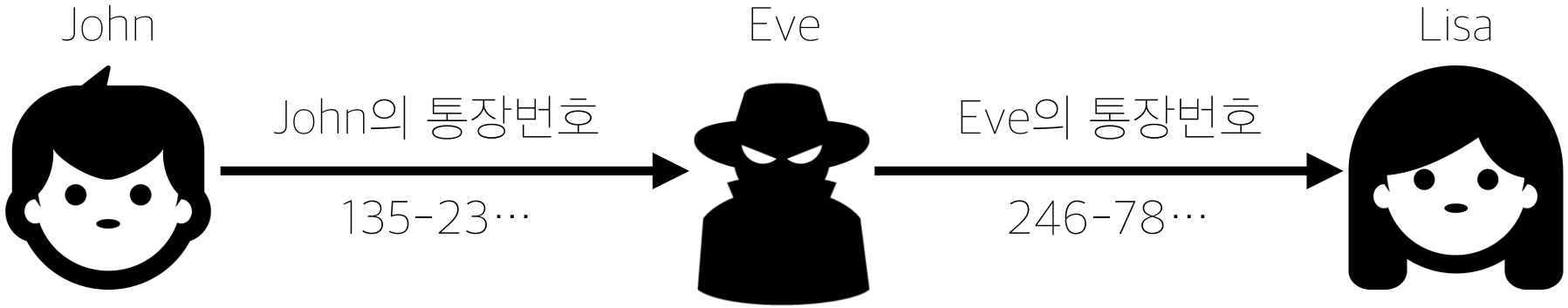
안전한 곳은 없다


Infected by
malware
Ransomware author's
attack by SQL Injection
일단 이거라도
어떻게 해보자
Eavesdropping:
Man-In-The-Middle(MITM)

상황을 조금이나마 해결해보자

중간자 공격(man in the middle attack, MITM)은 네트워크 통신을 조작하여 **통신 내용을 도청하거나 조작**하는 공격 기법이다. 중간자 공격은 통신을 연결하는 두 사람 사이에 중간자가 침입하여, **두 사람은 상대방에게 연결했다고 생각**하지만 실제로는 두 사람은 중간자에게 연결되어 있으며 중간자가 한쪽에서 **전달된 정보를 도청 및 조작한 후 다른 쪽으로 전달**한다.

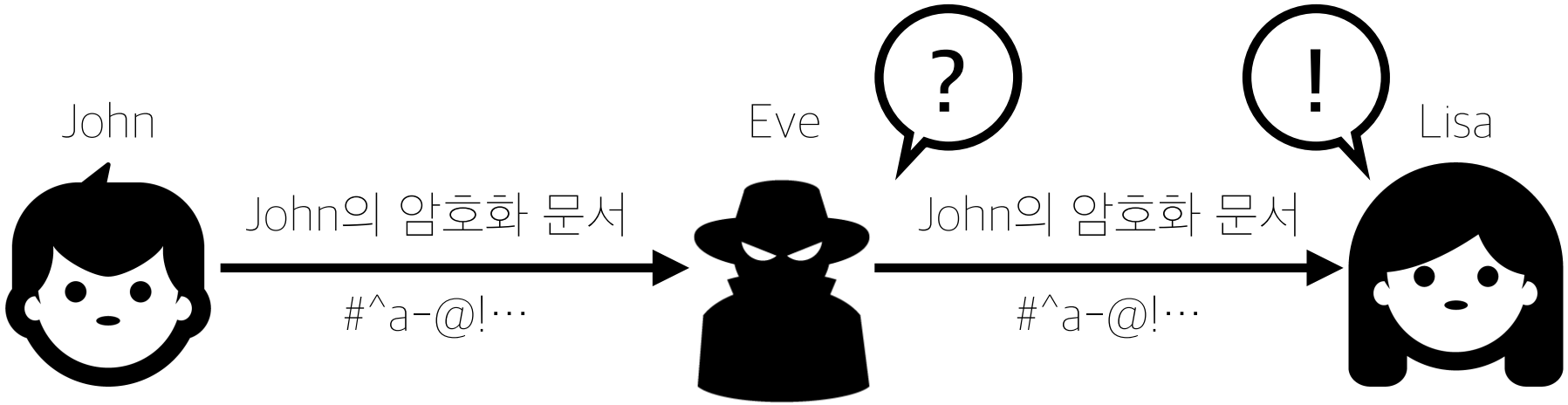


중간자공격, https://ko.wikipedia.org/wiki/%EC%A4%91%EA%B0%84%EC%9E%90_%EA%B3%B5%EA%B2%A9

상황을 조금이나마 해결해보자

‘Eve’가 내용을 모르게 해야 한다 !

공개 키 암호방식이 가장 만만하다



상황을 조금이나마 해결해보자

공개 키 암호 방식

공개 키는 누구나 소유할 수 있다.
공개 키를 이용하여 문서를 암호화하게 되면,
비밀 키를 이용해야만 문서를 해독할 수 있게 된다.

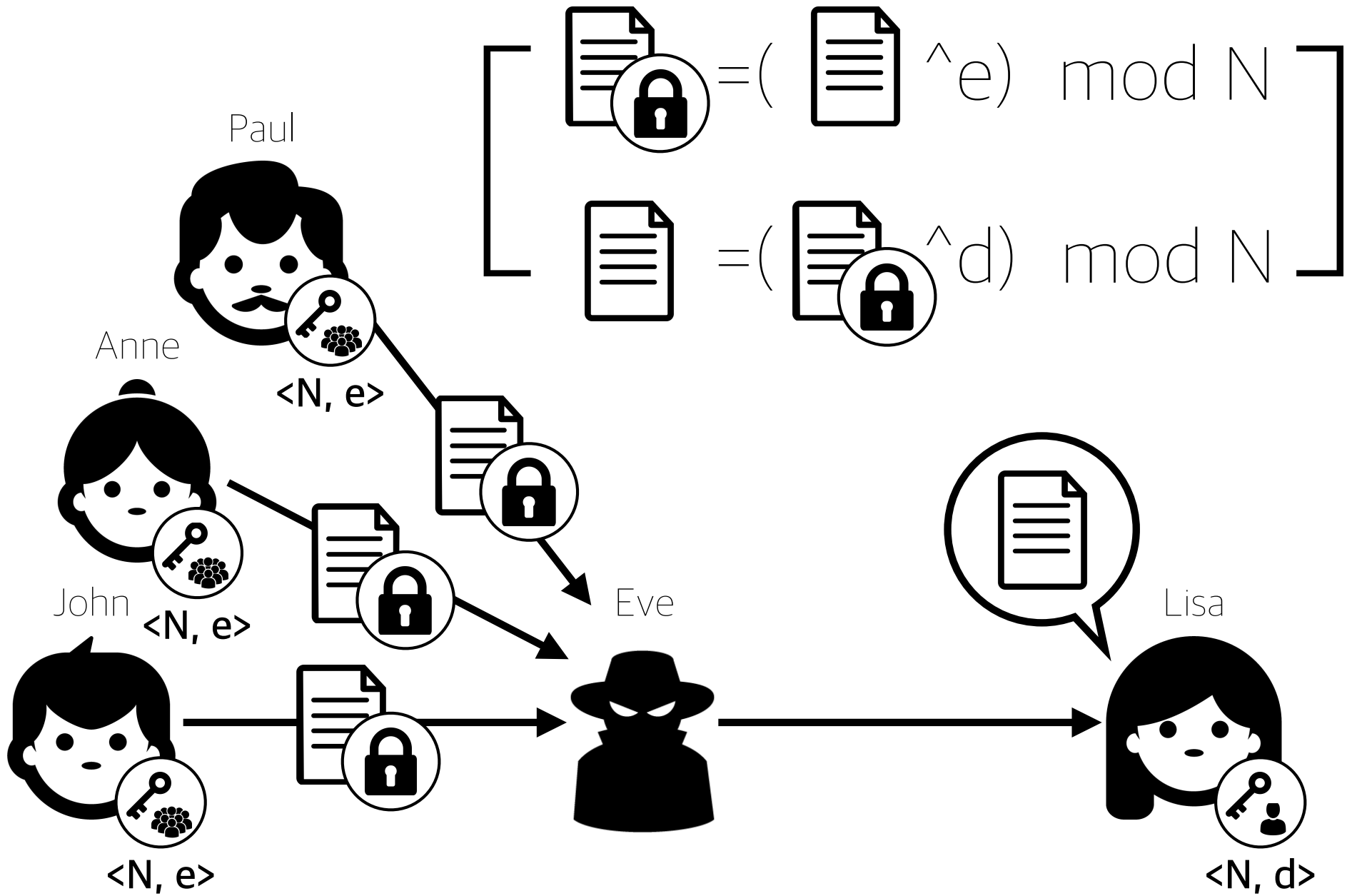
공개 키 암호 방식, https://ko.wikipedia.org/wiki/%EA%B3%B5%EA%B0%9C_%ED%82%A4_%EC%95%94%ED

상황을 조금이나마 해결해보자

RSA 암호

소인수 분해의 난해함에 기반하여,
공개 키 만을 가지고는 개인 키를 쉽게
짐작할 수 없도록 디자인되어 있다.

RSA 암호, https://ko.wikipedia.org/wiki/RSA_%EC%95%94%ED%98%B8


=(^e) mod N
=(^d) mod N
Paul
<N, e>
Anne
<N, e>
John
<N, e>
Eve
Lisa
<N, d>

1. 키 생성에 사용된 소수 혹은 비밀 키 등이
   도난 당하지 않는 이상, 문서가 해독될
   가능성은 매우 희박하다.
2. 여기서 John의 비밀 키로 문서를 암호화 한다면,
   오직 John의 공개 키로만 문서가 해독된다.
   이는 문서의 저자가 John임을 증명한다.
3. 따라서 RSA는 지금도 전자서명 알고리즘으로
   주로 사용되고 있다.